Міністерство освіти і науки України
Центральноукраїнський національний технічний університет

**Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А.,
Буравченко К.О., Смірнова Т.В., Поліщук Л.І.**

ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Навчальний посібник

Кропивницький
2020

УДК 004.7
ББК 32.973.202
С 50

Рекомендовано Вченою радою Центральноукраїнського національного технічного університету, протокол № 6 від 2 березня 2020 року

Рецензенти:
Павленко М.А., доктор технічних наук, професор, начальник кафедри математичного та програмного забезпечення АСУ Харківського університету Повітряних Сил ім.. Івана Кожедуба;
Семенов С.Г., доктор технічних наук, старший науковий співробітник, Завідувач кафедрою обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний університет».

Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І.
С 50 Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.

У навчальному посібнику розглянуто теоретичні й практичні питання основ і положень теорії інформаційної безпеки в комп'ютерних мережах, побудови систем захисту інформації в комп'ютерних мережах, адміністрування систем захисту інформації в комп'ютерних мережах

Навчальний посібник призначений для студентів, які навчаються за спеціальностями «Кібербезпека», «Комп'ютерні науки», «Комп'ютерна інженерія», а також аспірантів, науковців та інженерно-технічних працівників з напряму «Інформаційні технології».

ББК 32.973.202

© Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. 2020
© Видавець Лисенко В. Ф., 2020

ВСТУП

У сучасному суспільстві для задоволення його потреб виникають проблеми інформаційного забезпечення всіх сфер діяльності людини. Одна з таких проблем – ***забезпечення надійного захисту інформації***. Особливої гостроти вона набуває у зв’язку з масовою комп’ютеризацією всіх видів діяльності людини, при об’єднанні комп’ютерів у комп’ютерні мережі та підключення до Internet. Тому для спеціалістів різноманітного профілю актуальною є підготовка в галузі захисту інформації.

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

Очевидно, що надійно захистити повідомлення й комп’ютерні бази даних від розголошення і перехоплення може тільки повне їх шифрування. Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням сьогодні стає захист інформації в комп'ютерних мережах.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їх обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

В даному навчальному посібнику розглядається безпека мережі та заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований

доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

Метою даного навчального посібника є отримання досконалих знань в області теорії інформаційної безпеки комп’ютерних мереж та їх практичних застосувань, а також отримання студентами навичок адміністрування систем захисту інформації в комп’ютерних мережах та побудови систем захисту інформації в комп’ютерних мережах.

Представлений в навчальному посібнику матеріал надасть фахівцям практичні рекомендації і допоможе навчитися проектувати і розробляти системи захисту для будь-яких мереж і компаній.

РОЗДІЛ 1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО АТАКИ НА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ДАНІ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Комп'ютерні атаки й технології їхнього виявлення

Атакою на інформаційну систему називаються навмисні дії зловмисника, що використовують уразливості інформаційної системи й приводять до порушення доступності, цілісності й конфіденційності оброблюваної інформації.

Усунемо уразливості інформаційної системи – усунемо й можливість реалізації атак. На сьогоднішній день вважається невідомим, скільки існує методів атак.

Моделі атак

Традиційна модель атаки будується за принципом "один до одного" (рис. 1.1) або "один до багатьох" (рис. 1.2), тобто атака виходить із одного джерела. Розроблювачі мережних засобів захисту (міжмережних екранів, систем виявлення атак і т.д.) орієнтовані саме на традиційну модель атаки.

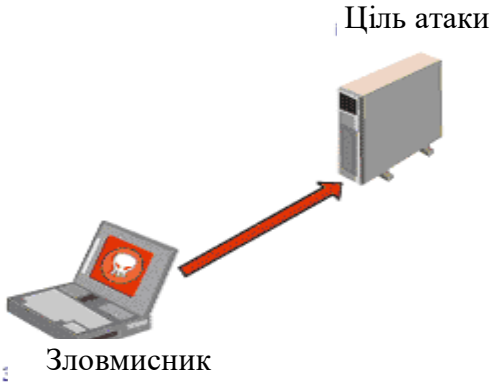

Рисунок 1.1 – Відношення "один до одного"

У різних точках мережі, яка захищається, установлюються агенти (сенсори) системи захисту, які передають інформацію на центральну

консоль керування. Це полегшує масштабування системи, забезпечує простоту віддаленого керування й т.д. Однак така модель не справляється з розподіленими атаками.

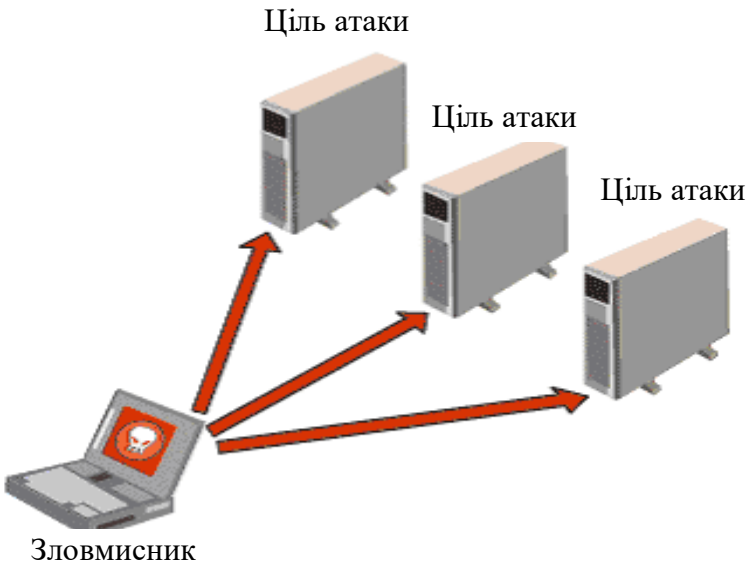

Рисунок 1.2 – Відношення "один до багатьох"

У моделі розподіленої атаки використовуються інші принципи. На відміну від традиційної моделі в розподіленої моделі використовуються відносини "багато до одного" (рис. 1.3) і "багато до багатьох" (рис. 1.4).

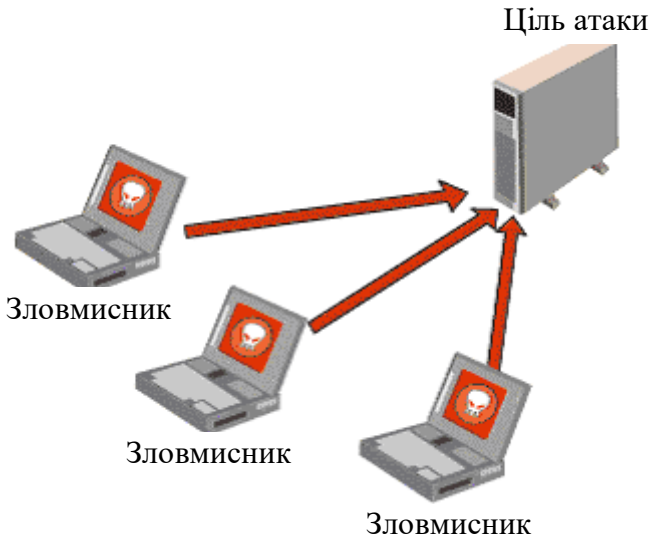

Рисунок 1.3 – Відношення "багато до одного"

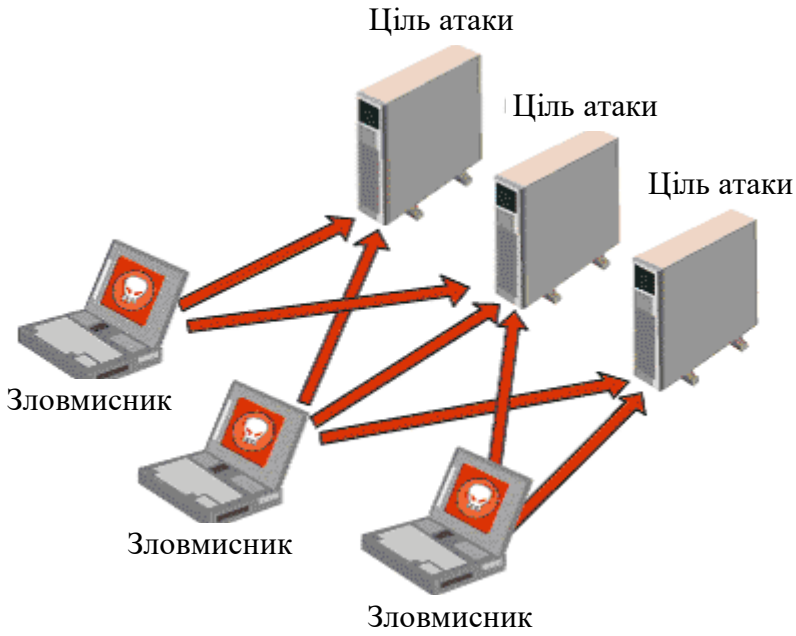

Рисунок 1.4 – Відношення "багато до багатьох"

Розподілені атаки засновані на "класичних" атаках типу "відмова в обслуговуванні", а точніше на їхній підмножині, відомому як Flood-атаки або Storm-атаки (зазначені терміни можна перевести як "шторм", "повінь" або "лавина"). Зміст даних атак полягає в посиланні великої кількості пакетів на вузол, який атакується. Вузол, що атакується, може вийти з ладу, оскільки він "захлинеться" у лавині пакетів, що посилаються, і не зможе обробляти запити авторизованих користувачів. За таким принципом працюють атаки SYN-Flood, Smurf, UDP Flood, Targa3 і т.д. Однак у тому випадку, якщо пропускна здатність каналу до вузла, що атакується, перевищує пропускну здатність атакуючого або вузол, що атакується, некоректно зконфігурований, то до "успіху" така атака не приведе. Наприклад, за допомогою цих атак даремно намагатися порушити працездатність свого провайдеру. Але розподілена атака відбувається вже не з однієї точки Internet, а відразу з декількох, що приводить до різкого зростання трафіку й виведенню вузла, що атакується, з ладу.

Етапи реалізації атак

Можна виділити наступні етапи реалізації атаки:

– попередні дії перед атакою або "збір інформації";

– власно "реалізація атаки";

– завершення атаки.

Звичайно, коли говорять про атаку, то мають на увазі саме другий етап, забуваючи про перший й останній.

Збір інформації й завершення атаки ("замітання слідів") у свою чергу також можуть бути атакою й можуть бути розділені на три етапи:

– передумови реалізації атаки;

– реалізація атаки;

– завершення атаки.

Збір інформації – це основний етап реалізації атаки. Саме на даному етапі ефективність роботи зловмисника є запорукою "успішності" атаки. Спочатку вибирається ціль атаки й збирається інформація про неї (тип і версія операційної системи, відкриті порти й запущені мережні сервіси, установлене системне й прикладне програмне забезпечення і його конфігурація й т.д.). Потім ідентифікуються найбільш уразливі місця системи, яка атакується, вплив на які приводить до потрібного зловмисника результату. Зловмисник намагається виявити всі канали взаємодії (цілі) атаки з іншими вузлами. Це дозволить не тільки вибрати тип реалізованої атаки, але й джерело її реалізації.

Наприклад, вузол, який атакується взаємодіє із двома серверами під керуванням ОС Unix і Windows. З одним сервером вузол, який атакується, має довірені відносини, а з іншим – немає. Від того, через який сервер зловмисник буде реалізовувати напад, залежить, яка атака буде задіяна, який засіб реалізації буде обрано й т.д. Потім, залежно від отриманої інформації й бажаного результату, вибирається атака, що дає найбільший ефект. Наприклад:

– SYN Flood, Teardrop, UDP Bomb – для порушення функціонування вузла;

– CGI-скрипт – для проникнення на вузол і крадіжки інформації;

– PHF – для крадіжки файлу паролів і віддаленого підбора пароля й т.п.

Традиційні засоби захисту, такі як міжмережні екрани або механізми фільтрації в маршрутизаторах, вступають у дію лише на другому етапі реалізації атаки, зовсім "забуваючи" про перший й третій. Це приводить до того, що найчастіше здійснену атаку дуже важко зупинити, навіть при наявності потужних і дорогих засобів захисту. Приклад тому – розподілені атаки. Логічно було б, щоб засоби захисту починали працювати ще на першому етапі, тобто запобігали б можливість збору інформації про систему, яка атакується. Це дозволило б якщо й не повністю запобігти атаці, та хоча б істотно ускладнити роботу зловмисника. Традиційні засоби також не дозволяють виявити вже зроблені атаки й оцінити збиток після їхньої реалізації, тобто не працюють на третьому етапі реалізації атаки. Отже, неможливо визначити заходу щодо запобігання таких атак надалі.

Залежно від бажаного результату порушник концентрується на тім або іншому етапі реалізації атаки. Наприклад:

– для відмови в обслуговуванні докладно аналізується мережа, яка атакується, у ній вишукуються слабкі місця;

– для розкрадання інформації основна увага приділяється непомітному проникненню на вузли, які атакуються, за допомогою виявлених раніше уразливостей.

Розглянемо основні механізми реалізації атак. Це необхідно для розуміння методів виявлення цих атак. Крім того, розуміння принципів дій зловмисників – застава успішної оборони мережі.

1. Збір інформації

Перший етап реалізації атак – це збір інформації про систему, яка атакується, або вузол. Він включає такі дії як визначення мережної топології, типу й версії операційної системи вузла, що атакується, а також доступних мережних і інших сервісів і т.п. Ці дії реалізуються різними методами.

Вивчення оточення

На цьому етапі нападаючий досліджує мережне оточення навколо передбачуваної цілі атаки. До таких областей, наприклад, відносяться вузли Internet-провайдеру "жертви" або вузли віддаленого офісу компанії, яка атакується. На цьому етапі зловмисник може намагатися визначити адреси "довірених" систем (наприклад, мережа партнера) і вузлів, які прямо з'єднані з метою атаки (наприклад, маршрутизатор ISP) і т.д. Такі дії досить важко виявити, оскільки вони виконуються протягом досить тривалого періоду часу й з зовні області, контрольованої засобами захисту (міжмережними екранами, системами виявлення атак і т.п.).

Ідентифікація топології мережі

Існує два основних методи визначення топології мережі, використовуваних зловмисниками:

– зміна TTL (TTL modulation);

– запис маршруту (record route).

За першим методом працюють програми traceroute для Unix і tracert для Windows. Вони використовують поле Time to Live ("час життя") у заголовку IP-пакета, що змінюється залежно від числа пройдених мережним пакетом маршрутизаторів. Для запису маршруту ICMP-пакета може бути використана утиліта ping . Найчастіше мережну топологію можна з'ясувати за допомогою протоколу SNMP, установленого на багатьох мережних пристроях, захист яких невірно зконфігурований. За допомогою протоколу RIP можна спробувати одержати інформацію про таблицю маршрутизації в мережі й т.д.

Багато які з цих методів використовуються сучасними системами керування (наприклад, HP OpenView, Cabletron SPECTRUM, MS Visio і т.д.) для побудови карт мережі. І ці ж методи можуть бути з успіхом застосовані зловмисниками для побудови карти мережі, яка атакується.

Ідентифікація вузлів

Ідентифікація вузла, як правило, здійснюється шляхом посилки за допомогою утиліти ping команди ECHO_REQUEST протоколу ICMP. Відповідне повідомлення ECHO_REPLY говорить про те, що вузол доступний. Існують вільно розповсюджувані програми, які автоматизують і прискорюють процес паралельної ідентифікації великої кількості вузлів, наприклад, fping або nmap. Небезпека даного методу в тому, що стандартними засобами вузла запити ECHO_REQUEST не фіксуються. Для цього необхідно застосовувати засоби аналізу трафіку, міжмережні екрани або системи виявлення атак.

Це найпростіший метод ідентифікації вузлів. Однак він має два недоліки.

– Багато мережних пристроїв і програм блокують ICMP-пакети й не пропускають їх у внутрішню мережу (або навпаки не пропускають їх назовні). Наприклад, MS Proxy Server не дозволяє проходження пакетів за протоколом ICMP. У результаті виникає неповна картина. З іншого боку, блокування ICMP-пакета говорить зловмисникові про наявність "першої лінії оборони" – маршрутизаторів, міжмережевих екранів і т.д.

– Використання ICMP-запитів дозволяє з легкістю виявити їхнє джерело, що, зрозуміло, не може входити до завдання зловмисника.

Існує ще один метод ідентифікації вузлів – використання "змішаного" режиму мережної карти, що дозволяє визначити різні вузли в сегменті мережі. Але він не застосовується в тих випадках, у яких трафік сегмента мережі недоступний нападаючий зі свого вузла, тобто цей метод застосуємо тільки в локальних мережах. Іншим способом ідентифікації вузлів мережі є так звана розвідка DNS, що дозволяє ідентифікувати вузли корпоративної мережі за допомогою звертання до сервера служби імен.

Ідентифікація сервісів або сканування портів

Ідентифікація сервісів, як правило, здійснюється шляхом виявлення відкритих портів (port scanning). Такі порти дуже часто пов'язані із сервісами, заснованими на протоколах TCP або UDP. Наприклад:

– відкритий 80-й порт має на увазі наявність Web-серверу;

– 25-й порт – поштового SMTP-серверу;

– 31337-й – серверної частини троянського коня BackOrifice;

– 12345-й або 12346-й – серверної частини троянського коня NetBus і т.д.

Для ідентифікації сервісів і сканування портів можуть бути використані різні програми, у т.ч. і вільно розповсюджувані. Наприклад, nmap або netcat.

Ідентифікація операційної системи

Основний механізм віддаленого визначення ОС – аналіз відповідей на запити, що враховують різні реалізації TCP/ IP-стека в різних операційних системах. У кожної ОС по-своєму реалізований стек протоколів TCP/IP, що дозволяє за допомогою спеціальних запитів і відповідей на них визначити, яка ОС установлена на віддаленому вузлі.

Інший, менш ефективний і вкрай обмежений, спосіб ідентифікації ОС вузлів – аналіз мережних сервісів, виявлених на попередньому етапі. Наприклад, відкритий 139-й порт дозволяє зробити висновок, що віддалений вузол, найімовірніше, працює під керуванням ОС сімейства Windows. Для визначення ОС можуть бути використані різні програми. Наприклад, nmap або queso.

Визначення ролі вузла

Передостаннім кроком на етапі збору інформації про вузол, який атакується, є визначення його ролі, наприклад, виконанні функцій міжмережного екрана або Web-сервера. Виконується цей крок на основі вже зібраної інформації про активні сервіси, імена вузлів, топології мережі й т.п. Наприклад, відкритий 80-й порт може вказувати на наявність Web-

сервера, блокування ICMP-пакета вказує на потенційну наявність міжмережного екрана, а DNS-ім'я вузла proxy.domain.ua або fw.domain.ua говорить саме за себе.

Визначення уразливостей вузла

Останній крок – пошук уразливостей. На цьому кроці зловмисник за допомогою різних автоматизованих засобів або вручну визначає уразливості, які можуть бути використані для реалізації атаки. Такі автоматизовані засоби можуть бути використані ShadowSecurityScanner, nmap, Retina і т.д.

2. Реалізація атаки

Із цього моменту починається спроба доступу до вузла, який атакується. При цьому доступ може бути як безпосередній, тобто проникнення на вузол, так і опосередкований, наприклад, при реалізації атаки типу "відмова в обслуговуванні". Реалізація атак у випадку безпосереднього доступу також може бути розділена на два етапи:

– проникнення;

– установлення контролю.

Проникнення

Проникнення має на увазі під собою подолання засобів захисту периметра (наприклад, міжмережного екрана). Реалізовуватися це може різними шляхами. Наприклад, використання уразливості сервісу комп'ютера, "який дивиться" назовні або шляхом передачі ворожого змісту по електронній пошті (макровіруси) або через апплети Java. Такий зміст може використовувати так звані "тунелі" у міжмережному екрані (не плутати з тунелями VPN), через які потім і проникає зловмисник. До цього ж етапу можна віднести підбор пароля адміністратора або іншого користувача за допомогою спеціалізованої утиліти (наприклад, L0phtCrack або Crack).

Встановлення контролю

Після проникнення зловмисник установлює контроль над вузлом, який атакується. Це може бути здійснене шляхом впровадження програми типу "троянський кінь" (наприклад, NetBus або BackOrifice). Після установки контролю над потрібним вузлом і "замітання" слідів, зловмисник може здійснювати всі необхідні несанкціоновані дії дистанційно без ведена власника атакованого комп'ютера. При цьому встановлення контролю над вузлом корпоративної мережі повинне зберігатися й після перезавантаження операційної системи. Це може бути реалізовано шляхом заміни одного із завантажувальних файлів або вставки посилання на ворожий код у файли автозавантаження або системний реєстр. Відомий випадок, коли зловмисник зміг перепрограмувати EEPROM мережної карти й навіть після перезавантаження ОС він зміг повторно реалізувати несанкціоновані дії. Більш простою модифікацією цього приклада є впровадження необхідного коду або фрагмента в сценарій мережного завантаження.

Цілі реалізації атак

Необхідно відзначити, що зловмисник на другому етапі може переслідувати дві цілі. По-перше, одержання несанкціонованого доступу до самого вузла й інформації, що втримується на ньому. По-друге, одержання несанкціонованого доступу до вузла для здійснення подальших атак на інші вузли. Перша ціль, як правило, здійснюється тільки після реалізації другої. Тобто, спочатку зловмисник створює собі базу для подальших атак і тільки після цього проникає на інші вузли. Це необхідно для того, щоб сховати або істотно затруднити знаходження джерела атаки.

3. Завершення атаки

Етапом завершення атаки є "замітання слідів" з боку зловмисника. Звичайно це реалізується шляхом видалення відповідних записів з журналів реєстрації вузла й інших дій, що повертають атаковану систему у вихідний, стан.

Класифікація атак

Існують різні типу класифікації атак. Наприклад, розподіл на пасивні й активні, зовнішні й внутрішні, навмисні й ненавмисні. Однак щоб не заплутатися в великому розмаїтті класифікацій, що мало застосовуються на практиці, пропонується більш "життєва" класифікація:

1. Віддалене проникнення (remote penetration). Атаки, які дозволяють реалізувати віддалене керування комп'ютером через мережу. Наприклад, NetBus або BackOrifice.

2. Локальне проникнення (local penetration). Атака, що приводить до одержання несанкціонованого доступу до вузла, на якому вона запущена. Наприклад, GetAdmin.

3. Віддалена відмова в обслуговуванні (remote denial of service). Атаки, які дозволяють порушити функціонування або перевантажити комп'ютер через Internet. Наприклад, Teardrop або trin00.

4. Локальна відмова в обслуговуванні (local denial of service). Атаки, які дозволяють порушити функціонування або перевантажити комп'ютер, на якому вони реалізуються. Прикладом такої атаки є "ворожий" апплет, що завантажує центральний процесор нескінченним циклом, що приводить до неможливості обробки запитів інших застосунків.

5. Мережні сканери (network scanners). Програми, які аналізують топологію мережі й виявляють сервіси, доступні для атаки. Наприклад, система nmap.

6. Сканери уразливостей (vulnerability scanners). Програми, які шукають уразливості на вузлах мережі і які можуть бути використані для реалізації атак. Наприклад, система SATAN або ShadowSecurityScanner.

7. Зломщики паролів (password crackers). Програми, які "підбирають" паролі користувачів. Наприклад, L0phtCrack для Windows або Crack для Unix.

8. Аналізатори протоколів (sniffers). Програми, які "прослуховують" мережний трафік. За допомогою цих програм можна автоматично шукати таку інформацію, як ідентифікатори й паролі користувачів, інформацію про кредитні карти й т.д. Наприклад, Microsoft Network Monitor, NetXRay компанії Network Associates або LanExplorer.

Компанія Internet Security Systems, Inc. ще більше скоротила число можливих категорій, довівши їх до 5:

– збір інформації (Information gathering);

– спроби несанкціонованого доступу (Unauthorized access attempts);

– відмова в обслуговуванні (Denial of service);

– підозріла активність (Suspicious activity);

– системні атаки (System attack).

Перші 4 категорії відносяться до віддалених атак, а остання – до локальних, реалізованих на вузлі, який атакується. Можна помітити, що в дану класифікацію не потрапив цілий клас так званих "пасивних" атак ("прослуховування" трафіку, "помилковий DNS-сервер", "підміна ARP-сервера" і т.п.).

Класифікація атак, реалізована в багатьох системах виявлення атак, не може бути категоричною. Наприклад, атака, реалізація якої для ОС Unix (наприклад, переповнення буфера statd) може мати самі жалюгідні наслідки (найвищий пріоритет), для ОС Windows може бути взагалі не застосовна або мати дуже низький ступінь ризику. Крім того, існує плутанина й у самих назвах атак і уразливостей. Та сама атака, може мати різні найменування в різних виробників систем виявлення атак.

Однієї із кращих баз уразливостей і атак є база даних X-Force, що перебуває за адресою: http://xforce.iss.net/. Доступ до неї може здійснюватися як шляхом передплати на вільно розповсюджуваний список розсилання X-Force Alert, так і шляхом інтерактивного пошуку в базі даних на Web-сервері компанії ISS.

DDoS – комп'ютерні атаки. Технології їхнього виявлення. Захист

Найпоширеніші останнім часом атаки категорії "відмова в обслуговуванні" – це DDoS атаки. DDoS – від англ. Distributed Denial of Service. При цьому виді атак з різних адрес Інтернету відбуваються численні звернення на сервер-жертву. Метою цієї атаки є блокування мережних сервісів за рахунок створення маси звернень на сервер-жертву.

Для виявлення й аналізу атак цього виду використовуються апаратно-програмні засоби. Атаки характеризуються наступними основними параметрами:

– потужність атаки (Мбіт/с);

– розподіленість (кількість підмереж з яких ведеться атака).

Захист від розподілених DDoS-атак ґрунтується на аналізі трафіку, що надходить на вузлом, який захищається. Під час нормальної роботи система захисту саме навчається, а після виявлення атаки або автоматично, або на вимогу, активно протидіє DDoS – трафіку. Ефективність захисту від DDoS-атак звичайно описується трьома основними параметрами:

– потужність атаки (Мбіт/с), що здатна витримати система;

– точність дій системи при виявленні й відбитті атаки;

– імовірність і кількість помилкових спрацьовувань (False Positive).

При виборі системи захисту від DDoS атак потрібно враховувати важливі фактори:

– потужність атаки (Мбіт/с), що здатна витримати система;

– точність дій системи при виявленні й відбитті атаки;

– імовірність і кількість помилкових спрацьовувань (False Positive);

– оперативна можливість перенаправлення трафіку (Зміна IP основного сервера);

– захист на вимогу – можливість включити захист від DDoS тільки на час атаки;

– пороги обмежень по трафіку/продуктивності системи.

Варіанти реакцій на виявлену атаку

Мало виявити атаку, – необхідно на неї відповідним чином відреагувати. Саме варіанти реагування багато в чому визначають ефективність системи виявлення атак. На сьогоднішній день пропонуються наступні варіанти реагування:

Повідомлення на консоль (включаючи резервну) системи виявлення атак або на консоль інтегрованої системи (наприклад, міжмережного екрана).

Звукове оповіщення про атаку.

– генерація керуючих послідовностей SNMP для систем мережного керування;

– генерація повідомлення про атаку по електронній пошті.

Додаткові повідомлення на мобільний пристрій або факс. Дуже цікава, хоча й рідко застосовувана можливість. Оповіщення про виявлення несанкціонованої діяльності посилає не адміністраторові, а зловмисникові. На думку прихильників даного варіанта реагування, порушник, довідавшись, що його виявили, змушений припинити свої дії.

Обов'язкова реєстрація подій, що виявляються. Як журнал реєстрації можуть виступати:

– текстовий файл;

– системний журнал (наприклад, у системі Cisco Secure Integrated Software);

– текстовий файл спеціального формату (наприклад, у системі Snort;

– локальна база даних MS Access;

– SQL-база даних (наприклад, у системі RealSecure).

Треба тільки враховувати, що обсяги інформації, що реєструється вимагають, як правило, SQL-базу – MS SQL або Oracle.

Трасування подій (event trace), тобто запис їх у тій послідовності й з тією швидкістю, з якими їх реалізовував зловмисник. Потім

адміністратор у будь-який заданий час може прокрутити (replay або playback) необхідну послідовність подій із заданою швидкістю (у реальному режимі часу, із прискоренням), щоб проаналізувати діяльність зловмисника. Це дозволить зрозуміти його кваліфікацію, використовувані засоби атаки й т.д.

Переривання дій атакуючого, тобто завершення з'єднання. Це можна зробити, як:

– перехоплення з'єднання (session hijacking) і посилання пакета із установленим прапором RST обом учасникам мережного з'єднання від імені кожного з них (у системі виявлення атак, що функціонує на рівні мережі);

– блокування облікового запису користувача, що здійснює атаку (у системі виявлення атак на рівні вузла). Таке блокування може бути здійснено або на заданий проміжок часу, або доти, поки обліковий запис не буде розблокована адміністратором. Залежно від привілеїв, з якими запущена система виявлення атак, блокування може діяти як у межах самого комп'ютера, на який спрямована атака, так і в межах усього домену мережі.

Реконфігурація мережного встаткування або міжмережевих екранів. У випадку виявлення атаки на маршрутизатор або міжмережевий екран посилається команда на зміну списку контролю доступу. Згодом всі спроби з'єднання з атакуючого вузла будуть відкидатися. Як і блокування облікового запису зловмисника, зміна списку контролю доступу може бути здійснено або на заданий інтервал часу або до того моменту, як зміна буде скасовано адміністратором реконфігуруємого мережного встаткування.

Блокування мережевого трафіку так, як це реалізовано в міжмережевих екранах. Цей варіант дозволяє обмежити трафік, а також адресатів, які можуть одержати доступ до ресурсів комп'ютера, що захищається, дозволяючи виконувати функції доступні в персональних міжмережевих екранах.

РОЗДІЛ 2. МІЖМЕРЕЖЕВІ ЕКРАНИ (ФАЄРВОЛИ, БРАНДМАУЕРИ)

В основу забезпечення безпеки локальних мереж і розміщених у них інформаційних систем повинні бути покладені наступні основні принципи:

– Забезпечення інформаційної безпеки вимагає комплексного й цілісного підходу. Інформаційна безпека повинна бути невід'ємною частиною систем керування в організації. Велике значення для забезпечення безпеки інформаційної системи мають соціальні фактори, а також міри адміністративної, організаційної й фізичної безпеки.

– Інформаційна безпека повинна бути економічно виправданою.

– Відповідальність за забезпечення безпеки повинна бути чітко визначена.

– Безпека інформаційної системи повинна періодично аналізуватися й переоцінюватися.

Припустимо, що локальна мережа має чіткі границі, тобто про будь-який хост можна сказати, чи перебуває він у локальній мережі чи ні. Ці границі будемо називати мережним периметром. Також будемо припускати, що існують явні точки входу в локальну мережу.

Основним завданням міжмережевого екрана є запобігання небажаного доступу в локальну мережу. Прикладом небажаного доступу є порушник, що намагається здійснити незаконне проникнення в системи, доступні по мережі. Він може просто одержувати задоволення від злому, а може намагатися ушкодити інформаційну систему або впровадити в неї що-небудь для своїх цілей. Наприклад, метою хакера може бути одержання номерів кредитних карток, що зберігаються в системі. Іншим прикладом небажаного доступу є розміщення в обчислювальній системі чого-небудь,

що впливає на прикладні програми й сервіси, які обчислювальна система надає своїм користувачам.

Атакуючий, бажаючий одержати доступ у локальну мережу або до інформаційних систем, може переслідувати наступні цілі:

– одержати доступ до інформації з метою читання або модифікації даних, що зберігаються в системі;

– здійснити атаки на сервіси, щоб перешкодити використовувати їх або змінити їхнє функціонування.

Розглянемо технології запобігання небажаного доступу в локальну мережу й до інформаційних систем.

Сервіси безпеки, які запобігають небажаний доступ, можна розбити на дві категорії:

– ***Перша категорія*** складається із процедур входу, заснованих на використанні різного роду автентифікаторів (паролів, апаратних ключів, сертифікатів і т.п.). Це дозволяє здійснити доступ тільки законним користувачам. До цієї категорії відносяться також різні міжмережеві екрани (firewall), які запобігають атакам, що засновані на використанні уразливостей на різних рівнях стека протоколів TCP/IP.

– ***Друга категорія*** складається з різних моніторів, що аналізують доступ і діяльність користувачів.

Міжмережеві екрани захищають комп'ютери й мережі від спроб несанкціонованого доступу з використанням вразливих місць, що існують у сімействі протоколів TCP/IP. Додатково вони допомагають вирішувати проблеми безпеки, пов'язані з наявністю уразливостей в іншому ПЗ, що установлено на комп'ютерах у мережі.

Міжмережеві екрани є апаратно-програмними пристроями або програмами, які регулюють потік мережного трафіку між мережами або хостами, що мають різні вимоги до безпеки. Більшість міжмережевих екранів розташовано на границі мережевого периметра, і в першу чергу вони призначені для захисту внутрішніх хостів від зовнішніх атак.

Однак атаки можуть також починатися й з хостів, розташованих у локальній мережі, при цьому вони можуть не проходити через міжмережеві екрани на границі мережевого периметра. Тому в цей час міжмережеві екрани розміщають не тільки на границі мережевого периметра, але й між різними сегментами мережі. Це забезпечує додатковий рівень безпеки.

Міжмережеві екрани пропускають або забороняють трафік, порівнюючи його характеристики із шаблонами, заданими в політиці міжмережевого екрана.

Можливості фільтрування, виконуваного міжмережевими екранами, з початку 90-х років істотно збільшилися. Найчастіше можливості міжмережевих екранів порівнюють по кількості рівнів у стеці TCP/IP, які вони можуть аналізувати.

Крім цього міжмережеві екрани можна порівнювати по можливостям спільного функціонування з іншими інструментальними засобами, такими як системи виявлення проникнень і сканери вмісту e-mail або веб з метою знаходження вірусів або небезпечного прикладного коду. Використання винятково тільки міжмережевих екранів не забезпечує повного захисту від всіх проблем, породжених Інтернетом. Як результат, міжмережеві екрани є тільки однією з частин архітектури інформаційної безпеки.

Існує кілька технологій міжмережевих екранів, які відрізняються можливостями аналізу мережевого трафіку. Розуміння можливостей кожного типу міжмережевого екрана, розробка політики міжмережевого екрана й використання технологій міжмережевих екранів, які необхідні в кожному конкретному випадку, важливо для надійного захисту локальних мереж і хостів.

Для забезпечення максимально ефективної роботи міжмережевих екранів варто дотримуватися наступних принципів:

– Визначити всі вимоги, які накладає зовнішнє оточення на функціонування міжмережевого екрана. Необхідно визначити топологію мережі, яка захищається, використовувані транспортні протоколи (IPv4 або IPv6) і специфіку сервісів, що захищаються, й типи технологій міжмережевих екранів, які найбільш ефективні в цьому випадку. Також варто пам'ятати про продуктивність і про інтеграцію міжмережевого екрана в існуючу мережеву інфраструктуру й інфраструктуру безпеки. Необхідно враховувати вимоги до фізичного оточення й до кваліфікації персоналу, а також вимоги, які можуть виникнути надалі, такі як перехід на технології IPv6 або впровадження VPN.

– Створити політику міжмережевого екрана, у якій визначено, як варто обробляти вхідний і вихідний трафік. Необхідно виконати аналіз ризиків і визначити при яких умовах якому типу трафіку дозволено проходити через міжмережевий екран. Звичайно весь вхідний і вихідний трафік, що явно не дозволений політикою міжмережевого екрана, повинен бути заборонений. Це знижує ризик атак і може зменшити обсяг трафіку в мережі. У політиці повинно бути визначено, як міжмережевий екран обробляє вхідний і вихідний трафік для конкретних IP-адрес, діапазонів адрес, протоколів, застосунків і типів умісту.

– Розробити набір правил міжмережевого екрана, які реалізують політику безпеки в організації й забезпечують максимальну продуктивність міжмережевого екрана. Проаналізувати продуктивність міжмережевого екрана. Набір політик безпек повинен максимально ефективно обробляти трафік. При створенні набору правил варто визначити типи дозволеного трафіку, включаючи протоколи, які необхідні для керування самим міжмережевим екраном. Деталі створення набору правил залежать від типу міжмережевого екрана й конкретного виробника, але часто продуктивність міжмережевого екрана залежить від оптимізації

набору правил. Наприклад, більшість міжмережевих екранів послідовно порівнюють трафік із правилами доти, поки не буде знайдена відповідність. Для таких міжмережевих екранів правила, які найчастіше будуть відповідати шаблонам трафіку, повинні бути розміщені вгорі списку.

– Управляти архітектурою, політиками, ПЗ й іншими компонентами міжмережевого екрана треба протягом усього часу його функціонування. Існує багато аспектів, що стосується керування міжмережевим екраном. Наприклад, вибір одного або декількох типів міжмережевих екранів і їхнє розташування в мережі може істотно впливати на політику безпеки, що зможуть реалізовувати ці міжмережеві екрани. При зміні вимог в організації може знадобитися змінити набір правил, щоб у мережі могли функціонувати нові додатки або хости. Необхідно також стежити за продуктивністю компонентів міжмережевого екрана, щоб потенційні проблеми з ресурсами були вчасно визначені. Також повинні постійно проглядатися логи й оповіщення для визначення загроз, як здійснених, так і не здійснених.

Технології міжмережевих екранів

Стек протоколів

Міжмережні екрани є апаратно-програмними пристроями або програмами, що управляють потоком мережного трафіку між мережами або хостами, які мають різні вимоги до безпеки. Міжмережеві екрани найчастіше використовуються при підключенні мережі до Інтернету, але вони можуть застосовуватися й для розмежування трафіку усередині однієї організації. Наприклад, можна встановити міжмережевий екран, щоб обмежити з'єднання із внутрішньою підмережею, у якій обробляються конфіденційні дані.

Класичною моделлю, що описує принципи мережевої взаємодії, є модель OSI (Open Systems Interconnection). Дана модель описує мережеву взаємодію як набір вкладених один в одного рівнів. Дані протоколів більш

високого рівня розташовані в тілі протоколів більше низького рівня. Кожний рівень виконує певні функції, для яких розроблені спеціальні протоколи.

Таблиця 2.1 – Модель OSI

Рівень 7	Прикладний рівень
Рівень 6	Представницький рівень
Рівень 5	Сеансовий рівень
Рівень 4	Транспортний рівень
Рівень 3	Мережний рівень
Рівень 2	Канальний рівень
Рівень 1	Фізичний рівень

Таблиця 2.2 – Стек протоколів TCP/IP складається із чотирьох рівнів

Рівень стека протоколів	Приклади протоколів
Прикладний рівень	Забезпечує взаємодюя користувальницьких застосунків з мережею. Протоколи: HTTP, FTP, TFTP. DNS, SMTP, Telnet, SNMP і т.п.
Транспортний рівень	Забезпечує передачу даних і корекцію помилок. Протоколи: TCP, UDP і т.п.
Мережний рівень	Виконує адресацію й маршрутизацію. Протоколи: IP, OSPF, ICMP, IGMP і т.п.
Канальний рівень	Упаковує дані в стандартні кадри для передачі через фізичний рівень і забезпечує перевірку й корекцію помилок. Протоколи: Ethernet, PPP і т.п. На цьому рівні працює ARP.

Канальний рівень (також називаний Data Link рівень) забезпечує взаємодію компонентів фізичної мережі. Канальний рівень являє собою реальну апаратуру фізичного з'єднання й фізичне середовище, таку як Ethernet. Це рівень, що зазвичай називається локальною мережею або LAN. Це перший рівень, що володіє можливістю адресації, за допомогою якої можна ідентифікувати окремий хост. Адреси призначаються на мережні інтерфейси й називаються MAC (Media Access Control) адресами. Ethernet-адреса, що належить Ethernet-карті, являє приклад MAC-адреси. Міжмережеві екрани рідко мають справу з даними на цьому рівні. Блок даних, переданий на канальному рівні, називають кадром.

Мережний рівень (також називаний IP-рівнем) маршрутизує пакети між локальними мережами. IPv4 і є основним протоколом мережного рівня для TCP/IP. Іншими, часто використовуваними протоколами мережного рівня є IPv6 і IGMP. Даний рівень відповідає за доставку пакетів між окремими локальними мережами, з'єднаними маршрутизаторами. Такі мережі часто позначаються WAN (Wide Area Network). Адреси даного рівня називаються IP-адресами; вони звичайно є унікальними, але при певних обставинах, наприклад, при трансляції мережевих адрес (Network Address Translation – NAT), можливі ситуації, коли різні фізичні системи мають ту саму IP-адресу. Блок даних, переданих по мережному рівню, називають дейтаграмою.

Транспортний рівень надає сервіси, орієнтовані на з'єднання, які використовуються для передачі даних між мережами. Частина протоколів (а саме TCP) можуть гарантувати надійність з'єднання. Прикладами протоколів транспортного рівня є TCP і UDP. На транспортному рівні виникає поняття сесії як потоку даних між двома додатками. Для сесії визначене поняття портів, які є кінцевими точками сесії: номер порту джерела визначає кінцеву точку комунікаційної сесії на вихідній системі; номер порту призначення визначає кінцеву точку комунікаційної сесії на

системі призначення. Хост може мати з іншими хостами практично будь-яке число сесій на транспортному рівні.

Прикладний рівень посилає й одержує дані конкретних застосунків, таких як DNS, HTTP, SMTP. Прикладний рівень сам може складатися з декількох підрівнів. Наприклад, SMTP або HTTP можуть інкапсулювати інші формати, такі як HTML.

Міжмережеві екрани аналізують дані одного або декількох рівнів. Вважається, що чим більше рівнів аналізує міжмережевий екран, тим більше розвиненим і ефективним він є. Чим більше число рівнів може бути проаналізовано, тим більше точна й ретельна перевірка може бути виконана. Міжмережеві екрани, які розуміють прикладний рівень, потенційно можуть аналізувати уразливості на рівні застосунку й надавати сервіси, орієнтовані на кінцевого користувача, наприклад, виконувати автентифікацію користувача й записувати в логи події, що стосуються конкретного користувача.

Сучасні міжмережеві екрани функціонують на кожному з перерахованих рівнів. Існує кілька типів технологій міжмережевих екранів. Одним зі способів порівняння можливостей міжмережевих екранів є аналіз рівнів стека протоколів TCP/IP, які аналізують міжмережвий екран.

Незалежно від архітектури, міжмережевий екран може надавати додаткові сервіси. Ці сервіси включають трансляцію мережних адрес (NAT), підтримку протоколу динамічної конфігурації хосту (DHCP), функції шифрування, тим самим будучи кінцевою точкою VPN-шлюзу.

Багато міжмережевих екранів також включають різні технології фільтрації, так званого активного вмісту. Вміст називається активним, так як він є кодом, що може бути виконаний на кінцевій системі. Наприклад, при використанні таких технологій може бути виконане сканування файлів на наявність вірусів. Міжмережеві екрани також застосовуються для фільтрації найнебезпечнішого активного вмісту, такого як Java, JavaScript і ActiveX. Або вони можуть бути використані для фільтрації вмісту, що

відповідає певному зразку, або пошуку ключових слів з метою обмеження доступу до заборонених сайтів або доменам.

Стани TCP-з'єднання

IP-протокол забезпечує спосіб адресації джерела й одержувача. IP-протокол також має справу з фрагментацією й реассемблюванням пакетів, які потім передаються на транспортний рівень.

TCP є надійним протоколом у мережах, заснований на комутації пакетів, забезпечуючи гарантовану доставку пакетів. Так як пакетні фільтри аналізують параметри TCP-протоколу, розглянемо докладно цей протокол.

Кожний октет даних, переданий по з'єднанню, має послідовний номер. У пакеті вказується номер першого переданого октету. Пакет також містить номер октету, що був отриманий відправником даного пакета. При відправленні пакет на стороні відправника не відкидається, а розміщується в чергу для можливої повторної передачі, якщо протягом певного часу не буде отримане підтвердження від протилежної сторони про одержання даного пакета. Якщо підтвердження не отримане при закінченні цього часу, пакет передається повторно. Тим самим забезпечується надійність з'єднання, тобто гарантування того, що всі пакети будуть доставлені одержувачу.

Для ідентифікації початкової й кінцевої точок TCP-з'єднання вводиться поняття номера порту. Номера портів вибираються незалежно для кожного TCP-з'єднання, при цьому вони не обов'язково повинні бути унікальними. Пари (IP-адреса, порт) називаються сокетом.

Кожний кінець TCP-з'єднання є або клієнтом, або сервером. З'єднання ініціюється клієнтом. Сервер чекає встановлення з'єднання від клієнта, у цьому випадку говорять, що сервер слухає порт. TCP-з'єднання може бути відкрито або в пасивному – сервером, або в активному режимі – клієнтом.

Сервер може використовувати будь-які номери портів. Проте визначені деякі базові принципи призначення номерів портів. Існують "добре відомі" номери портів, які звичайно відповідають певним додаткам. При ініціалізації TCP-сесії на стороні клієнта відкривається порт, номер якого у відповідності зі специфікацією протоколу TCP повинен бути в діапазоні від 1023 до 65535. Номер порту на стороні клієнта може бути щораз різним.

Застосунок, що хоче надавати сервіс, доступний по мережі іншим додаткам, відкриває порт у пасивному режимі. Для одержання сервісу застосунок, названий клієнтом, повинен відкрити порт в активному режимі й ініціювати створення з'єднання із сервером.

Установлення TCP-з'єднання відбувається з використанням так званого "потрійного рукостискання". З'єднання ініціює клієнт, посилаючи пакет із установленим бітом SYN. Сервер відповідає клієнтові пакетом із установленими бітами SYN і ACK. Сервер також передає початковий порядковий номер у поле Sequence Number. Нарешті, клієнт посилає серверу повідомлення із установленим бітом ACK, у поле Sequence Number вказує свій початковий номер, у поле Acknowledgement Number вказує отриманий від сервера початковий порядковий номер, збільшений на одиницю.

Протягом свого життєвого циклу з'єднання проходить через кілька станів.

Стани на стороні клієнта:

– CLOSED;

– SYN-SENT;

– ESTABLISHED;

– FIN-WAIT-1;

– CLOSE-WAIT;

– FIN-WAIT-2;

– CLOSING;

– LAST-ACK;

– CLOSED;

Стани на стороні сервера:

– CLOSED;

– LISTEN;

– SYN-RESEIVED;

– ESTABLISHED;

– FIN-WAIT-1;

– CLOSE-WAIT;

– FIN-WAIT-2;

– CLOSING;

– TIME-WAIT;

– CLOSED.

Стан CLOSED є фіктивним, так як він являє собою стан, для якого не існує структур даних на стороні клієнта й сервера, а, отже, не може існувати з'єднання.

LISTEN – стан сервера, у якому він очікує запит від клієнта на створення з'єднання.

SYN-SENT – стан клієнта, у якому він очікує відповіді від сервера після посилки запиту на створення з'єднання.

SYN-RECEIVED – стан сервера, у якому він очікує підтвердження після того, як і клієнт, і сервер одержали й надіслали запит на створення з'єднання.

ESTABLISHED – стан як клієнта, так і сервера, що являє собою відкрите з'єднання: отримані дані доставляються на прикладний рівень. Звичайний стан при пересиланні даних по з'єднанню.

Ініціатором закриття з'єднання може бути як клієнт, так і сервер.

FIN-WAIT-1 – стан ініціатора закриття з'єднання, при якому даною стороною був посланий пакет із прапором FIN. Ініціатор закриття з'єднання очікує підтвердження на запит закриття.

CLOSE-WAIT – стан сторони, що відповідає, закриття з'єднання, при якому було послане підтвердження ACK на запит закриття (FIN). При цьому канал стає симплексним: передача можлива тільки в одному напрямку – від сторони, що відповідає, закриттю з'єднання, тобто від того, хто послав підтвердження ACK.

FIN-WAIT-2 – стан ініціатора закриття з'єднання, при якому було отримане підтвердження ACK запиту закриття з'єднання від віддаленої сторони. Після цього дана сторона чекає одержання пакета з установленим прапором FIN. При одержанні пакета із прапором FIN канал вважається остаточно зруйнованим.

LAST-ACK – стан сторони, що відповідає, закриття з'єднання, при якому послане підтвердження (пакет із установленим прапором FIN) завершення з'єднання, раніше посланого віддаленій стороні.

CLOSING – обидві сторони ініціювали закриття з'єднання одночасно: після відправлення пакета із прапором FIN ініціатор закриття одержує пакет із прапором FIN.

TIME-WAIT – являє собою очікування протягом певного часу, щоб бути впевненим, що віддалена сторона одержала підтвердження запиту на закриття з'єднання.

TCP-з'єднання переходить із одного стану в інше в результаті виникнення подій. Подіями є виклики функцій OPEN, SEND, RECEIVE, CLOSE, ABORT і STATUS, що входять пакети, які містять прапори SYN, ACK, RST і FIN, а також таймаути.

Класифікація міжмережевих екранів

Міжмережеве екранування часто сполучають із іншими технологіями, найчастіше з маршрутизацією. Багато технологій, зв'язуються часто з міжмережевими екранами, насправді є частиною інших технологій. Наприклад, трансляцію мережевих адрес (NAT) часто вважають технологією міжмережевих екранів, але насправді це є технологією маршрутизації. Багато які міжмережеві екрани також

включають можливості фільтрування вмісту, необхідні для реалізації політики, прийнятої в організації, що необов'язково пов'язана з безпекою. Деякі міжмережеві екрани надають технології систем виявлення вторгнень (IDS), які можуть реагувати на атаки.

Міжмережеві екрани часто розташовані на границі мережевого периметра. У цьому випадку можна говорити, що міжмережевий екран має зовнішній і внутрішній інтерфейси. Іноді ці інтерфейси називають відповідно незахищеним і захищеним. Однак говорити, що якийсь інтерфейс є захищеним, а якийсь ні, не зовсім коректно, так як політика міжмережевого екрана може бути визначена в обох напрямках. Наприклад, можна визначити політику, що запобігає пересиланню файлів певного типу зсередини зовні мережевого периметра.

Фільтрування пакетів

Базовою можливістю міжмережевого екрана є фільтрування пакетів. Спочатку міжмережеві екрани були частиною маршрутизаторів, забезпечуючи керування доступом на основі адрес хостів і комунікаційних сесій. Ці пристрої, також так звані міжмережевими екранами без аналізу стану, не підтримували інформацію про стан потоку трафіку, що проходить через міжмережевий екран. Це означає, що вони не можуть визначити, що кілька запитів належать одній сесії. Фільтрування пакетів є основою більшості сучасних міжмережевих екранів, хоча залишилося небагато пакетних фільтрів, які виконують фільтрування без підтримки стану. На відміну від могутніших фільтрів, пакетні фільтри аналізують тільки заголовки мережевого й транспортного рівнів, а не вміст пакетів. Керування трафіком визначається набором директив, які називаються ruleset. Можливості фільтрування пакетів вбудовані в більшість ОС і пристроїв, що виконують маршрутизацію. Самим типовим прикладом є маршрутизатор, у якому визначені списки керування доступом.

Керування трафіком здійснюється на основі аналізу наступної інформації, що утримується в пакеті:

– IP-адреса джерела в пакеті – адреса хосту, з якого прийшов пакет.

– IP-адреса одержувача в пакеті – адреса хосту, якому призначений пакет.

– Транспортний протокол, що використовується для взаємодії хостів відправника й одержувача, такий як TCP, UDP або ICMP.

– Можливо деякі характеристики комунікаційної сесії транспортного рівня, такі як порти джерела й одержувача (наприклад, TCP 80 для порту одержувача й TCP 1320 для порту джерела).

– Інтерфейс, через який проходить пакет, і напрямок (вхідний або вихідний).

Фільтрування вхідного трафіку ще називають вхідним фільтруванням. Вихідний трафік також може фільтруватися, цей процес називається вихідним фільтруванням. Вихідне фільтрування дає можливість обмежити внутрішній трафік, наприклад, блокуючи використання зовнішніх FTP-серверів або запобігаючи атаки, які можуть запускатися зсередини на зовнішні цілі.

Фільтри пакетів без підтримки стану вразливі для атак, пов'язаних з особливостями TCP/IP. Наприклад, багато таких пакетних фільтрів не можуть визначити, що інформація в мережній адресі підроблена або якимось чином змінена, або що є присутня комбінація параметрів, дозволена стандартами, але яка використовує уразливості в конкретному застосунку або ОС. Атаки підробки, такі як використання некоректних адрес у заголовках пакетів, можуть дати можливість атакуючій обійти контроль, виконуваний міжмережевим екраном. Міжмережеві екрани, які виконуються на більше високих рівнях, можуть перешкоджати деяким атакам, пов'язаним з підробкою адрес, перевіряючи, що сесія встановлена, або автентифікуючи користувачів перед тим, як дозволити проходження трафіку. У силу цього більшість міжмережевих екранів, які реалізують

фільтрацію пакетів, також підтримують деяку інформацію про стан для пакетів, що проходять через міжмережевий екран.

У деяких випадках корисно фільтрувати фрагментовані пакети. Фрагментація пакетів допускається специфікаціями TCP/IP і в деяких ситуаціях буває необхідна. Однак фрагментація пакетів робить визначення деяких атак більше важкоими, так як атака розміщається у фрагментованих пакетах. Наприклад, деякі мережні атаки використовують пакети, які в нормальних ситуаціях не можуть з'явитися, скажімо, посилаючи певні фрагменти пакета, але не посилаючи перший фрагмент, або посилаючи фрагменти пакета, які перекривають один одного. Щоб запобігти використанню фрагментованих пакетів для виконання атак, міжмережевий екран можна зконфігурувати таким чином, щоб блокувати фрагментовані пакети.

У даний момент фрагментовані пакети часто з'являються не тому, що є атакою, а внаслідок використання технологій VPN, які інкапсулюють пакети всередину інших пакетів. Якщо інкапсуляція пакета призводить до того, що новий пакет перевищує максимально допустимий розмір, пакет буде фрагментований. Фрагментовані пакети, які блокуються міжмережевими екранами, є типовою проблемою, пов'язаної з використанням VPN.

Деякі міжмережеві екрани можуть дефрагментувати пакети перед тим, як пересилати їх у внутрішню мережу. Варто розуміти, що це вимагає додаткових ресурсів самого міжмережевого екрана, особливо пам'яті. Така функціональність повинна використовуватися дуже обґрунтовано, інакше міжмережевий екран легко може стати об'єктом DoS-атаки. Вибір того, що робити із фрагментованим пакетом: відкинути, реассемблювати або пропустити, повинен бути компромісом між необхідної інтероперабельністю й повною безпекою мережі.

Пакетні фільтри можуть бути реалізовані в наступних компонентах мережної інфраструктури:

– прикордонні маршрутизатори;

– операційні системи;

– персональні міжмережеві екрани.

Основною перевагою пакетних фільтрів є їхня швидкість. Так як пакетні фільтри зазвичай перевіряють дані тільки в заголовках мережного й транспортного рівнів, вони можуть виконувати це дуже швидко. Із цих причин пакетні фільтри, вбудовані в прикордонні маршрутизатори, ідеальні для розміщення на границі з мережею з невисоким ступенем довіри. Пакетні фільтри, вбудовані в прикордонні маршрутизатори, можуть блокувати основні атаки, фільтруючи небажані протоколи, виконуючи найпростіший контроль доступу на рівні сесій і потім передаючи трафік іншим міжмережевим екранам для перевірки даних на більш високих рівнях стека протоколів.

На рисунку 2.1 показана топологія мережі, в якій прикордонний маршрутизатор з можливостями пакетного фільтра використовується як перша лінія оборони. Маршрутизатор приймає пакети від сумнівної мережі, наприклад, Інтернет, виконує контроль доступу у відповідності зі своєю політикою, наприклад, блокує SNMP, дозволяє HTTP і т.п. Потім він передає пакети могутнішому міжмережевому екрану для подальшого керування доступом і фільтрування даних на більш високих рівнях стека протоколів. На рисунку також показана проміжна мережа між прикордонним маршрутизатором і внутрішнім міжмережевим екраном, що називається DMZ-мережею.

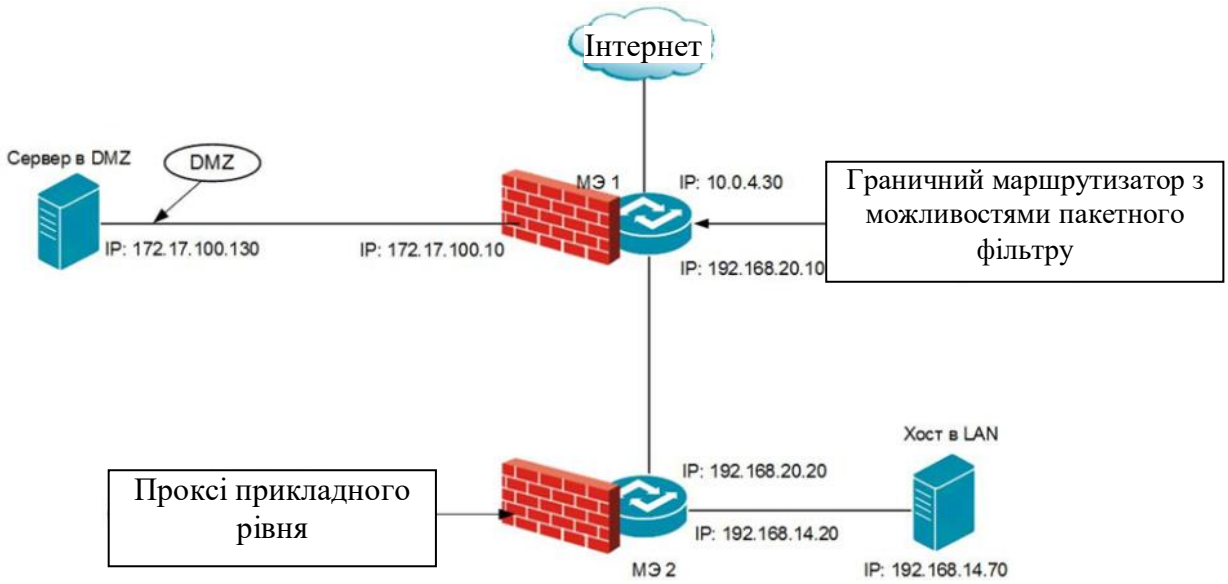

Рисунок 2.1 – Приклад топології мережі з використанням пакетного фільтра й DMZ

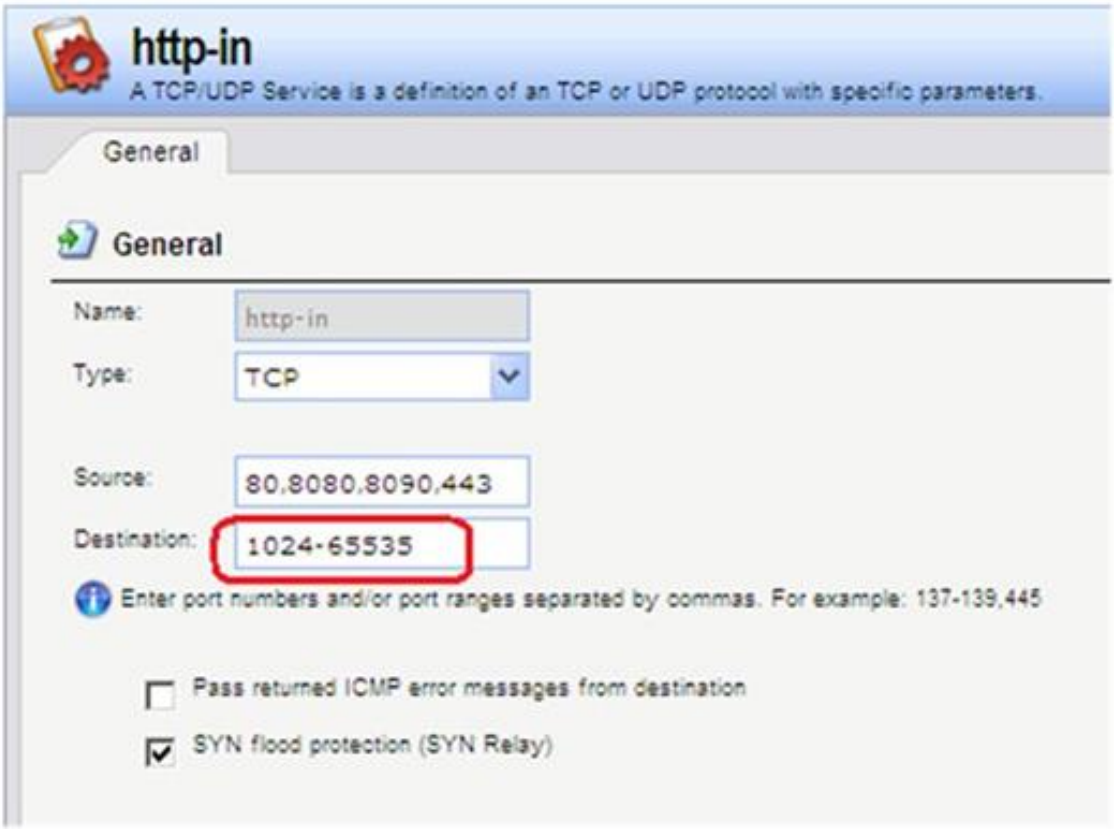

Рисунок 2.2 – Необхідність відкривати порти з «великими» номерами на стороні клієнта

Порт на стороні сервера має фіксований номер. На стороні клієнта відкривається порт, номер якого може бути щораз різним.

Рисунок 2.3 – Набір правил пакетного фільтра стану без аналізу

У цьому випадку пакетний фільтр повинен дозволяти вхідний трафік для всіх таких портів "з великими номерами", щоб клієнт, який ініціалізував з'єднання, міг одержувати пакети, що повертаються сервером. Відкриття портів створює ризик несанкціонованого проникнення в локальну мережу.

Переваги пакетних фільтрів:

Основною перевагою пакетних фільтрів є їхня швидкість.

Пакетний фільтр прозорий для клієнтів і серверів, так як не розриває TCP-з'єднання.

Недоліки пакетних фільтрів:

– Так як пакетні фільтри не аналізують дані більше високих рівнів, вони не можуть запобігти атакам, які використовують уразливості, специфічні для застосунку. Наприклад, пакетний фільтр не може блокувати конкретні команди застосунку; якщо пакетний фільтр дозволяє даний трафік для застосунку, то всі операції в даному застосунку, будуть дозволені.

– У логах пакетного фільтра втримується інформація тільки про параметри мережевого й транспортного рівнів. Логи пакетного фільтра звичайно містять ту ж інформацію, що використовувалася при ухваленні рішення про можливість доступу (адреса джерела, адреса призначення, тип трафіку й т.п.).

– Більшість пакетних фільтрів не підтримують можливість автенифікації користувача. Дана можливість забезпечується міжмережевими екранами, що аналізують більш високі рівні.

– Пакетні фільтри звичайно вразливі для атак, які використовують такі уразливості TCP/IP, як підробка (spoofing) мережної адреси. Багато пакетних фільтрів не можуть визначити, що в мережному пакеті змінена адресна інформація транспортного рівня. Spoofing-атаки звичайно виконуються для обходу керування доступом, здійснюваного міжмережевим екраном.

– Пакетні фільтри важко конфігурувати. Можна випадково переконфігурувати пакетний фільтр для дозволу типів трафіку, джерел і призначень, які повинні бути заборонені.

– Так як номер порту клієнта може бути будь-яким, так званим "більшим номером" (з 1023 до 65535), то на міжмережевому екрані доводиться відкривати всі порти з номерами більше 1022.

Отже, пакетні фільтри найбільше підходять, якщо потрібно більша пропускна здатність, а створення докладних балок і автенифікація користувача не настільки важливі.

Практично всі сучасні міжмережеві екрани включають більшу кількість можливостей, зараз важко знайти міжмережевий екран, що має можливості тільки пакетного фільтру. Прикладом може бути маршрутизатор, що здійснює перевірку списку контролю доступу для керування мережевим трафіком. Висока продуктивність пакетних фільтрів також сприяє тому, що вони реалізуються в пристроях, що забезпечують високу доступність і особливу надійність; деякі виробники пропонують

апаратні й програмні рішення як високо доступні, так і особливо надійні. Також більшість SOHO (Small Office Home Office) пристроїв міжмережевих екранів і міжмережевих екранів, вбудованих за замовчуванням в ОС, надають можливості пакетних фільтрів.

Пакетні фільтри з аналізом стану

Аналіз стану додає можливість відстеження стану з'єднання й блокування пакетів, які не відповідають очікуваному стану. Для цього виконується аналіз даних транспортного рівня. Також як і при простому фільтруванні пакетів міжмережевий екран аналізує вміст мережевого рівня на відповідність правилам. Але на відміну від фільтрації пакетів, інспекція стану відслідковує історію кожного з'єднання, використовуючи для цього таблицю станів. Хоча деталі записів таблиці станів багато в чому залежать від конкретної реалізації міжмережевого екрана, звичайно вони містять IP-адресу джерела, IP-адресу одержувача й інформацію про стан з'єднання.

У TCP-протоколі існують три основні стани – з'єднання: встановлюється, використовується й завершується.

Причому в останньому випадку кожна з кінцевих точок може запросити завершення з'єднання. При аналізі стану міжмережевий екран перевіряє певні значення в TCP-заголовках. Для кожного отриманого пакета шукається запис у таблиці станів і визначається, що прапори в заголовках пакета відповідають очікуваному стану. Наприклад, той хто атакує може створити пакет, у заголовку якого зазначено, що він є частиною встановленого з'єднання, у надії, що він пройде через міжмережевий екран. Якщо міжмережевий екран використовує аналіз станів, то він зрозуміє, що пакет не є частиною встановленого з'єднання, так як в таблиці відсутній відповідний запис, і відкине такий пакет.

У найпростішому випадку міжмережевий екран пропускає будь-який пакет, якщо він вважає, що пакет є частиною відкритого з'єднання (або з'єднання, що ще не повністю встановлене). Хоча багато міжмережевих екранів точно можуть визначити стан таких протоколів, як

TCP і UDP, і вони можуть блокувати пакети, які не відповідають стану протоколу. Наприклад, часто міжмережевий екран перевіряє такі параметри, як послідовні номери TCP, і відкидає пакети, номери яких поза очікуваним діапазоном. Якщо міжмережевий екран надає сервіс NAT, то інформація NAT часто також утримується в таблиці станів.

Нижче наведений приклад таблиці станів. Якщо хост із внутрішньої мережі намагається з'єднатися з хостом за міжмережевим екраном, то першою справою перевіряться, чи дозволено це набором правил міжмережевого екрана. Якщо це дозволено, то в таблицю станів додається запис, що вказує без аналізу ініціалізується нове з'єднання. Після завершення трикрокового рукостискання TCP стан з'єднання буде змінено на "Встановлене" ("Establish" або "TCP_OPEN", залежно від реалізації), і всьому наступному трафіку, що відповідає даному запису, буде дозволено проходити через міжмережевий екран.

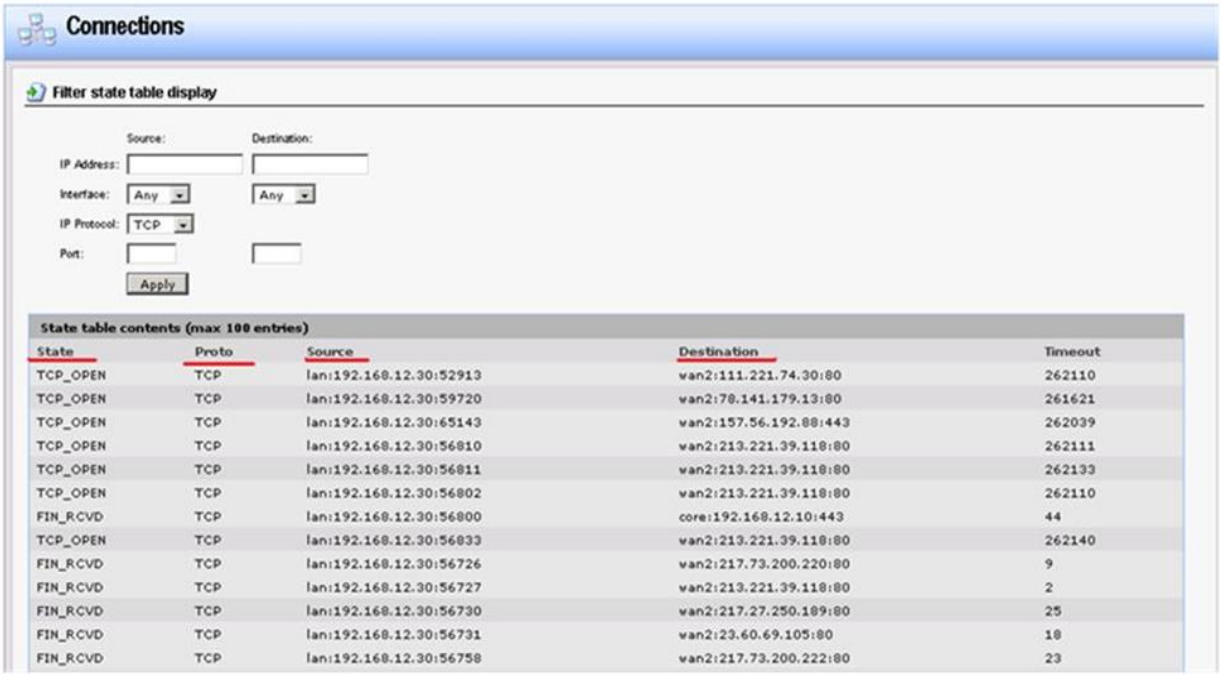

Рисунок 2.4 – Приклад таблиці станів пакетного фільтра з аналізом станів

Так як деякі протоколи, зокрема UDP, не підтримують стани, і для них не існує ініціалізації, встановлення й завершення з'єднання, то для них неможливо визначити стан на транспортному рівні як для TCP. Для цих протоколів міжмережеві екрани з підтримкою стану мають можливість тільки відслідковувати IP-адреси й порти джерела й одержувача. Так наприклад відповідь DNS від зовнішнього джерела буде пропускатися тільки в тому випадку, якщо міжмережевий екран до цього бачив відповідний DNS-запит від внутрішнього хосту. Так як міжмережевий екран не має можливості визначити завершення сесії, запис видаляється з таблиці станів після заздалегідь зконфігурованого таймаута. Міжмережеві екрани прикладного рівня, які вміють розпізнавати DNS поверх UDP, завершують сесію після того, як отриманий DNS-відповідь.

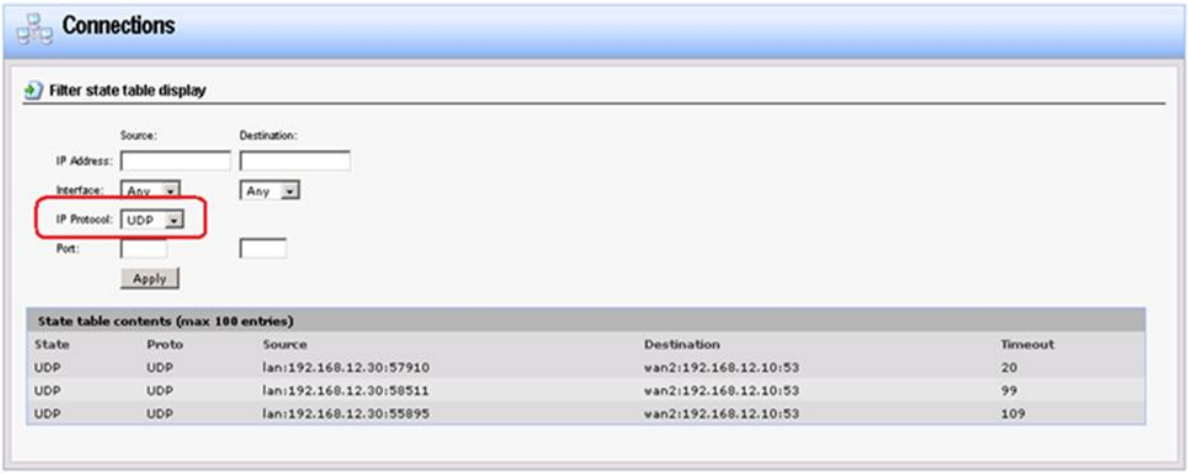

Рисунок 2.5 – Приклад таблиці станів для протоколу UDP

За суттю, міжмережеві екрани з аналізом стану додають у пакетний фільтр розуміння логіки протоколу транспортного рівня. Міжмережеві екрани з аналізом стану розділяють сильні й слабкі сторони пакетних фільтрів, але все-таки міжмережеві екрани з аналізом стану звичайно вважаються більш безпечними, ніж пакетні фільтри.

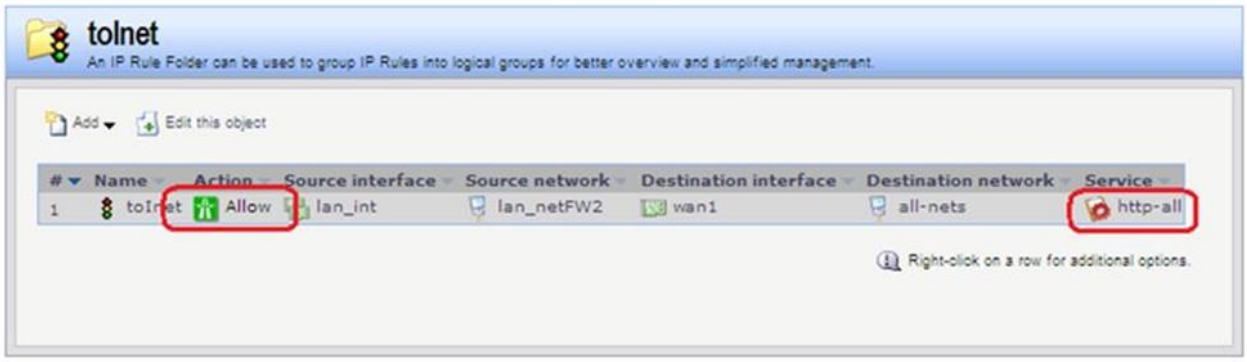

Рисунок 2.6 – Правила пакетного фільтра з аналізом станів

Переваги міжмережевих екранів з аналізом стану:

– дозволяють проходження пакетів тільки для встановлених з'єднань;

– прозорі для клієнтів і серверів, так як не розривають TCP-з'єднання.

Недоліки міжмережевих екранів з аналізом стану:

– Реально використовуються тільки в мережевій інфраструктурі TCP/IP. Хоча треба відзначити, що міжмережеві екрани з аналізом стану можна реалізувати в інших мережевих протоколах так як й пакетні фільтри.

РОЗДІЛ 3. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ (VPN)

Приватні мережі використовуються організаціями для з'єднання з віддаленими сайтами й з іншими організаціями. Приватні мережі складаються з каналів зв'язку, орендованих у різних телефонних компаній і постачальників послуг Інтернету. Ці канали зв'язку характеризуються тим, що вони з'єднують тільки два об'єкти, будучи відділеними від іншого трафіку, так як орендовані канали забезпечують двосторонній зв'язок між двома сайтами.

Приватні мережі мають безліч переваг:

– інформація зберігається в секреті;

– віддалені сайти можуть здійснювати обмін інформацією негайно;

– віддалені користувачі не відчувають себе ізольованими від системи, до якої вони здійснюють доступ.

На жаль, цей тип мереж володіє одним великим недоліком – високою вартістю. Використання приватних мереж – дуже коштовне задоволення. Використовуючи менш швидкісні канали зв'язку, можна заощадити гроші, але тоді у віддалених користувачів почнуться недоліки по швидкості, і деякі із зазначених вище переваг стануть менш очевидними.

Зі збільшенням числа користувачів Інтернету багато організацій перейшли на використання віртуальних приватних мереж (VPN). Віртуальні приватні мережі забезпечують багато переваг приватних мереж за меншу ціну. Проте, із впровадженням VPN з'являється цілий ряд питань і небезпек для організації. Правильно побудована віртуальна приватна мережа може принести організації велику користь. Якщо ж VPN реалізована некоректно, вся інформація, передана через VPN, може бути доступна з Інтернету.

Визначення віртуальних приватних мереж

Отже, ми маємо намір передавати через Інтернет секретні дані організації без використання орендованих каналів зв'язку, як і раніше приймаючи всі міри для забезпечення конфіденційності трафіку. Яким же чином нам вдасться відокремити свій трафік від трафіку інших користувачів глобальної мережі? Відповіддю на це питання є шифрування.

В Інтернеті можна зустріти трафік будь-якого типу. Значна частина цього трафіку передається у відкритому виді, і будь-який користувач, що спостерігає за цим трафіком, зможе його розпізнати. Це відноситься до більшої частини поштового й веб-трафіку, а також сеансам зв'язку через протоколи telnet і FTP. Трафік Secure Shell (SSH) і Hypertext Transfer Protocol Secure (HTTPS) є шифруємим трафіком, і його не зможе переглянути користувач, що відслідковує пакети. Проте, трафік типу SSH і HTTPS не утворить віртуальну приватну мережу VPN.

Віртуальні приватні мережі володіють декількома характеристиками:

– трафік шифрується для забезпечення захисту від прослуховування;

– здійснюється автентифікація віддаленого сайту;

– віртуальні приватні мережі забезпечують підтримку безлічі протоколів;

– з'єднання забезпечує зв'язок тільки між двома конкретними абонентами.

Так як SSH і HTTPS не здатні підтримувати декілька протоколів, теж саме відноситься й до реальних віртуальних приватних мереж. VPN-пакети змішуються з потоком звичайного трафіку в Інтернеті й існують окремо з тієї причини, що даний трафік може зчитуватися тільки кінцевими точками з'єднання.

Розглянемо більш детально кожну з характеристик VPN. Вище вже говорилося про те, що трафік VPN шифрується для захисту від

прослуховування. Шифрування повинно бути досить потужним, щоб можна було гарантувати конфіденційність переданої інформації на той період, поки вона буде актуальна. Паролі мають термін дії, рівним 30 дням (мається на увазі політика зміни пароля через кожні 30 днів); однак секретна інформація може не втрачати своєї цінності протягом багатьох років. Отже, алгоритм шифрування й застосування VPN повинні запобігти нелегальному дешифруванню трафіку на кілька років.

Друга характеристика полягає в тому, що здійснюється автентифікація віддаленого сайту. Ця характеристика може вимагати автентифікацію деяких користувачів на центральному сервері або взаємну автентифікацію обох вузлів, які з'єднує VPN. Використовуваний механізм автентифікації контролюється політикою. Політика може передбачити автентифікацію користувачів за двома параметрами або з використанням динамічних паролів. При взаємній автентифікації може знадобитися, щоб обидва сайти демонстрували знання певного загального секрету (під секретом мається на увазі деяка інформація, заздалегідь відома обом сайтам), або можуть знадобитися цифрові сертифікати.

Віртуальні приватні мережі забезпечують підтримку різних протоколів, особливо на прикладному рівні. Наприклад, віддалений користувач може використовувати протокол SMTP для зв'язку з поштовим сервером, одночасно використовуючи NetBIOS для з'єднання з файловим сервером. Обоє зазначених протоколу можуть працювати через той самий цикл зв'язку або канал VPN (рисунок 3.1).

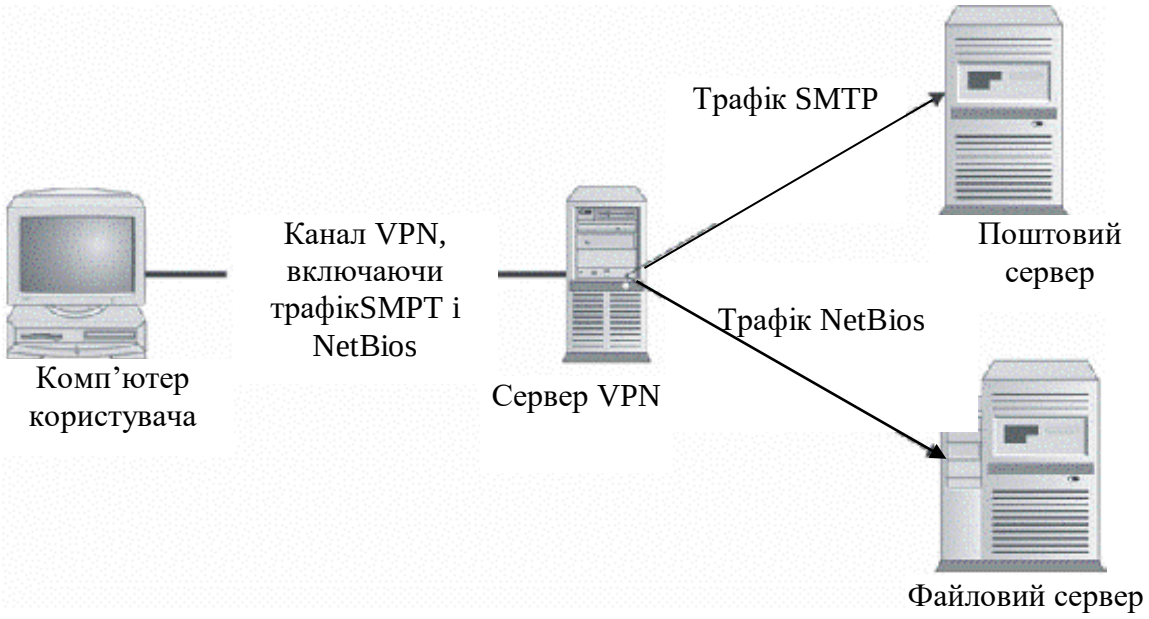

Рисунок 3.1 – Віртуальні приватні мережі підтримують безліч протоколів

VPN з'єднує два конкретних об'єкти, створюючи в такий спосіб унікальний канал зв'язку між двома абонентами. Кожна з кінцевих точок VPN може одноразово підтримувати кілька з'єднань VPN з іншими кінцевими точками, однак кожна із точок є окремою від інших, і трафік розділяється за допомогою шифрування.

Віртуальні приватні мережі, як правило, підрозділяються на два типи:

– користувальницькі VPN;

– вузлові VPN.

Різниця між ними полягає в методі використання, а не в способі відділення трафіку кожним із двох типів мереж.

Розгортання користувальницьких віртуальних приватних мереж

Користувальницькі VPN являють собою віртуальні приватні мережі, побудовані між окремою користувальницькою системою й вузлом або мережею організації. Часто користувальницькі VPN використовуються

співробітниками, що перебувають у відрядженні або працюють віддалено. Сервер VPN може бути міжмережним екраном організації або бути окремим VPN-сервером. Користувач підключається до Інтернету через підключення до локального постачальника послуг і ініціює VPN-з'єднання з вузлом організації через Інтернет.

Вузол організації запитує в користувача автентифікаційні дані й, у випадку успішної автентифікації, дозволяє користувачеві здійснити доступ до внутрішньої мережі організації, так якби користувач перебував у середині вузла й фізично розташовувався всередині мережі. Очевидний той факт, що швидкість мережного з'єднання буде обмежуватися швидкістю підключення користувача до Інтернету.

Користувальницькі VPN дозволяють організаціям обмежувати доступ віддалених користувачів до систем або файлів. Це обмеження повинне базуватися на політику організації й залежить від можливостей продукту VPN.

У той час як користувач має VPN-з'єднання із внутрішньою мережею організації, він також може з'єднуватися й працювати з Інтернетом або виконувати інші дії як звичайний користувач Інтернету. Мережа VPN підтримується окремим застосунком на комп'ютері користувача (рисунок 3.2).

У деяких випадках комп'ютер користувача може виступати в ролі маршрутизатора між Інтернетом і мережею VPN (і, отже, внутрішньою мережею організації). Цей тип мережного атакуючого впливу необхідно ретельно вивчити перед застосуванням користувальницької віртуальної приватної мережі. Деякі клієнти VPN містять політику, що знижує ризик прояву даної погрози.

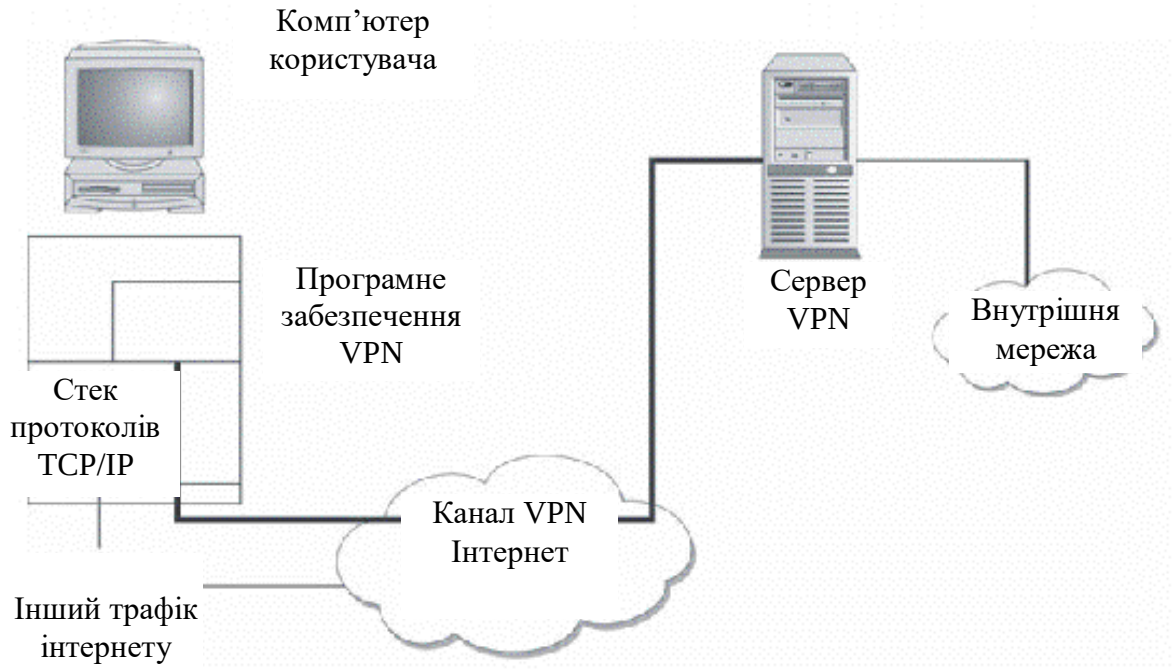

Рисунок 3.2 – Конфігурація користувальницької VPN

Переваги користувальницьких VPN

Користувальницькі VPN володіють двома основними перевагами:

– Співробітники, що перебувають у відрядженні, можуть здійснювати доступ до електронної пошти, файлів і внутрішніх систем у будь-який час.

– Співробітники, що працюють дома, можуть здійснювати доступ до служб мережі, як і співробітники, що працюють в організації, без оренди дорогих виділених каналів.

Обидві ці переваги можна приписати до економії коштів. Економія може полягати у відмові від використання дорогих міжміських і міжнародних з'єднань, орендованих каналів зв'язку або у виконанні співробітниками завдань по адмініструванню серверів, що приймають вхідні з'єднання.

Проблеми, пов'язані з користувальницькими VPN

Правильне використання користувальницьких VPN може знизити витрати організації, але користувальницькі VPN не є рішенням всіх

можливих проблем. При їхньому використанні мають місце значні ризики, пов'язані з безпекою, і проблеми реалізації, з якими доводиться рахуватися.

Можливо, найбільшою проблемою безпеки при використанні VPN співробітником є одночасне з'єднання з іншими сайтами Інтернету. Як правило, програмне забезпечення VPN на комп'ютері користувача визначає, чи необхідно трафік передавати через VPN, або його необхідно відправити на який-небудь інший сайт у відкритому виді. Якщо на комп'ютер користувача була зроблена атака з використанням "троянського коня", можливо, що якийсь зовнішній нелегальний користувач використовує комп'ютер співробітника для підключення до внутрішньої мережі організації (рисунок 3.3). Атаки даного типу здійснюються досить складно, але вони зовсім реальні.

Користувальницькі VPN вимагають такої ж уваги до питань, пов'язаних з керуванням користувачами, як і внутрішні системи. У деяких випадках користувачі VPN можуть бути прив'язані до ідентифікаторів користувачів у домені Windows або до іншої системи централізованого керування користувачами. Ця можливість спрощує керування користувачами, однак адміністраторам як і раніше варто зберігати пильність і стежити за тим, яким користувачам потрібно віддалений VPN-доступ, а яким – ні.

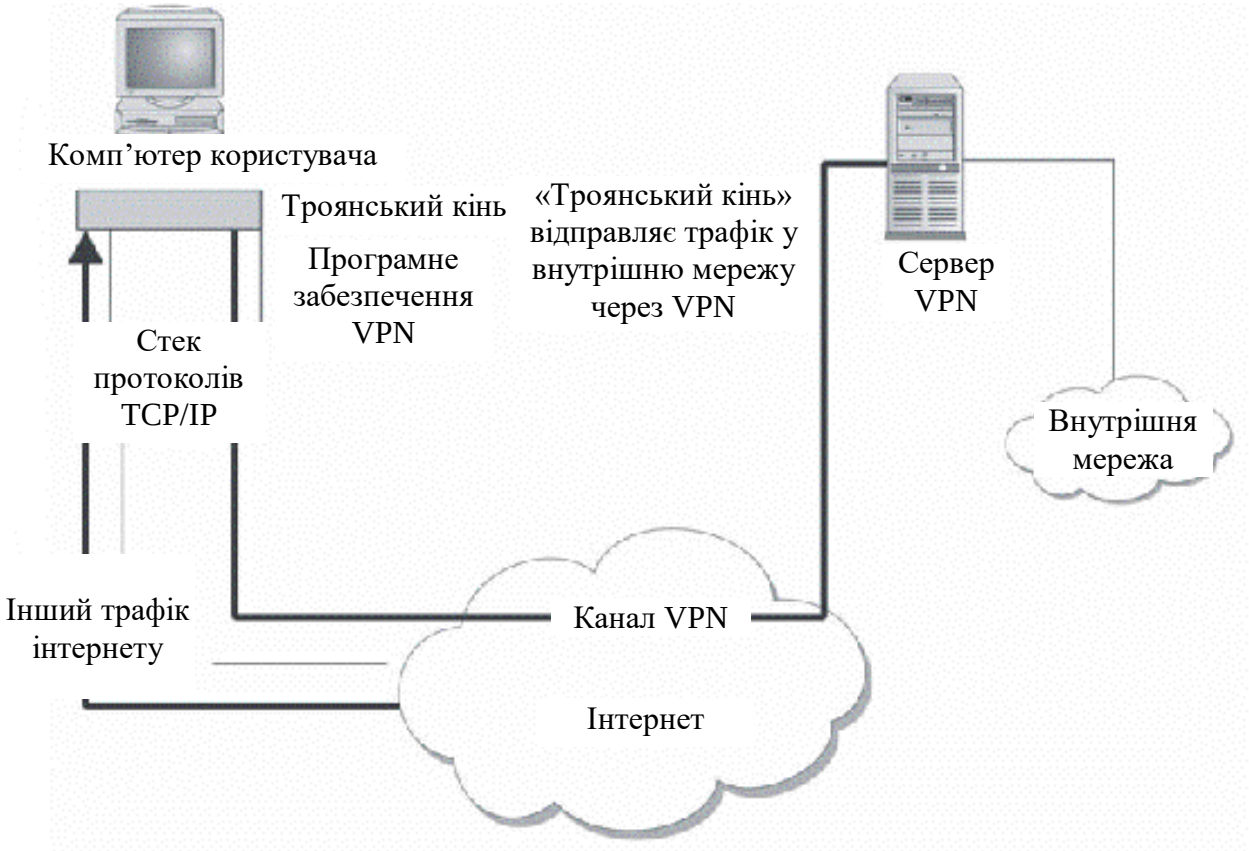

Рисунок 3.3 – Використання "троянського коня" для проникнення у внутрішню мережу організації

Якщо керування VPN-користувачами не пов'язане із центральною системою керування користувачами, цей факт повинен ураховуватися в процедурах керування користувачами, що залишають організацію.

Користувачі повинні проходити автентифікацію перед використанням мереж VPN. Так як VPN дозволяє здійснювати віддалений доступ до внутрішньої мережі організації, ця автентифікація повинна бути двофакторною, тобто запитувати два автентифікаційні параметри. Одним з параметрів може бути сам комп'ютер користувача. У цьому випадку другим параметром повинно бути щось відоме користувачеві або безпосередньо з ним зв'язане. У кожному разі, другий параметр не повинен перебувати на комп'ютері й не повинен бути з ним зв'язаний.

В організаціях повинна прийматися в розрахунок навантаження трафіком. Головною точкою навантаження є VPN-сервер у вузлі організації. Ключовим параметром навантаження є очікуване число одночасних з'єднань. При установці кожного з'єднання VPN-сервер повинен мати можливість розшифровувати додатковий трафік. Хоча процесор може забезпечувати підтримку більших обсягів трафіку, він може не забезпечувати шифрування й розшифровку великої кількості пакетів без значних затримок. Отже, сервер VPN повинен створюватися з урахуванням очікуваного числа одноразових з'єднань.

Ще один момент може вплинути на використання організацією користувальницької VPN. Він пов'язаний з використанням трансляції мережних адрес (NAT) на протилежному кінці з'єднання. Якщо очікується, що співробітники організації будуть намагатися використовувати VPN з вузлів, захищених міжмережевими екранами, можуть виникнути проблеми. Наприклад, якщо організація А є консалтинговою компанією зі співробітниками, що працюють в організації Б, в А може виникнути потреба надати своїм співробітникам зворотний зв'язок для роботи з електронною поштою й одержання доступу до файлів. Однак, якщо ці співробітники працюють із комп'ютерів, що входять до складу внутрішньої мережі організації Б, у якій використовується динамічна NAT для приховання адрес внутрішніх систем, це виявиться неможливим. Якщо у вашій організації перевага віддається використанню VPN саме таким чином, варто перевірити можливості програмного забезпечення VPN.

Керування користувальницькими VPN

Керування користувальницькими VPN, головним чином, полягає в керуванні користувачами і їхніми комп'ютерами. При поділі співробітників необхідно виконувати відповідні процедури по керуванню користувачами.

Зрозуміло, на комп'ютерах користувачів повинні встановлюватися правильні версії програмного забезпечення VPN і реалізовуватися відповідні конфігурації. Якщо комп'ютери належать організації, це

програмне забезпечення є стандартним компонентом для кожного комп'ютера. Якщо організація дозволяє співробітникам використовувати VPN зі своїх домашніх комп'ютерів, їй знадобиться збільшити загальний рівень підтримки цих користувачів, так як різні комп'ютери й постачальники послуг Інтернету можуть вимагати наявність різних конфігурацій.

В організаціях також може розглядатися питання про надання співробітникам міжмережевого екрана офісного або домашнього рівня. Багато таких систем можуть управлятися віддалено, що дозволяє організації відслідковувати й налаштовувати системи.

Одним із ключових аспектів користувальницької VPN, про який не слід забувати, є установка антивірусної програми на комп'ютері користувача. Цей програмний пакет повинен забезпечувати регулярне відновлення своїх баз (принаймні, щомісяця) для протистояння вірусам і "троянським коням", що проникають на комп'ютер користувача.

Розгортання вузлових мереж VPN

Вузлові віртуальні приватні мережі використовуються організаціями для підключення до віддалених вузлів без застосування дорогих виділених каналів або для з'єднання двох різних організацій, між якими потрібен зв'язок для здійснення інформаційного обміну, пов'язаного з діяльністю цих організацій. Як правило, VPN з'єднує один міжмережевий екран або прикордонний маршрутизатор з іншим аналогічним пристроєм (рисунок 3.4).

Щоб ініціювати з'єднання, один з вузлів здійснює спробу передати трафік іншому вузлу. Внаслідок цього на обох протилежних вузлах з'єднання VPN ініціюється VPN. Обоє кінцевих вузла визначають параметри з'єднання залежно від політик, наявних на вузлах. Обидва сайти будуть автентифікувати один одного за допомогою деякого загального визначеного секрету або за допомогою сертифіката з відкритим ключем.

Деякі організації використовують вузлові VPN як резервні канали зв'язку для орендованих каналів.

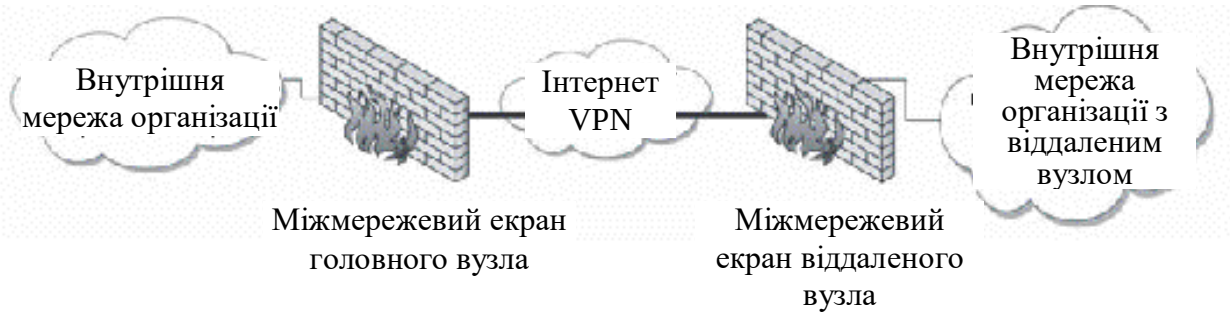

Рисунок 3.4 – Міжвузлове з'єднання VPN, що проходить через Інтернет

При роботі з даною конфігурацією необхідно забезпечувати правильне налаштування маршрутизації. Крім того, фізичний канал зв'язку, використовуваний для VPN, обов'язково повинен відрізнятися від каналу, використовуваного орендованим з'єднанням. Може виявитися так, що і те і те з'єднання здійснюються через той самий фізичний канал зв'язку, внаслідок чого не буде забезпечуватися належний рівень надмірності.

Переваги вузлових VPN

Як і у випадку з користувальницькими VPN, основною перевагою вузлових VPN є економічність. Організація з невеликими, віддаленими один від одного офісами може створити віртуальну приватну мережу, що з'єднує всі віддалені офіси з центральним вузлом (або навіть один з одним) зі значно меншими витратами.

На базі політики організації можуть бути розроблені правила, що визначають, яким чином віддалені сайти будуть підключатися до центрального сайту або один до одного. Якщо вузлова VPN призначена для з'єднання двох організацій, то на доступ до внутрішніх мереж і комп'ютерних систем можуть накладати строгі обмеження.

Проблеми, пов'язані з вузловими VPN

Вузлові VPN розширюють периметр безпеки організації, додаючи нові віддалені вузли або навіть віддалені організації. Якщо рівень безпеки віддаленого вузла невеликий, VPN може дозволити зловмисникові одержати доступ до центрального вузла й інших частин внутрішньої мережі організації. Отже, необхідно застосовувати жорсткі політики й реалізовувати функції аудита для забезпечення безпеки організації в цілому. У випадках, коли дві організації використовують вузлову VPN для з'єднання своїх мереж, дуже важливу роль грають політики безпеки, встановлені по обидві сторони з'єднання. У даній ситуації обидві організації повинні визначити, які дані можуть передаватися через VPN, а які – ні, і відповідним чином налаштувати політики на своїх міжмережевих екранах.

Автентифікація вузлових VPN також є важливою умовою для забезпечення безпеки. При установці з'єднання можуть використовуватися довільні секрети, але той самий загальний секрет не повинен використовуватися для більш ніж одного з'єднання VPN. Якщо передбачається використовувати сертифікати з відкритими ключами, необхідно створити процедури для підтримки зміни й відстеження терміну дії сертифікатів.

Як і у випадку з користувальницькими VPN, сервер VPN повинен підтримувати дешифрування й шифрування VPN-трафіку. Якщо рівень трафіку високий, сервер VPN може виявитися перевантаженим. Особливо це відноситься до ситуації, коли міжмережевий екран є VPN-сервером, і має місце Інтернет-трафік великого обсягу.

Нарешті, необхідно обміркувати питання, пов'язані з адресацією. Якщо вузлова VPN використовується всередині однієї організації, у ній необхідна наявність однакової схеми адресації для всіх вузлів. У цьому випадку адресація не представляє якої-небудь складності. Якщо ж VPN використовується для з'єднання двох різних організацій, необхідно вжити

заходів для попередження будь-яких конфліктів, пов'язаних з адресацією. На рисунку 3.5 відображена виникла конфліктна ситуація. Тут обидві організації використовують частини того самого приватного адресного простору (мережа 10.1.1.x).

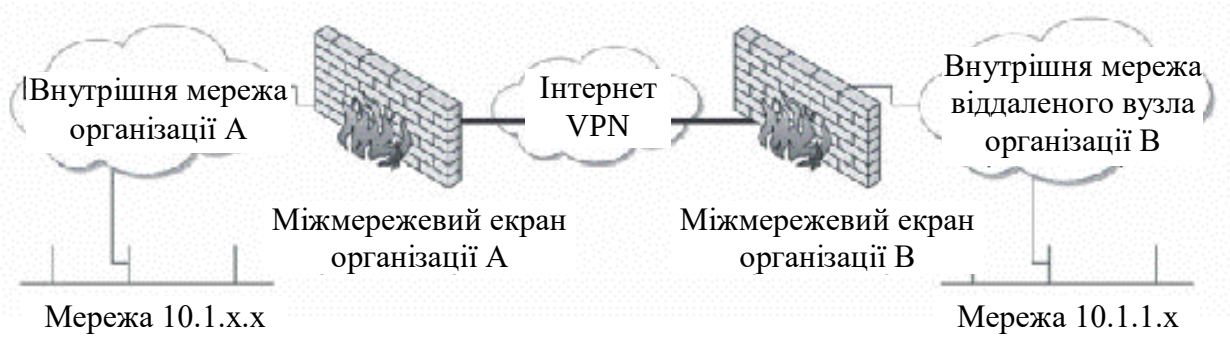

Рисунок 3.5 – Вузлова VPN може викликати конфлікти, пов'язані з адресацією

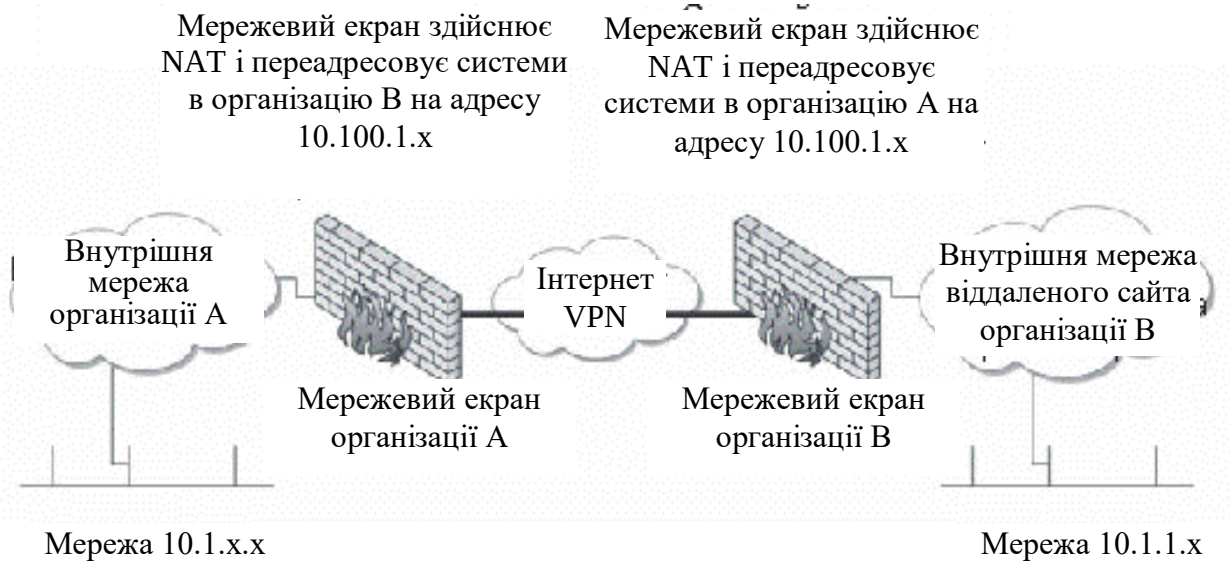

Рисунок 3.6 – Вузлова VPN використовує NAT для запобігання конфліктів адресації

Очевидно, що схеми адресації будуть конфліктувати один з одним, і маршрутизація трафіку не буде функціонувати. В цьому випадку кожна сторона з'єднання VPN повинна виконувати трансляцію мережних адрес і

переадресовувати системи іншої організації на їхню власну схему адресації (рисунок 3.6).

Керування вузловими VPN

При здійсненні контролю над маршрутизацією можуть знадобитися додаткові функції по керуванню. На маршрутизаторах внутрішніх мереж буде потрібно створити маршрути до віддалених сайтів. Ці маршрути, поряд з керуванням схемою адресації, повинні чітко документуватися щоб уникнути ненавмисного видалення маршрутів у процесі керування маршрутизатором.

Поняття стандартних технологій функціонування VPN

Мережа VPN складається з чотирьох ключових компонентів:

– Сервер VPN.

– Алгоритми шифрування.

– Система автентифікації.

– Протокол VPN.

Ці компоненти реалізують відповідність вимогам по безпеці, продуктивності й здатності до взаємодії. Те, наскільки правильно реалізована архітектура VPN, залежить від правильності визначення вимог. Визначення вимог повинне містити в собі наступні аспекти:

– Кількість часу, протягом якого необхідно забезпечувати захист інформації.

– Число одночасних з'єднань користувачів.

– Очікувані типи з'єднань користувачів (співробітники, що працюють віддалено або перебувають у поїздці).

– Число з'єднань із віддаленим сервером.

– Типи мереж VPN, яким знадобиться з'єднання.

– Очікуваний обсяг вхідного й вихідного трафіку на віддалених вузлах.

– Політика безпеки, що визначає налаштування безпеки.

При розробці системи також може виявитися корисним указати додаткові вимоги, пов'язані з місцем розташування співробітників, що перебувають у поїздці (маються на увазі вузли в інших організаціях або в номерах готелів), а також типи служб, які будуть працювати через VPN.

Сервер VPN

Сервер VPN являє собою комп'ютер, що виступає в ролі кінцевого вузла з'єднання VPN. Даний сервер повинен мати характеристики, достатні для підтримки очікуваного навантаження. Більша частина виробників програмного забезпечення VPN повинна надавати рекомендації із приводу продуктивності процесора й конфігурації пам'яті, залежно від числа одноразових VPN-з'єднань. Варто забезпечити наявність системи з відповідними параметрами, а також подбати про її подальшу модернізацію.

Може знадобитися створення декількох серверів VPN, щоб забезпечити підтримку очікуваного навантаження. У цьому випадку очікувані VPN-з'єднання повинні якомога швидше розподілятися між системами.

Деякі виробники включають у свої системи методи обходу помилок і дозволяють наявність надлишкових серверів VPN. Обхід помилок може не мати на увазі розподіл навантаження, тому з'єднання можуть як і раніше вимагати розподілу між серверами. Цю обставину необхідно брати до уваги при побудові систем.

VPN-сервер повинен бути розташований у мережі. Сервер може бути міжмережевим екраном або прикордонним маршрутизатором (рисунок 3.7), що спрощує розміщення VPN-сервера. Як альтернатива сервер може бути й окремою системою. У цьому випадку сервер повинен бути розташований у виділеній демілітаризованій зоні (DMZ) (рисунок 3.8). В ідеальному випадку демілітаризована зона VPN повинна містити тільки VPN-сервер і бути окремим від DMZ Інтернету, що містить веб-сервери й поштові сервери організації. Причиною є те, що VPN-сервер

дозволяє доступ до внутрішніх систем авторизованим користувачам і, отже, повинен розглядатися як об'єкт із більшим ступенем довіри, ніж поштові й веб-сервери, доступ до яких може бути здійснений особами, що не користуються довірою. Демілітаризована зона VPN захищається набором правил міжмережевого екрана й дозволяє передачу тільки того трафіку, що вимагає VPN.

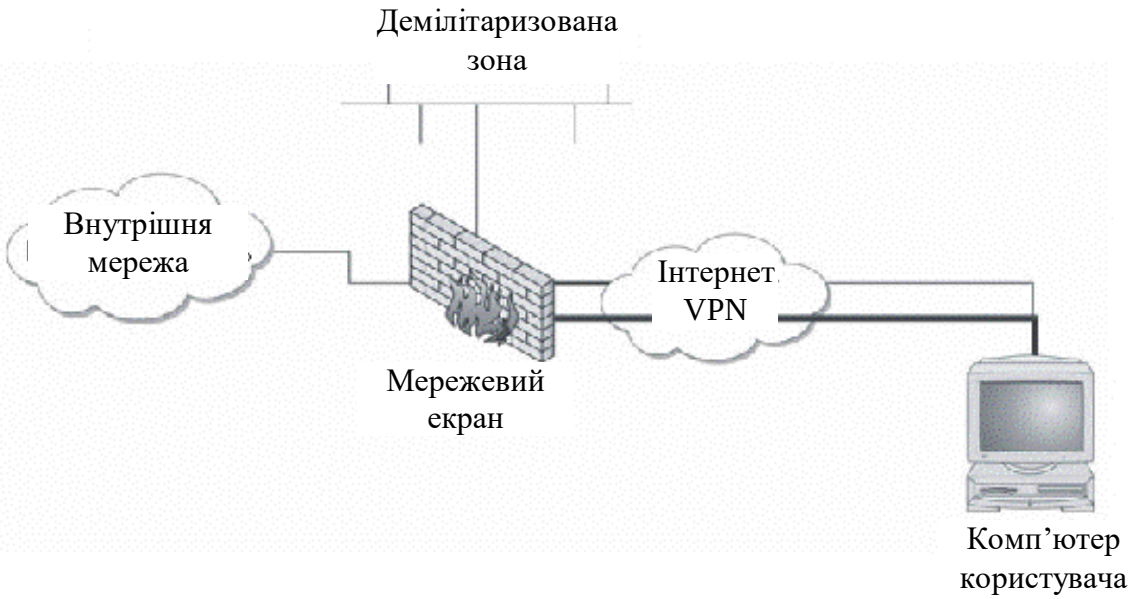

Рисунок 3.7 – Архітектура мережі VPN, у якій міжмережний екран є VPN-сервером

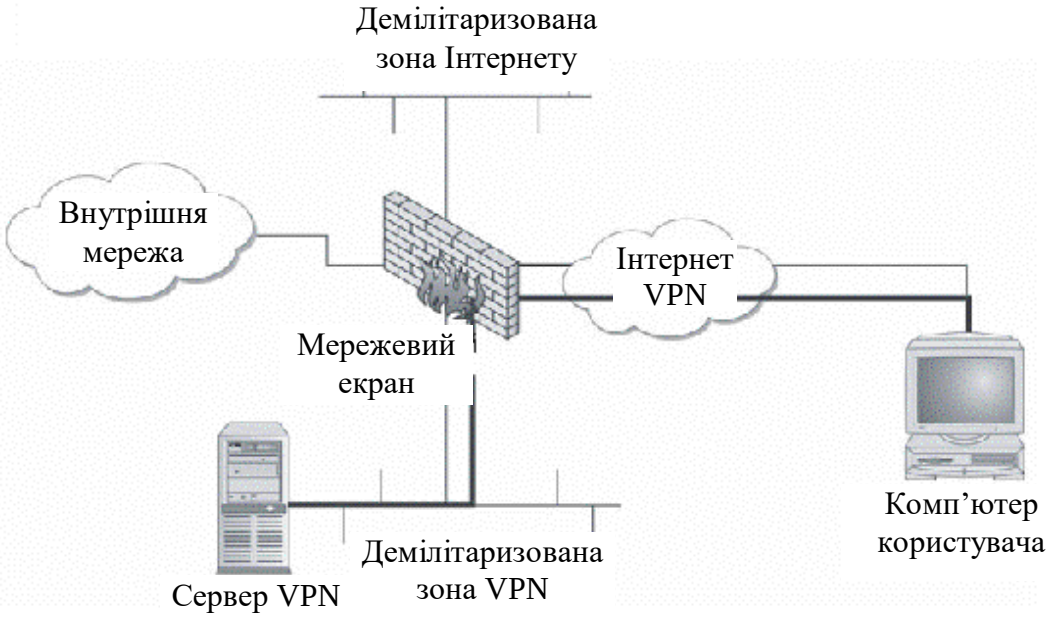

Рисунок 3.8 – Архітектура мережі VPN для окремого сервера VPN

Якщо VPN-сервер розташований у демілітаризованій зоні VPN, міжмережевий екран може зажадати вдосконалення для підтримки навантаження трафіку. Навіть незважаючи на те, що міжмережевий екран не буде виконувати функцію шифрування, вихідний міжмережевий екран може мати недостатні характеристики для забезпечення обчислювальної потужності, необхідної для трафіку VPN. Якщо трафік VPN є важливим для організації, на міжмережевому екрані повинна бути присутня деяка система обходу помилок. Як альтернатива можна використовувати окрему платформу VPN. Такий пристрій забезпечить розвантаження міжмережевого екрана, взявши на себе функції обробки VPN.

Правила політики міжмережевого екрана для демілітаризованої зони VPN визначені в табл. 3.1. Тут утримуються правила, необхідні для демілітаризованої зони Інтернету й демілітаризованої зони VPN.

Таблиця 3.1 – Правила політики міжмережевого екрана, що включають демілітаризовану зону VPN

Номер правила	**Вихідний IP**	**Кінцевий IP**	**Служба**	**Дія**
1	Будь-який	VPN-сервер	Служба VPN	Прийняття.
2	VPN-сервер	Внутрішня мережа	Будь-який	Прийняття
3	Будь-який	VPN-сервер	Будь-який	Відхилення
4	Будь-який	Веб-сервер	HTTP	Прийняття
5	Будь-який	Поштовий сервер	SMTP	Прийняття
6	Поштовий сервер	Будь-який	SMTP	Прийняття
7	Внутрішня мережа	Будь-який	HTTP, HTTPS, FTP, telnet, SSH	Прийняття
8	Внутрішня DNS	Будь-який	DNS	Прийняття
9	Будь-який	Будь-який	Будь-який	Скидання

Правила 1, 2 і 3 відносяться до демілітаризованої зони VPN. Правило 1 дозволяє клієнтам VPN здійснювати доступ до сервера VPN з використанням будь-якої служби, необхідної програмним забезпеченням VPN. Правило 2 дозволяє VPN-серверу здійснювати маршрутизацію цих з'єднань у внутрішню мережу. Правило 3 виключає з'єднання демілітаризованої зони Інтернету з демілітаризованою зоною VPN, ізолюючи демілітаризовану зону VPN від систем в DMZ Інтернету, що користуються меншою довірою.

Алгоритми шифрування

Алгоритм шифрування, використовуваний в VPN, повинен бути стандартним потужним алгоритмом. Виникає питання: яка ж система шифрування найкраща? Взагалі, всі стандартні й потужні алгоритми можуть ефективно використовуватися при побудові VPN. Різні виробники віддають перевагу різним алгоритмам, залежно від обмежень реалізації продукту, аспектів, пов'язаних з ліцензуванням, і переваг по програмуванню. Встановлюючи програмний пакет VPN, варто вислухати коментарі фахівців і переконатися в тому, що виробник використовує потужний алгоритм шифрування.

Варто відмітити, що вибір алгоритму не має принципового значення, якщо він буде стандартним і достатньо потужним. Набагато більше впливає на загальний рівень безпеки реалізація системи. Неправильно реалізована система може зробити марним самий потужний алгоритм шифрування. Взявши до уваги сказане вище, давайте вивчимо ризики, пов'язані з використанням VPN. Для того щоб одержати доступ до інформації, переданої через VPN, зловмисник повинен:

– захопити весь сеанс з'єднання, тобто розмістити пристрій прослуховування між протилежними кінцями з'єднання в тому місці, через яке повинен передаватися весь трафік VPN;

– використовувати більші обчислювальні потужності й велику кількість часу для перехоплення ключа за допомогою грубої сили й для дешифрування трафіку.

Зловмисникові набагато простіше використовувати наявну вразливість на комп'ютері користувача або вкрасти портативний комп'ютер. Якщо інформація не являє собою особливої важливості, в VPN можна використовувати будь-який широко розповсюджений, потужний алгоритм шифрування.

Система автентифікації

Третім компонентом архітектури VPN є система автентифікації. Як уже зазначалося раніше, система автентифікації VPN повинна бути двофакторною. Користувачі можуть проходити автентифікацію з використанням того, що вони знають, того, що в них є або за допомогою даних про те, ким вони є. При використанні користувальницьких VPN віддається перевага першим двом варіантам.

Гарною комбінацією засобів автентифікації є смарт-карти в парі з персональним ідентифікаційним номером або паролем. Виробники програмного забезпечення, як правило, надають організаціям на вибір кілька систем автентифікації. У даному переліку присутні провідні виробники смарт-карт.

Використання смарт-карт спричинить збільшення вартості використання VPN для кожного користувача. Незважаючи на те, що ця обставина підвищить вартість використання з'єднання, забезпечення більше високого рівня захисту цє того варте.

Якщо в організації воліють при використанні VPN покладатися тільки на паролі, вони повинні бути потужними (як мінімум, сполучення з восьми букв, цифр і спеціальних символів) і регулярно змінюватися (кожні 30 днів).

Протокол VPN

Протокол VPN визначає, яким чином система VPN взаємодіє з іншими системами в Інтернеті, а також рівень захищеності трафіку. Якщо розглянута організація використовує VPN тільки для внутрішнього інформаційного обміну, питання про взаємодію можна залишити без уваги. Однак якщо організація використовує VPN для з'єднання з іншими організаціями, власні протоколи використовувати, швидше за все, не вдасться. У розмові про алгоритм шифрування було згадано, що зовнішні навколишні фактори можуть впливати на безпеку системи більше ніж алгоритм шифрування. Протокол VPN впливає на загальний рівень безпеки системи. Причиною цьому є той факт, що протокол VPN використовується для обміну ключами шифрування між двома кінцевими вузлами. Якщо цей обмін не захищений, зловмисник може перехопити ключі й потім розшифрувати трафік, звівши нанівець всі переваги VPN.

При з'єднанні рекомендується використовувати стандартні протоколи. У цей час стандартним протоколом для VPN є IPSec. Цей протокол являє собою доповнення до IP, що здійснює інкапсуляцію й шифрування заголовка TCP і корисної інформації, що втримується в пакеті. IPSec також підтримує обмін ключами, віддалену автентифікацію сайтів і узгодження алгоритмів (як алгоритму шифрування, так і геш-функції). IPSec використовує UDP-порт 500 для початкового узгодження, після чого використовується IP-протокол 50 для всього трафіку. Для правильного функціонування VPN ці протоколи повинні бути дозволені.

Деякі постачальники мережних послуг обмежують використання цих протоколів у своїх мережах. Для того щоб мати можливість їхнього використання, клієнтові прийдеться придбати бізнес-пакет послуг замість звичайного стандартного пакета.

Головною альтернативою протоколу IPSec є протокол Secure Socket Layer (SSL), використовуваний для захисту HTTP (для HTTPS використовується порт 443). Однак, беручи до уваги, що технологія SSL

призначена для роботи на прикладному рівні, вона може виявитися не настільки ефективною в порівнянні з IPSec.

Типи систем VPN

Тепер, після обговорення функціонування мереж VPN, давайте розглянемо безпосереднє застосування VPN усередині організації. Крім питань, пов'язаних з політикою й керуванням, організації потрібно вибрати тип системи VPN. На даний час можна виділити три типи VPN:

– апаратні системи;

– програмні системи;

– веб-системи.

Апаратні системи

Апаратні системи VPN, як правило, базуються на апаратній платформі, використовуваній в якості VPN-сервера. На цій платформі виконується програмне забезпечення виробника, а також, можливо, деяке спеціальне програмне забезпечення, призначене для поліпшення можливостей шифрування. У більшості випадків для побудови VPN на системі віддаленого користувача необхідна наявність відповідного програмного забезпечення. Апаратні платформи також можуть використовуватися для побудови міжвузлових VPN, хоча це залежить від виробника встаткування.

Апаратна система VPN має дві переваги.

– ***Швидкість.*** Устаткування, як правило, оптимізовано для підтримки VPN, за допомогою чого забезпечується перевага у швидкості в порівнянні з комп'ютерними системами загального призначення. За рахунок цього досягається можливість підтримки більшого числа одночасних VPN-з'єднань.

– ***Безпека.*** Якщо апаратна платформа спеціально розроблена для застосунку VPN, з її системи видалені всі зайві програми й процеси. За рахунок цього знижується ступінь схильності атакам у порівнянні з комп'ютерною системою загального призначення, у якій працюють інші

процеси. Це не виходить, що комп'ютер загального призначення не може бути належним чином захищений. Як правило, використання комп'ютера загального призначення вимагає додаткових зусиль по налаштуванню безпеки.

Той факт, що VPN використовується на базі апаратної платформи, не означає, що система ніколи не піддасться атаці. Власник системи повинен регулярно перевіряти наявність відновлень, що випускаються виробником системи.

Програмні системи

Програмні VPN працюють на комп'ютерних системах загального призначення. Вони можуть бути встановлені на виділеній для VPN системі або разом з іншим програмним забезпеченням, таким як міжмережевий екран. При завантаженні програмного забезпечення необхідно забезпечити достатню потужність апаратної платформи для підтримки VPN. Так як VPN-продукт установлюється на комп'ютери, наявні в організації, керівництво організації повинне подбати про відповідність комп'ютерів пропонованим вимогам:

– Програмні VPN-системи можуть використовуватися в такий же спосіб, як і апаратні системи. Існує програмне забезпечення для підтримки користувальницьких і вузлових VPN.

– При установці програмного забезпечення VPN необхідно забезпечити відповідну конфігурацію системи, а також усунути всі уразливості, установивши потрібні відновлення.

Веб-системи

Головним недоліком більшості користувальницьких систем VPN є потреба в установці програмного забезпечення на систему-клієнт. Безперечно, програмне забезпечення, що встановлювалося на клієнтські системи, збільшувало обсяг робіт по керуванню користувальницькими VPN. Більше того, клієнтське програмне забезпечення в багатьох випадках не працювало належним чином з деякими додатками, завантаженими на

комп'ютер-клієнт. Ця обставина підвищувала вартість підтримки й приводило до того, що багато організацій стали встановлювати на спеціально виділені комп'ютери тільки програмне забезпечення VPN.

Зазначені проблеми привели до того, що деякі виробники VPN стали розглядати веб-браузери в якості VPN-клієнтів і реалізовувати цей підхід на практиці. Він полягає в тому, що користувач за допомогою браузера підключається до VPN через SSL. SSL забезпечує шифрування трафіку, а підтвердження дійсності користувача виконується за допомогою засобів автентифікації, вбудованих у систему. Для надання користувачеві необхідних послуг використовується кілька різних механізмів. Серед них можна виділити надбудови браузера й віртуальні машини Java.

У той час як вартість підтримки й обслуговування безсумнівно нижче, то на даний час жодна з безклієнтних систем VPN не забезпечує повну функціональність. Цим мережам VPN властиві обмеження, що полягають у наборі використовуваних застосунків і методі підключення користувачів до внутрішніх систем. Організаціям варто розглядати варіант використання таких систем, так як це знижує витрати на обслуговування, однак необхідно враховувати безпосередні вимоги користувачів і погодити їх з обмеженнями, наявними в системах.

Визначення розходжень між типами VPN

На підприємстві ухвалено рішення використовувати VPN, у результаті чого встановлений VPN-конструктор. Необхідно скласти оціночний звіт про методи шифрування, протоколи тунелювання й аспекти безпеки, пов'язані з додатками, які можуть використовувати VPN, такими як засоби передачі голосу й відеоданих через служби IP (відеоконференції) і засоби віддаленого зберігання/резервування й відновлення. Чи обов'язково шифрування даних у кожному з випадків?

Для кожного з застосунків варто з'ясувати наступне.

– Який тип VPN краще використовувати для застосунку – міжвузлову або користувальницьку VPN?

– Де розташовані кінцеві вузли VPN? Яким небезпекам можуть піддаватися ці кінцеві вузли?

– Чи накладають кінцеві вузли або користувачі застосунку які-небудь додаткові вимоги до механізму автентифікації, пов'язаному з VPN?

– Визначите відповідному застосунку механізми автентифікації.

– Відстежити інформацію під час передачі. Чи є вона відкритою для перехоплення або прослуховування? Якщо так, визначите, чи забезпечує використовуваний механізм шифрування належний рівень захисту інформації.

Отже, те, що добре працює з одним застосунком, може зовсім не працювати з іншою програмою. Міжвузлові й користувальницькі VPN мають різні вимоги до автентифікації й безпеки кінцевих вузлів. Це необхідно взяти до уваги при побудові VPN для використання застосунком. Вибір механізму шифрування й потужність використовуваного алгоритму шифрування прямо впливає на те, які атаки будуть припинятися. У процесі розробки необхідно брати до уваги всі наявні погрози безпеки.

РОЗДІЛ 4. ТЕХНОЛОГІЇ ТУНЕЛЮВАННЯ

Протокол GRE

Існують різні способи інкапсуляції одного протоколу в інший. Розглянемо протокол GRE (Generic Routing Encapsulation), що дозволяє інкапсулювати будь-який протокол. Це може бути використане для будь-яких цілей, наприклад:

– Використовується в поєднанні з PPTP для створення віртуальних приватних мереж (VPN);

– застосовується в технології WDS для координації дій точок доступу і контролера WDS.

– використовується в технологіях мобільного IP.

Будемо вважати, що є пакет, який необхідно інкапсулювати і доставити деякому одержувачеві. Цей пакет буде вмістом GRE-пакета. GRE-пакет, що вийшов, потім інкапсулюється в пакет деякого іншого протоколу, і відправляється. Будемо називати цей зовнішній протокол протоколом доставки.

Результуючий пакет має наступний формат:

Заголовок протоколу доставки
Заголовок GRE
Вміст пакету GRE

Рисунок 4.1 – Формат GRE-пакета

В GRE-заголовку втримується тип інкапсульованого протоколу. Якщо вмістом пакета є IPv4, то тип протоколу повинен бути 0x800 для IPv6 повинен бути 0x86DD.

Коли кінцева точка тунелю декапсулює GRE-пакет, у якого вмістом є пакет IPv4, адреса одержувача в заголовку вмісту пакета може використовуватися для подальшої доставки пакета. Повинна виконуватися перевірка на те, щоб адреса одержувача у вкладеному пакеті не дорівнювала адресі в інкапсулюючому пакеті, так як це є іншим кінцем тунелю, і в цьому випадку відбувається зациклення.

Як протокол доставки може також використовуватися протокол IPv4.

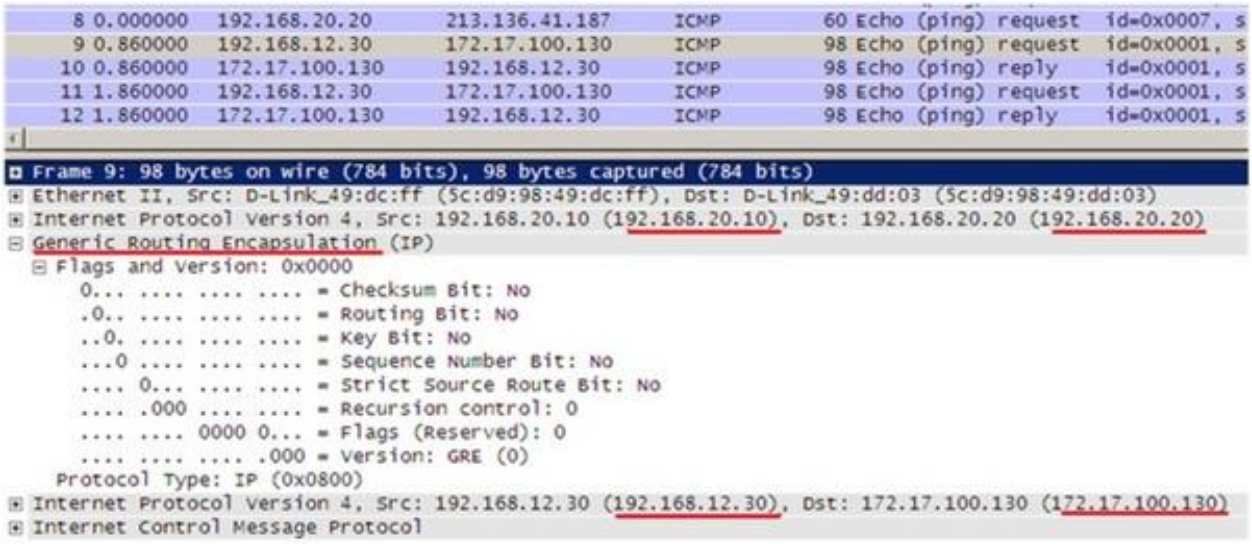

Рисунок 4.2 – Протокол GRE

Віртуальні приватні мережі

Virtual Private Network (VPN) – це різні технології, які дозволяють створювати логічні мережі, що використовують як транспорт інші мережні протоколи. При цьому характеристики безпеки створеної логічної мережі можуть відрізнятися від характеристик безпеки мережі, що використовується як транспорт. Такі мережі можуть створюватися на різних рівнях стека OSI вихідної транспортної мережі. Створювана логічна мережа не обов'язково повинна бути маршрутизуємою, вона може забезпечувати з'єднання типу точка-точка.

VPN використовуються у двох основних сценаріях:

– Для з'єднання двох віддалених локальних мереж, використовуючи як транспорт мережу з іншими параметрами безпеки.

– Для входу віддаленого користувача в локальну мережу, використовуючи як транспорт мережу з іншими параметрами безпеки.

При створенні VPN завжди варто пам'ятати, що безпека комп'ютерної системи й мережного трафіку залежить від багатьох факторів. Розгортання VPN з використанням тої або іншої технології є тільки частиною комплексного підходу до забезпечення безпеки.

Безпека, забезпечувана VPN, залежить від багатьох параметрів операційного оточення, у якому VPN виконується. Наприклад, від безпеки ОС, джерела випадкових чисел, способів керування системою й т.д.

Розглянемо основні протоколи створення VPN і проаналізуємо їхні характеристики з погляду безпеки створюваних з'єднань, можливостей масштабування й наявності яких-небудь додаткових можливостей.

Таблиця 4.1

Назва протоколу	Конфіден-ційність з’днання	Цілісність з’днання	Способи автентифікації учасників	Захист від можливості на майбутнє підлаштову-ватися під одну зі сторін
PPP	Є	Немає	CHAP	Немає
PPPoE	Є	Немає	CHAP	Немає
PPTP	Є	Немає	CHAP	Немає
L2TP	Є	Немає	CHAP	Немає
IPSec	Є	Є	Загальний секрет, сертифікат	Є
L2TP/IPSec	Є	Є	CHAP, загальний секрет, сертифікат	Є
GRE/IPSec	Є	Є	Загальний секрет, сертифікат	Є
SSL	Є	Є	Сертифікат	Є

Протоколи канального рівня

Протокол Point-to-Point Protocol (PPP)

PPP – двоточковий протокол канального рівня (Data Link) мережевої моделі OSI. Зазвичай використовується для встановлення прямого зв'язку між двома вузлами мережі, причому він може забезпечити автентифікацію з'єднання, шифрування (з використанням ECP, RFC 1968) і стиснення даних. Використовується на багатьох типах фізичних мереж: нуль-модемний кабель, телефонна лінія, стільниковий зв'язок і т. д.

Часто зустрічаються підвиди протоколу PPP такі, як Point-to-Point Protocol over Ethernet (PPPoE), використовуваний для підключення по Ethernet, і іноді через DSL; і Point-to-Point Protocol over ATM (PPPoA), який використовується для підключення по ATM Adaptation Layer 5 (AAL5), який є основною альтернативою PPPoE для DSL.

PPP являє собою ціле сімейство протоколів:

– протокол керування лінією зв'язку (LCP);

– протокол управління мережею (NCP);

– протоколи автентифікації (PAP, CHAP);

– багатоканальний протокол PPP (MLPPP).

Протокол PPP визначає механізм інкапсуляції для пересилання пакетів, що належать будь-яким мережним протоколам, по каналах точка-точка 2 рівня. Звичайно користувач одержує з'єднання канального рівня (так зване L2-з'єднання) до Network Access Server (NAS), використовуючи одну з технологій доступу типу точка-точка: dial-up POTS, ISDN, ADSL і т.п. Протокол PPP виконується поверх даного з'єднання. У найпростішому випадку завершення L2-з'єднання й кінцева точка PPP-протоколу розташовані на одному і тому самому фізичному пристрої NAS.

L2TP розширює можливості PPP, допускаючи, щоб кінцеві точки L2 і PPP були розташовані на різних пристроях, з'єднаних між собою мережею, по якій можуть передаватися пакети. При використанні L2TP користувач створює L2-з'єднання з концентратором (наприклад, модемом,

ADSL DSLAM і т.п.), потім концентратор тунелює окремі PPP-кадри до NAS. Це дозволяє обробляти PPP-кадри окремо від точки завершення L2-з'єднання.

Одна очевидна перевага такого поділу полягає в тому, що замість вимоги завершення L2-з'єднання на NAS (що може вимагати тягти проведення на великі відстані), з'єднання може закінчуватися на локальному концентраторі, що створює логічну PPP-сесію поверх поділюваної інфраструктури таку, як frame relay або Інтернет. З погляду користувача не існує розходження між завершенням L2 безпосередньо на NAS або використанням L2TP.

Протокол L2TP визначає створення тунелів між двома вузлами й наступною інкапсуляцією тунелюємих PPP сесій.

У протоколах, що виконують пересилання PPP-даних по мережі Ethernet, використовується наступна термінологія.

Таблиця 4.2.

L2TP концентратор доступу (L2TP Access Concentrator – LAC)	Вузол, що є однією з кінцевих точок L2TP-тунелю. LAC є протилежною стороною L2TP мережного серверу (LNS). LAC розташований між LNS і віддаленою системою й перенаправляє пакети до кожної з них. Пакети, що посилаються від LAC до LNS, тунелюються за протоколом L2TP. З'єднання між LAC і віддаленою системою є або локальним, або виконується за протоколом PPP. Якщо замість L2TP використовується протокол PPTP, то аналогічний вузол називається PPTP концентратор доступу – PAC.

Продовження таблиці 4.2.

L2TP мережний сервер (L2TP Network Server – LNS)	Вузол, що є однієї з кінцевих точок L2TP-тунелі. LNS є протилежною стороною LAC. LNS є логічною кінцевою точкою PPP-сесії, що тунелюється від віддаленої системи за допомогою LAC. LNS також є кінцевою точкою тунелю між LNS і LAC. Якщо замість L2TP використовується протокол PPTP, то аналогічний вузол називається PPTP мережний сервер – PNS.
Сервер мережного доступу (NAS)	Пристрій, що надає користувачам мережний доступ на вимогу. Цей доступ є доступом типу точка-точка, що використовує PSTN або ISDN канали. Функції NAS може виконувати й LAC, і LNS.
L2TP/ PPTP-тунель	Тунель між LAC і LNS. Тунель складається з керуючого з'єднання й нуля або більше L2TP-сесій. L2TP/ PPTP-тунель передає інкапсульовані дейтаграми PPP і керуючі повідомлення між LAC і LNS.
L2TP/ PPTP-сесія	У протоколах PPTP і L2TP визначене поняття сесії. LNS і LAC підтримують стан для кожного виклику, що ініційований LAC або на який відповів LAC. L2TP-сесія створюється між LAC і LNS, коли PPP-з'єднання встановлене між віддаленою системою й LNS. Дейтаграми, що відносяться до PPP-з'єднання, посилають по тунелі між LAC і LNS. Між установленими сесіями й відповідними викликами існує взаємооднозначна відповідність.
Керуюче з'єднання L2TP/PPTP	Керуюче з'єднання використовується для встановлення й підтримки як для сесій, так і самого L2TP/ PPTP-тунелю й створюється для кожної пари LAC, LNS. Керуюче з'єднання визначає всі характеристики тунелю й пов'язаних з ним сесій.

Протокол PPP призначений для створення не маршрутизуємих каналів, по яким передаються пакети між двома учасниками. Канали є повнодуплексними й функціонують в обох напрямках. Протокол забезпечує інкапсуляцію різних протоколів мережного рівня в один канал.

Протокол PPP визначає спосіб передачі дейтаграм по послідовних каналах. Протокол PPP складається з наступних протоколів:

– Протокол керування каналом (Link Control Protocol – LCP) для встановлення, конфігурування й тестування послідовного з'єднання.

– Сімейство протоколів керування мережею (Network Control Protocol – NCP) для встановлення й конфігурування різних протоколів мережного рівня.

– Для узгодження параметрів каналу використовується протокол керування каналом LCP. Протокол LCP може також виконувати автентифікацію кінцевих точок каналу.

У PPP-каналах необхідно задавати багато параметрів маршрутизуємих мережних протоколів. Наприклад, призначення й керування IP-адресами. Для рішення цих проблем використовуються протоколи керування мережею NCP.

Конфігурування виконується за допомогою переговорів про використовуваний набір опцій. Для цього кожна сторона каналу описує протилежній стороні свої можливості й вимоги.

Для того, щоб встановити з'єднання точка-точка, кожний кінець PPP-каналу повинен по-перше послати LCP-пакети для конфігурування й тестування каналу даних. Після того, як канал встановлений і виконані перемовини про додаткові опції, які необхідні LCP, PPP повинен послати NCP-пакети для вибору й конфігурування протоколів мережного рівня. Після того, як протокол мережного рівня зконфігурований, по каналу можуть посилати дейтаграми. Канал буде залишатися відкритим доти, поки явно не буде закритий LCP- або NCP-пакетами, або поки не відбудеться яка-небудь зовнішня подія.

Діаграма станів Протягом свого життєвого циклу PPP-канал проходить через наступні стани.

Рисунок 4.3 – Діаграма станів PPP-каналу

Встановлення каналу

Для встановлення з'єднання використовується LCP-протокол, у якому виконується обмін конфігураційними пакетами. Ініціалізація каналу виконується за допомогою пакета Configure-Request, на який одержувач відповідає Configure-Ack. Ініціалізація каналу завершується, і стан LCP стає відкритим після того, як пакет Configure-Ack відправлений і отриманий.

```
16 13.430000  192.168.20.10   192.168.20.20   PPP LCP    68 Configuration Request
17 13.430000  192.168.20.20   192.168.20.10   L2TP       60 Control Message - ZLB      (tunnel i
18 13.430000  192.168.20.20   192.168.20.10   PPP LCP    73 Configuration Request
19 13.430000  192.168.20.10   192.168.20.20   PPP LCP    73 Configuration Ack

⊞ Frame 16: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
⊞ Ethernet II, Src: D-Link_49:dc:ff (5c:d9:98:49:dc:ff), Dst: D-Link_49:dd:03 (5c:d9:98:49:dd:03)
⊞ Internet Protocol Version 4, Src: 192.168.20.10 (192.168.20.10), Dst: 192.168.20.20 (192.168.20.20)
⊞ User Datagram Protocol, Src Port: l2f (1701), Dst Port: l2f (1701)
⊞ Layer 2 Tunneling Protocol
⊟ Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Link Control Protocol (0xc021)
⊟ PPP Link Control Protocol
    Code: Configuration Request (0x01)
    Identifier: 0x00
    Length: 14
  ⊟ Options: (10 bytes)
      Maximum Receive Unit: 1456
      Magic number: 0x9c933d03
```

Рисунок 4.4 – Приклад LCP-запиту

Протоколом LCP конфігуруються тільки ті опції, які не залежать від конкретних протоколів мережного рівня. Конфігуруванням протоколів мережного рівня займаються окремі протоколи керування мережею (NCP).

Будь-які не-LCP-пакети, отримані в цьому стані, відкидаються.

Одержувач LCP-запиту на конфігурацію переходить у стан пересилання дейтаграм мережного рівня після ініціалізації каналу й виконання автентифікації.

Автентифікація

У деяких випадках перед обміном пакетами протоколу мережного рівня може вимагатися автентифікація протилежної сторони.

Автентифікація повинна мати місце відразу ж після встановлення каналу.

Перехід зі стану автентифікації в стан пересилання дейтаграм мережного рівня не відбувається доти, поки автентифікація не завершитися.

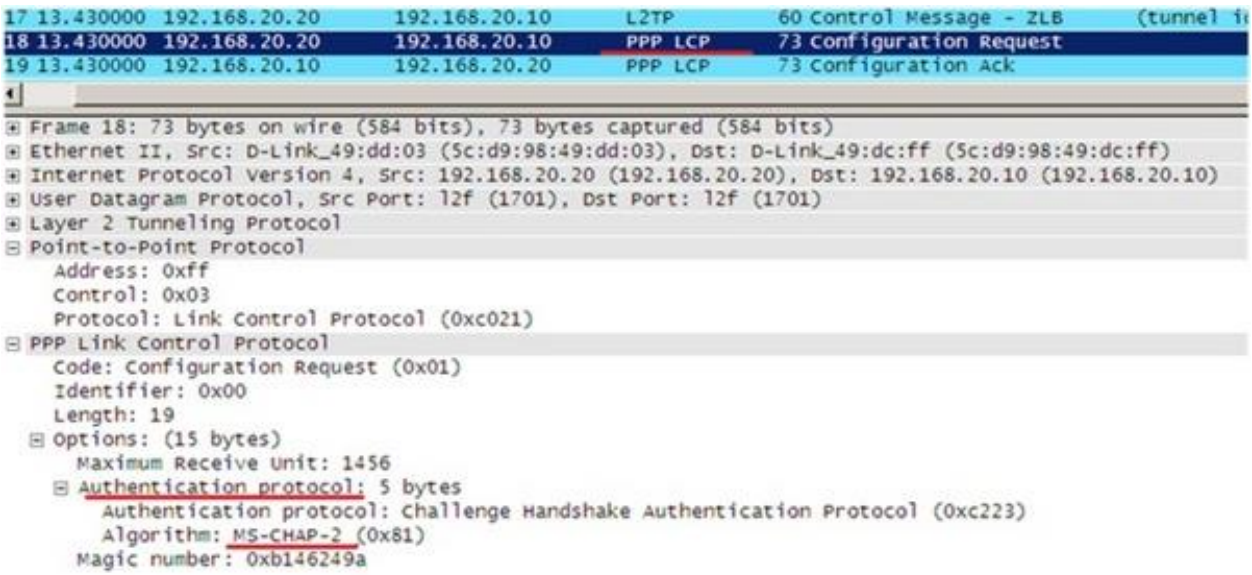

Рисунок 4.5 – Приклад запиту на автентифікацію

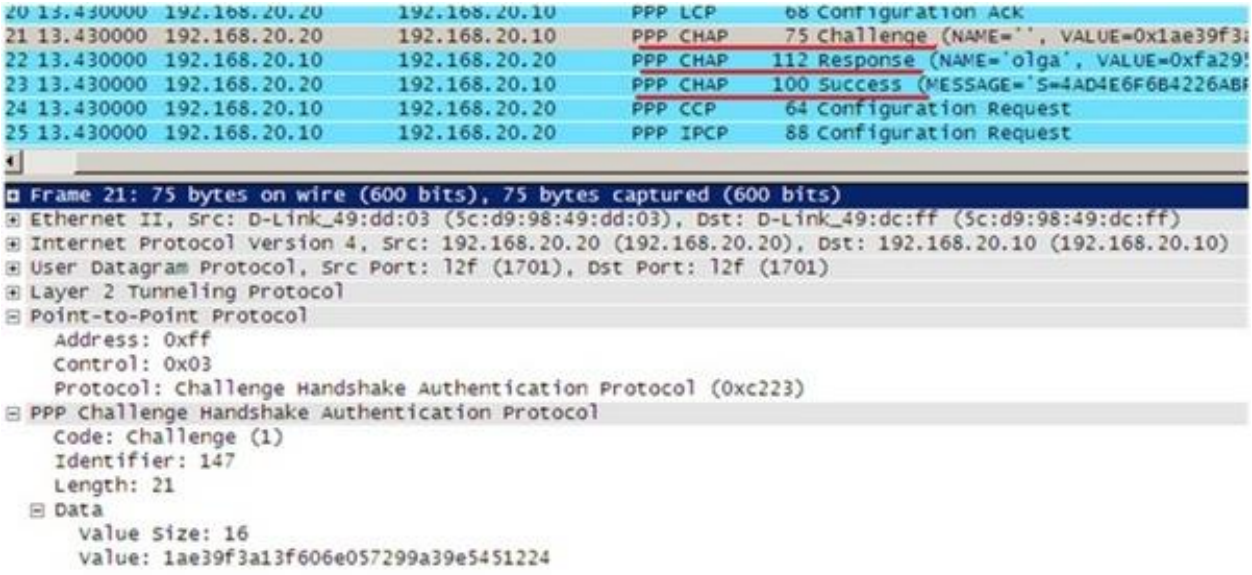

Рисунок 4.6 – CHAP-автентифікація в протоколі PPP

Протокол автентифікації Challenge-Handshake (CHAP)

Протокол CHAP використовується для періодичної перевірки автентифікації протилежної сторони за допомогою трикрокового рукостискання. Протокол виконується при початковому встановленні каналу й може повторюватися в будь-який час після того, як канал установлений.

1. Після завершення фази встановлення каналу та сторона, що запитує автентифікацію протилежної сторони, посилає їй повідомлення "challenge".

2. Протилежна сторона відповідає значенням, обчисленим за допомогою однобічної геш-функції.

3. Сторона, що запросила автентифікацію, порівнює відповідь із власним обчисленим значенням. Якщо значення збіглися, автентифікація вважається виконаною, у противному випадку з'єднання скидається.

4. Через довільні інтервали часу сторона, що запросила автентифікацію, надсилає новий запит протилежній стороні, і повторюються кроки 1 – 3.

Переваги

CHAP забезпечує захист від replay-атак, якщо як запит посилає випадкове значення.

Даний метод автентифікації заснований на тому, що обоє учасників знають якийсь секрет, що ніколи не посилається по каналу.

Хоча автентифікується тільки одна сторона, CHAP-перемовини можна вести в обох напрямках з тим же самим секретом, забезпечуючи взаємну автентифікацію.

Так як даний протокол може використовуватися для автентифікації багатьма різними системами, поле name може використовуватися для знаходження потрібного секрету. За допомогою даного поля можна також підтримувати декілька пар name/secret для кожної системи.

Недоліки

Потрібно, щоб секрет був доступний у незашифрованому виді. Секрет, що зберігається в базі даних у вигляді результату застосування однобічної функції, не може використовуватися.

Це незручно при великій кількості учасників, так як кожний секрет повинен зберігатися на обох кінцях каналу.

Щоб уникнути посилки секрету по інших каналах у мережі, рекомендується, щоб значення запиту й відповіді перевірялися на центральному сервері, а не кожним сервером мережного доступу. У противному випадку секрет буде посилатися цим серверам у зашифрованому виді. Також потрібна певна форма довіри учасників один одному.

Вимоги розробки

Переважніше, щоб секрет був приблизно тієї ж довжини, що й значення гешу використовуваної геш-функції. Наприклад, 16 октетів для MD4. Використовувана геш-функція повинна гарантувати, що розрахунково складно визначити секрет, знаючи запит і відповідь.

Кожний запит є унікальним, так як повторне використання попереднього значення запиту дозволить атакуючий раніше перехопити відповідь.

Формат конфігураційного параметра

Формат конфігураційного параметра протоколу автентифікації наступний:

Type	Length	Authentication-Protocol
Algorithm		

Type	3
Length	5
Authentication Protocol	c223

Algorithm визначає використовуваний алгоритм. Значення алгоритмів визначаються IANA (Адміністрація адресного простору Інтернет). Для MD5 значенням є 4.

Формат пакета

В інформаційне поле PPP-кадру інкапсулюється рівно один CHAP-пакет.

Code	Identifier	Length
Data ...		

Code визначає тип CHAP-пакета.

1. Запит.
2. Відповідь.
3. Успіх.
4. Неуспіх.

Identifier використовується для визначення пар відповідних запитів і відповідей.

Length визначає довжину CHAP-пакета.

Data формат даного поля визначається полем Code.

Пакет Challenge використовується як перший пакет протоколу CHAP. Автентифікуюча сторона посилає CHAP-пакет з полем Code, установленим в 1 (Challenge). Можуть посилати додаткові пакети Challenge доти, поки не буде отриманий пакет Response або не мине лічильник повторів.

Пакет Challenge також може передаватися в будь-який час протягом виконання протоколу мережного рівня, щоб гарантувати, що не було підміни учасників з'єднання.

Протилежна сторона очікує пакети Challenge протягом фаз автентифікації й протоколу мережного рівня. Після одержання пакета Challenge учасник посилає CHAP-пакет і полем Code, установленим в 2 (Response).

Після того, як пакет Response отриманий, автентифікуюча сторона порівнює значення, отримане у відповіді, із власним обчисленим значенням. Залежно від результату автентифікуюча сторона посилає або пакет Success, або пакет Failure.

Варто розуміти, що, так як пакет Success може бути загубленем, автентифікуюча сторона повторює пакети Response протягом виконання протоколу мережного рівня після завершення фази автентифікації. Всі пакети Response, отримані в будь-якій іншій фазі, відкидаються без відправлення відповіді.

Якщо пакет Failure загублений, автентифікуюча сторона завершує з'єднання, і пакети Terminate-Request і Terminate-Ack протоколу мережного рівня забезпечують альтернативний спосіб визначення, що автентифікація була невдалою.

Поле Identifier змінюється в кожному новому пакеті Challenge. Поле Identifier у пакеті Response копіюється з поля Identifier відповідного пакета Challenge.

У поле Data утримуються значення Value і Name. Значення Value у пакеті Challenge повинне бути унікальним і не залежати від секрету. Значення Value у пакеті Response є результатом обчислення геш-функції від наступних значень: Identifier, secret, значення Value з пакета Challenge.

У поле Name записана ідентифікація системи, що послала пакет. У цьому випадку синтаксис може бути кожний, як рядок символів ASCII, так і унікальний ідентифікатор в ASN.1 синтаксисі.

Обговорення безпеки

Не існує особливих вимог, як і коли повинна виконуватися повторна спроба при невдалій автентифікації. Проте, у протоколі мережевого рівня може в будь-який момент початися протокол автентифікації. Вважається, що лічильник невдалих спроб автентифікації не повинен скидатися доти, поки не буде виконана успішна автентифікація або не скинуте з'єднання.

Не існує вимоги, щоб автентифікація була взаємної або що в обох напрямках повинен виконуватися той самий протокол.

Розширення Microsoft PPP CHAP версії 1

Огляд

Microsoft розробив протокол MS-CHAP для автентифікації віддалених робочих станцій, що з однієї сторони мав би звичну для локальних користувачів функціональність, а з іншої сторони використовував би алгоритми шифрування й хешування.

MS-CHAP заснований на протоколі CHAP. Розходження між цими протоколами наступні:

– Пакет Response у протоколі MS-CHAP має формат, сумісний з Windows NT 3.5, 3.51 і 4.0. Формат MS-CHAP не вимагає, щоб

автентифікатор зберігався в явному виді або у вигляді результату однобічного перетворення.

– MS-CHAP надає механізми запиту автентифікуючою стороною повторної автентифікації й зміни пароля.

– MS-CHAP визначена множина значень кодів, які вертаються клієнтові при невдалій автентифікації.

Конфігурування LCP

Конфігурування LCP для MS-CHAP аналогічно конфігуруванню стандартного CHAP, за винятком того, що поле Algorithm має значення 0x80, а не 0x04. Реалізації PPP, що не підтримують MS-CHAP, але коректно реалізують LCP Config-Rej, не повинні мати проблем з даним нестандартним параметром.

Пакет Challenge

Пакет Challenge у протоколі MS-CHAP аналогічний пакету Challenge у стандартному протоколі CHAP.

Автентифікуюча сторона посилає 8-октетне значення в поле Value.

Пакет Response

Формат пакета Response аналогічний формату пакета Response у стандартному протоколі CHAP. Однак поле Value відрізняється:

– В 1-ом октеті може бути встановлений прапор "Використовується сумісність відповіді з Windows NT".

– LAN Manager або Windows NT сумісна відповідь.

Сумісний з LAN Manager відповідь є результатом виконання функції LmChallengeResponse()від пароля й отриманого запиту. Пароль LAN Manager не може бути довшим 14 символів і чутливий до регістра.

Сумісний з Window NT відповідь є результатом виконання функції NTChallengeResponse() від пароля й отриманого запиту. Пароль Windows NT є рядком від 0 до 256 символів Unicode, пароль чутливий до регістра. Звичайно довжина пароля в Windows NT обмежена 14 символами.

Якщо встановлено прапор "Використовується сумісність відповіді з Windows NT", то використовується Windows NT відповідь. Відповідь "LAN Manager" може використуватися, якщо аккаунт не має гешу пароля Windows NT, наприклад, якщо пароль не був змінений після завантаження з бази даних аккаунтів LAN Manager 2.x. Якщо прапор встановлений, то відповідь Windows NT ігнорується й використовується відповідь LAN Manager.

Поле Name містить ім'я користувальницького аккаунта протилежної сторони. Ім'я домену Windows NT може бути префіксом ім'я користувача.

Пакет Success

Формат пакета Success аналогічний формату стандартного пакета Success у CHAP.

Пакет Failure

Формат пакета Failure аналогічний формату стандартного пакета Failure у протоколі CHAP. Однак, на відміну від стандартних правил CHAP, вміст поля Message впливає на протокол.

Формат поля Message наступний:

E=eeeeeeeeee R=r C=cccccccccccccccc V=vvvvvvvvvv

Де "eeeeeeeeee" є десятковий код помилки, що може бути одним з наступних значень:

646 ERROR_RESTRICTED_LOGON_HOURS

647 ERROR_ACCT_DISABLED

648 ERROR_PASSWD_EXPIRED

649 ERROR_NO_DIALIN_PERMISSION

691 ERROR_AUTHENTICATION_FAILURE

709 ERROR_CHANGING_PASSWORD

Якщо встановлено прапор "r", то можлива повторна спроба, якщо прапор не встановлений, те повторна спроба не допускається. Якщо автентифікуюча сторона встановлює даний прапор в 1, вона відключає

короткі таймаути, припускаючи, що протилежна сторона запропонує користувачеві ввести нові значення й повторити відповідь.

"ccccccccccccccc" є новим значенням виклику (challenge). Дане поле не є обов'язковим. Якщо воно не посилає, то автентифікуюча сторона вважає, що повторна відповідь буде обчислена з використанням попереднього значення виклику, до якого додане десяткове число 23.

10 цифр "vvvvvvvvvv" містять код версії, що позначає версію протоколу MS-CHAP, підтримувану сервером. Це важливо тільки при виборі пакета Change Password. Якщо поле відсутнє, то вважається, що використовується версія 1.

Пакет Change Password

Пакет Change Password не посилається в стандартному протоколі CHAP. Допускається, щоб протилежна сторона змінила пароль аккаунта, зазначеного в останньому пакеті Response. У версії 1 пакет Change Password повинен посилати тільки в тому випадку, якщо автентифікуюча сторона повернула ERROR_PASSWD_EXPIRED.

Обговорення безпеки

Автентифікуюча сторона повинна обмежити число спроб введення пароля, щоб запобігти атакам, пов'язаним з перебором паролів. Так як пароль ховається за допомогою геш-функції, то можливість злому пароля залежить від криптографічної стійкості використовуваної геш-функції. Також необхідно досить часто міняти пароль.

Розширення Microsoft PPP CHAP версії 2

Протокол ***MS-CHAP-V2*** максимально відповідає як протоколу MS-CHAP-V1, так і стандартному протоколу CHAP. Розходження між протоколами MS-CHAP-V1 і MS-CHAP-V2 наступні:

– Протокол MS-CHAP-V2 надає можливість вести перемовини про алгоритм при автентифікації в протоколі LCP.

– Протокол MS-CHAP-V2 забезпечує можливість взаємної автентифікації учасників, додаючи виклик у пакет Response, на який протилежна сторона відповідає в пакеті Success.

– Обчислення поля "Windows NT compatible challenge response" змінено в пакеті Response включенням виклику протилежної сторони й ім'ям користувача.

– В MS-CHAP-V1 поле "LAN Manager compatible challenge response" завжди посилало в пакеті Response. В MS-CHAP-V2 дане поле замінене на поле Peer-Challenge.

– Змінено формат поля Message у пакеті Failure.

– Пакети Change Password версій 1 і 2 більше не підтримуються. Вони замінені єдиним пакетом Change-Password.

Конфігурація LCP

Конфігурація LCP аналогічна тієй, котра використовується в стандартному CHAP, за винятком того, що поле Algorithm має значення 0x81, а не значення 0x05 (MD5). Реалізації PPP, які не підтримують MS-CHAP-V2, але коректно реалізують LCP Config-Rej, не мають проблем з подібною нестандартною опцією.

Пакет Challenge

Пакет Challenge у протоколі MS-CHAP-V2 має той же самий формат, що й у стандартному протоколі CHAP.

Автентифікуюча сторона посилає 16-октетний виклик у поле Value. Протилежна сторона може використовувати свій алгоритм для вибору 16-октетного значення.

Пакет Response

Формат пакета Response у протоколі MS-CHAP-V2 аналогічний формату пакета Response у стандартному протоколі CHAP. Відрізняється тільки формат поля Value.

16 октетів: виклик протилежної сторони.

8 октетів: зарезервовано, повинно бути встановлено в нуль.

24 октети: NT-Response.

1 октет: прапори

Поле Peer-Challenge містить створене протилежною стороною 16-октетне випадкове число. Дане випадкове число використовується при обчисленні поля NT-Response.

Поле NT-Response є функцією від пароля, ім'я користувача, вмісту поля Peer-Challenge і містить результат функції GenerateNTResponse(). Пароль Windows є рядком довжини від 0 до 256 чутливих до регістра символів Unicode. При обчисленні значення поля NT-Response використовується тільки ім'я користувача без імені відповідного домену, незалежно від того, чи є присутнім ім'я домену в полі Name чи ні.

Поле Name є рядком довжиною від 0 до 256 чутливих до регістра символів ASCII, які є ім'ям користувача.

Пакет Success

Формат пакета Success аналогічний формату пакета Success у стандартному протоколі CHAP. Однак поле Message містить рядок відповіді довжиною 42 октету й повідомлення в друкується формате, що. Формат даного поля наступний:

S=<auth_string> M=<message>

<auth_string> складається з 20 октетів чисел, представлених у кодуванню ASCII у вигляді 40 шістнадцяткових чисел. Дане значення отримане з виклику в пакеті Challenge, полів Peer-Challenge і NT-Response з пакета Response, пароля протилежної сторони. Дане значення є результатом функції GenerateAuthenticatorResponse(). Автентифікатор перевіряється при одержанні пакета Success. Якщо автентифікатор відсутній або не коректний, протилежна сторона завершує сесію.

Пакет Failure

Формат пакета Failure аналогічний формату пакета Failure у стандартному протоколі CHAP. Однак текст зберігається в поле Message,

значення якого, на відміну від стандартного протоколу CHAP, не впливає на операції протоколу.

Формат поля Message наступний:

E=eeeeeeeeee R=r C=cccccccccccccccccccccccccccccccc V=vvvvvvvvvv

M=<msg>

Де "eeeeeeeeee" подання в ASCII десяткового коду помилки (не більше 10 цифр), яке відповідає одному з перерахованих:

– 646 ERROR_RESTRICTED_LOGON_HOURS

– 647 ERROR_ACCT_DISABLED

– 648 ERROR_PASSWD_EXPIRED

– 649 ERROR_NO_DIALIN_PERMISSION

– 691 ERROR_AUTHENTICATION_FAILURE

– 709 ERROR_CHANGING_PASSWORD

Якщо встановлено прапор "r", то допускається повтор, у протилежному випадку повтор не допускається. Установка прапора "r" означає, що на автентифікуючей стороні відключені всі короткі таймаути й передбачається, що протилежна сторона запропонує користувачеві ввести новий креденціал і повторити відповідь.

"cccccccccccccccccccccccccccccccc" є поданням в ASCII шістнадцяткового значення виклику. Дане поле завжди присутнє й має довжину 32 октети.

"vvvvvvvvvv" є поданням в ASCII коду версії, що вказує на те, що сервер підтримує протокол зміни пароля. Для протоколу MS-CHAP-V2 дане значення повинно дорівнювати 3.

<msg> є текстом у відповідному кодуванні й мові.

Пакет Change-Password

Пакет Change-Password не підтримується ні стандартним протоколом CHAP, ні протоколом MS-CHAP-V1. Даний пакет дозволяє протилежній стороні змінити пароль, зазначений у попередньому пакеті

Response. Пакет Change-Password повинен посилати тільки якщо автентифікуюча сторона надсилає ERROR_PASWD_EXPIRED у поле Message пакета Failure.

Формат даного пакета наступний:

Таблиця 4.3

Довжина поля	**Назва поля**	**Примітка**
1 октет	Code	
1 октет	Identifier	Дане поле дозволяє визначити пари запитів і відповідей.
2 октети	Length	
516 октетів	Encrypted-Password	Дане поле містить результат виконання функції NewPasswordEncruptedWithOldNt PasswordHash().
16 октетів	Encrypted-Hash	Дане поле містить результат виконання функції OldNtPasswordHashEncryptedWith NewNtPasswordHash().
16 октетів	Peer-Challenge	16-октетне випадкове число, аналогічне випадковому числу в пакеті Response.
8 октетів		Зарезервовано.
24 октети	NT-Response	Аналогічно відповідному полю в пакеті Response, але обчислене для нового пароля й виклику, отриманого в пакеті Failure.
2 октети		Прапори.

Пересилання дейтаграм мережевого рівня

Після завершення виконання LCP-протоколу повинен бути зконфігурований протокол мережевого рівня, такий як IP, IPX і т.п. Конфігурування протоколу мережевого рівня виконується протоколом керування мережею (Network Control Protocol – NCP).

Після того, як протокол NCP перейде у відкритий стан, PPP починає передачу пакетів відповідного протоколу мережевого рівня. У даному стані трафік на канальному рівні складається з комбінації пакетів LCP, NCP і протоколу мережного рівня

Протокол шифрування MPPE Microsoft

Протокол призначений для шифрування PPP-пакетів. У протоколі використовується потоковий алгоритм шифрування RC4. Про довжину ключа ведуться перемовини. MPPE (Microsoft Point-to-Point Encryption) підтримує 40-бітні, 56-бітні й 128-бітні ключі. Ключі сесії міняються часто, частота зміни ключів залежить від установлених опцій.

Ініціатор переговорів указує в опціях всі алгоритми, які він підтримує.

Одержувач відповідає повідомленням з кодом NAK з єдиною встановленою опцією. Якщо Одержувач підтримує кілька алгоритмів шифрування, то вказується найбільш сильний. Потім Ініціатор повинен або послати інший запит, що містить ту ж саму опцію, що й у повідомленні NAK Одержувача, або перервати перемовини, скидаючи з'єднання.

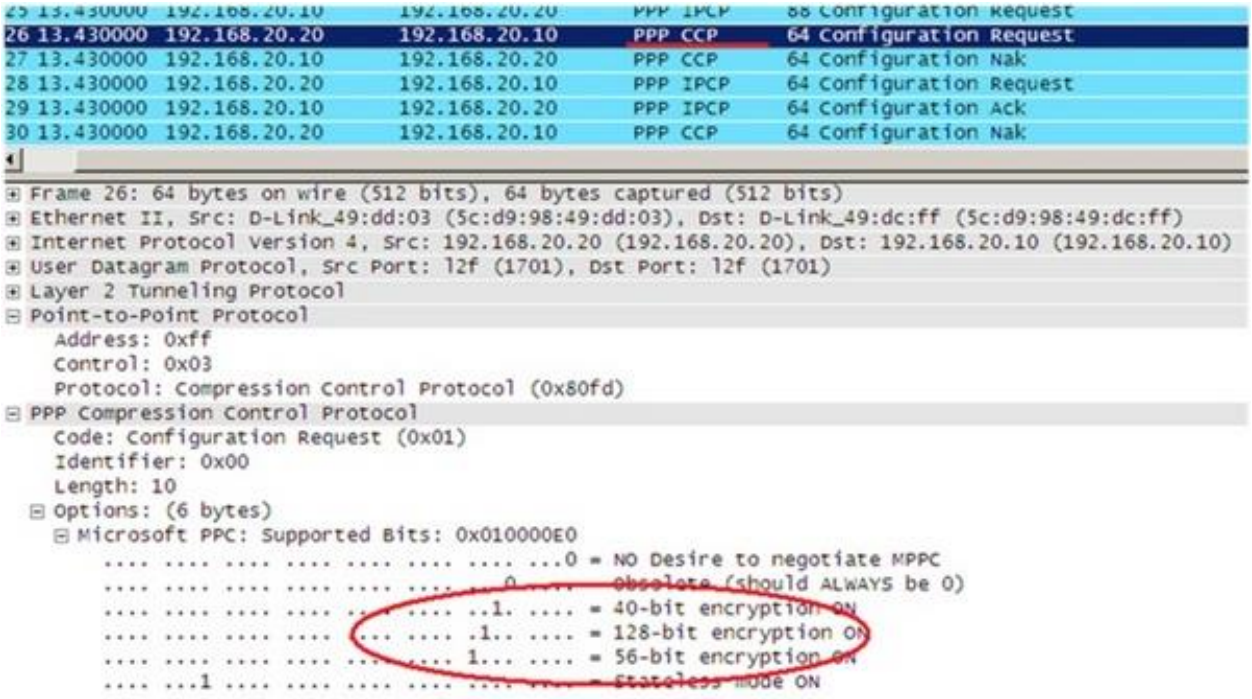

Рисунок 4.7 – Перемовини про використовувану довжину ключа

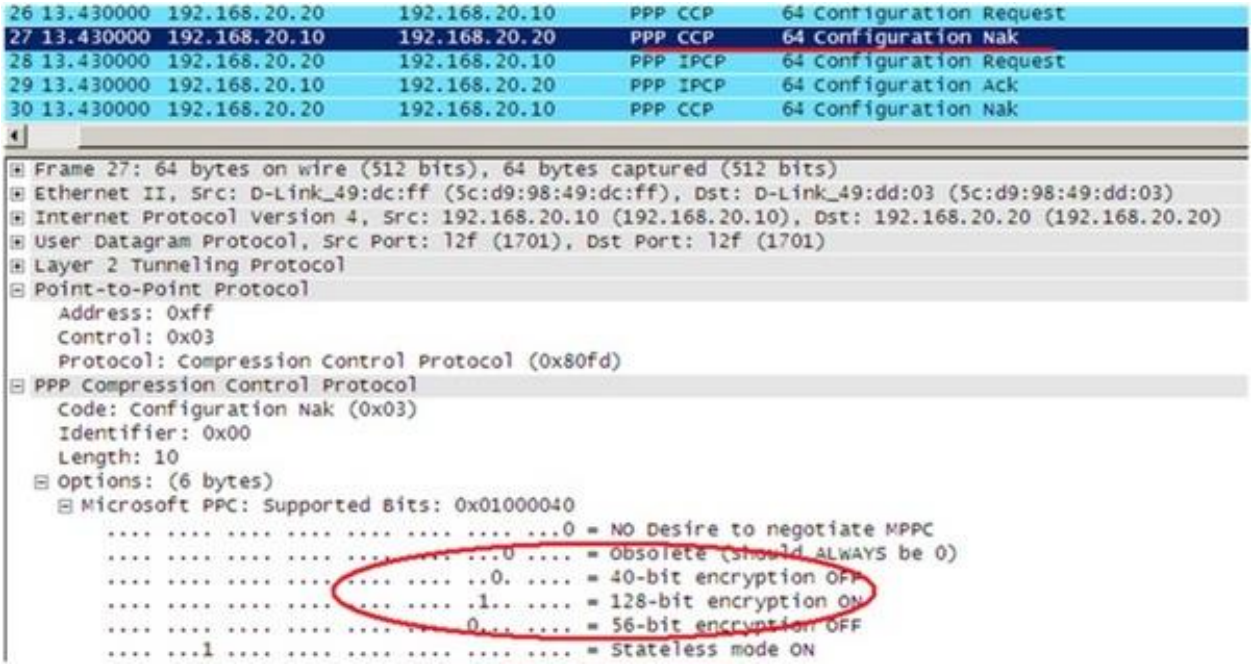

Рисунок 4.8 – Завершення переговорів про використовувану довжину ключа

Для того, щоб передавати MPPE-пакети, протокол PPP повинен перейти в стан пересилання дейтаграм мережного рівня. В інформаційне поле PPP інкапсулюється одна MPPE-дейтаграма. Для всіх зашифрованих дейтаграм у поле Protocol зазначений тип 0x00FD.

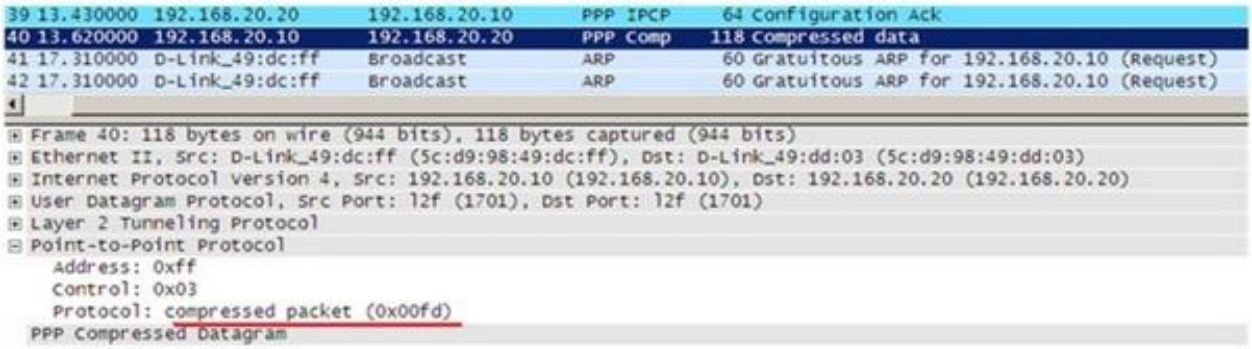

Рисунок 4.9 – Обмін зашифрованими дейтаграмами в протоколі PPP

Протокол конфігурування IP – IPCP

Протокол керування IP (Internet Protocol Control Protocol – IPCP) призначений для конфігурування IP-протоколу на обох кінцях каналу точка-точка. IPCP використовує той же самий механізм обміну пакетами, що й протокол керування каналом LCP. Обмін IPCP-пакетами починається в стані обміну дейтаграмами мережного рівня. IPCP відрізняється від LCP наступним:

Поле протоколу даних канального рівня. Єдиний пакет інкапсульований в інформаційне поле PPP-даних канального рівня.

Поле кодів. Використовуються наступні коди:

– Configure-Request – запит конфігурації.

– Configure-Ack – підтвердження на запит конфігурації.

– Configure-Nak – негативне підтвердження.

– Configure-Reject – відхилення конфігурацію.

– Terminate-Request – завершення запиту.

– Terminate-Ack – підтвердження завершення.

– Code-Reject – код відхилення.

Перед тим, як посилати будь-які IP-пакети, протокол IPCP повинен перейти у відкритий стан. Максимальна довжина IP-пакета, переданого по PPP-каналу, та ж сама, що й максимальна довжина інформаційного поля PPP-даних канального рівня. IP-дейтаграми більшого розміру будуть фрагментовані. Якщо необхідно уникнути фрагментування й наступного збору пакетів, то варто використовувати опції TCP Maximum Segment Size і MTU discovery.

Конфігураційні опції IPCP дозволяють вести перемовини про необхідні параметри IP. IPCP використовує той же самий формат конфігураційних опцій, що й LCP.

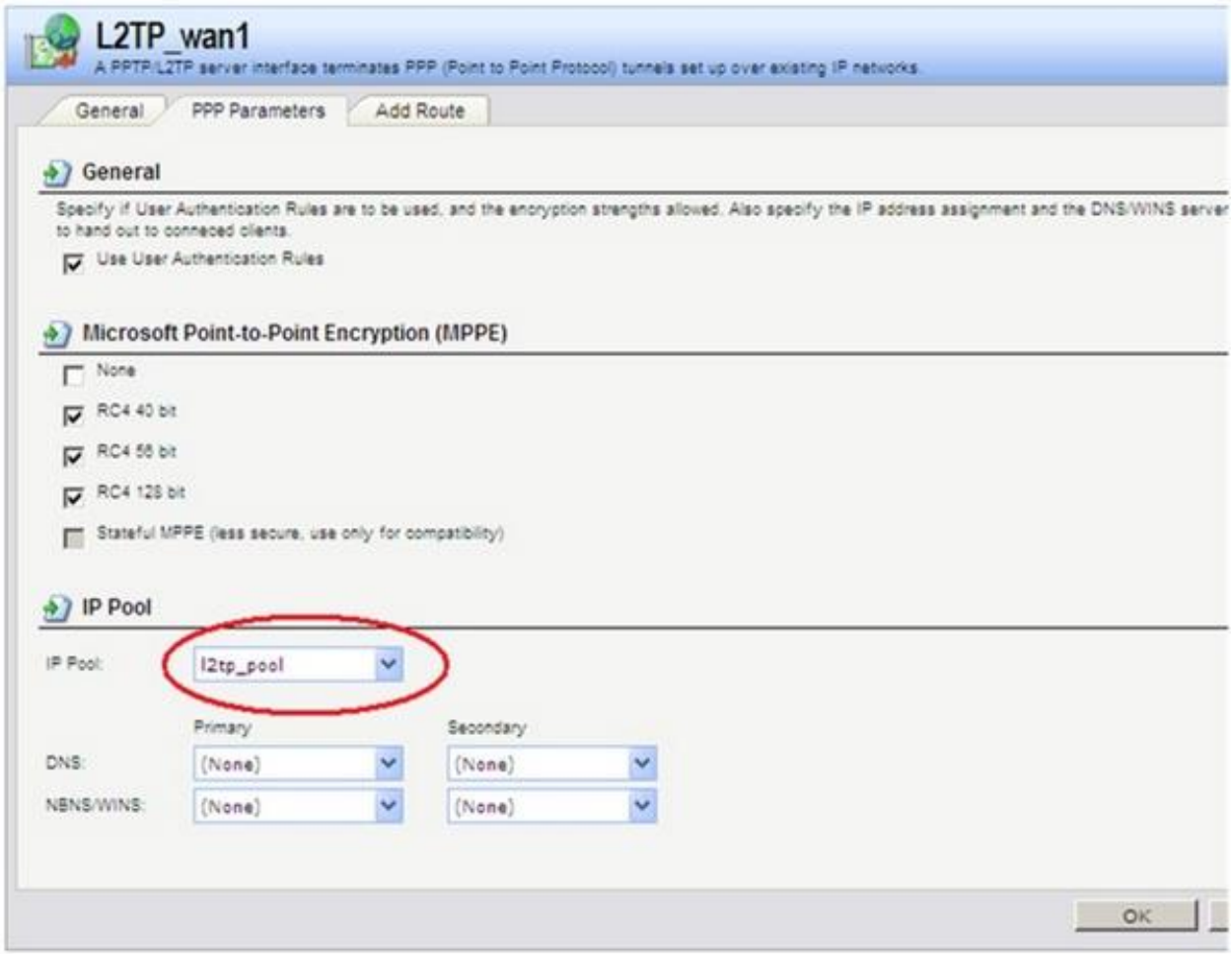

Рисунок 4.10 – Завдання діапазону IP-адрес, які будуть видаватися клієнтові:

Протокол стискування IP. Даний параметр дозволяє домовитися про використання конкретного протоколу стискування. За замовчуванням стискування не потрібене.

IP-адреса. Даний параметр надає спосіб ведення переговорів про IP-адресу, що буде призначена локальній стороні каналу. Він дозволяє відправникові Configure-Request вказати бажану IP-адресу або запросити протилежну сторону видати йому IP-адресу. Протилежна сторона може надати дану інформацію в параметрі Nak, указавши IP-адресу, що буде використовуватися.

Адреси DNS-серверів і вузлів NetBIOS Name Серверів (NBNS) у віддаленій мережі. Можуть бути зазначені IP-адреси первинного і вторинного DNS-серверів. Можливість використання інформації про адреси DNS-серверів залежить від топології віддаленої мережі й від застосунку на локальній стороні.

Параметри дозволяють домовитися про IP-адреси первинного і вторинного DNS-серверів, які будуть використовуватися на локальній стороні.

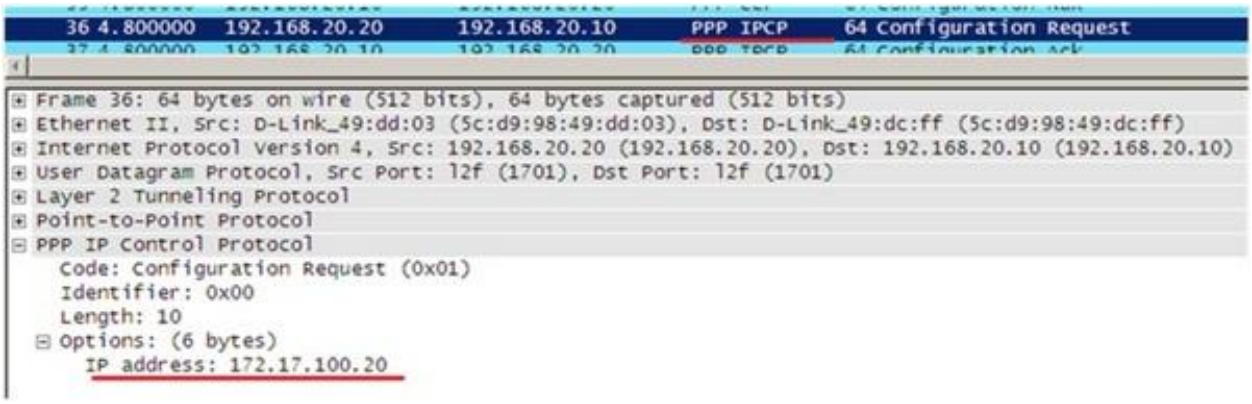

Рисунок 4.11 – Призначення IP-адреси клієнтові

РОЗДІЛ 5. АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ IP (IPSec)

Призначення сімейства протоколів IPSec

IPsec (скорочення від *IP Security*) – набір протоколів для забезпечення захисту даних, переданих по міжмережевому протоколу IP. Дозволяє здійснювати підтвердження дійсності (автентифікацію), перевірку цілісності й/або шифрування IP-пакетів. IPsec також містить у собі протоколи для захищеного обміну ключами в мережі Інтернет. В основному, застосовується для організації VPN-з'єднань.

Розглянемо архітектуру сімейства протоколів IPSec. Ціль даного сімейства протоколів полягає в тому, щоб забезпечити різні сервіси безпеки на рівні IP для протоколів IPv4 і IPv6. Розглянемо сервіси безпеки, що надаються протоколами IPSec, і використання цих протоколів у мережах TCP/IP.

Коли дані сервіси коректно встановлені, вони не заважають роботі користувачів, хостів і інших компонентів Інтернету, які не застосовують дані сервіси безпеки для захисту свого трафіку. Ці сервіси є алгоритмонезалежними. Це означає можливість додавання нових криптографічних алгоритмів без зміни самих протоколів. Наприклад, різні групи користувачів можуть використовувати різні набори алгоритмів.

Визначено стандартний набір алгоритмів за замовчуванням для забезпечення інтероперабельності у всьому Інтернеті. Використання цих алгоритмів разом із захистом трафіку, надаваний IPSec, і протоколами управління ключа дозволить розробнику систем і застосунків забезпечити високий ступінь криптографічної безпеки.

IPSec може бути реалізований як в ОС, так і в маршрутизаторі або міжмережевому екрані.

IPSec забезпечує конфіденційність, цілісність даних, керування доступом і автентифікацію джерела даних для IP-дейтаграм. Ці сервіси

надаються за допомогою підтримки стану між джерелом і одержувачем IP-дейтаграм. Даний стан визначає конкретні сервіси забезпечення безпеки на рівні дейтаграми, використовувані криптографічні алгоритми для надаваних сервісів і ключі для цих алгоритмів.

Перелічимо основні завдання протоколів IPSec:

– Забезпечення криптографічного захисту на рівні IP для протоколів IPv4 і IPv6, а саме забезпечення конфіденційності й цілісності даних і цілісності деякої послідовності дейтаграм.

– Забезпечення прозорості для IP-трафіку, для якого не потрібне використання протоколів IPSec.

– Забезпечення розширюваності, тобто можливості додавати нові набори алгоритмів без зміни самого протоколу.

IPSec призначений для безпечної взаємодії з використанням криптографії для протоколів IPv4 і IPv6. Сервіси безпеки включають керування доступом, цілісність і конфіденційність даних і захист від replay-атак, що забезпечується гарантуванням цілісності деякої послідовності дейтаграм. Ці сервіси надаються на рівні IP, забезпечуючи захист для IP-протоколу й протоколів більше високого рівня.

IPSec підтримує дві форми цілісності:

– цілісність даних;

– цілісність визначеної послідовності дейтаграм.

Цілісність даних виявляє модифікацію конкретної IP-дейтаграми, безвідносно послідовності дейтаграм у потоці трафіку. Цілісність послідовності дейтаграм є анти-replay сервісом, за допомогою якого визначається одержання дублікатів IP-дейтаграм. Це відрізняється від забезпечення цілісності з'єднання, для якого існують більше строгі вимоги до цілісності трафіку, а саме, можливість визначення загублених повідомлень.

Розглянемо виконання протоколів IPSec, основні компоненти системи і їхню взаємодію для забезпечення сервісів безпеки.

IPSec виконується на хості (Host – H) або шлюзі безпеки (Security Gateway – SG), забезпечуючи захист IP-трафіку. Термін "шлюз безпеки" використовується для позначення маршрутизатора, що реалізує IPsec-протоколи.

Захист заснований на вимогах, визначених у базі даних політики безпеки (Security Policy Database – SPD), установлюваної й підтримуваної адміністратором. У загальному випадку пакети обробляються одним із трьох способів, заснованих на інформації IP-заголовка й транспортного рівня відповідно до записів в SPD. Кожний пакет або відкидається, або пропускається без обробки, або обробляється відповідно до запису SPD для даного пакета.

Можливі способи реалізації IPSec

Існує кілька способів реалізації IPSec на хості або разом з маршрутизатором або міжмережним екраном (для створення шлюзу безпеки).

– Інтеграція IPSec у конкретну реалізацію протоколу IP. Це вимагає доступу до вихідного коду IP і робиться як на хостах, так і на шлюзах безпеки.

– "in-the-stack" (BITS) реалізації, коли IPSec реалізований "знизу" існуючої реалізації стека IP-протоколів, вбудовуючи свою реалізацію між стандартною реалізацією IP-протоколів і локальних мережних драйверів. Доступу до вихідного коду стека IP у цьому випадку не потрібно. Даний підхід звичайно реалізується на хостах, коли IPSec реалізований у вигляді бібліотеки, яка підключається.

– Використання зовнішнього криптопроцесору. Це називається "in-the-wire" (BITW) реалізацією. Такі реалізації можуть використовуватися як на хостах, так і на шлюзах. Звичайно BITW-пристрої є IP-адресуємими.

Протоколи захисту трафіку й поняття безпечної асоціації

Надавані IPSec сервіси по захисту трафіку реалізуються за допомогою двох протоколів забезпечення безпечного трафіку: Authentication Header (AH) й Encapsulating Security Payload (ESP).

Для захисту трафіку в IPSec визначені наступні протоколи:

– Протокол Encapsulating Security Payload (ESP) забезпечує конфіденційність і цілісність протоколів, розташованих вище в стеці протоколів і додатково може забезпечуватися анти-replay сервіс, тобто цілісність деякої послідовності дейтаграм.

– Протокол Authentication Header (AH) забезпечує цілісність протоколів, розташованих вище в стеці протоколів і цілісність окремих полів IP-заголовка, які не змінюються при пересиланні від відправника до одержувача, додатково може забезпечуватися анти-replay сервіс, тобто цілісність деякої послідовності дейтаграм. В IPSec v2 реалізація даного протоколу не є обов'язковою.

– Параметри цих протоколів визначаються в протоколі розподілу ключів Internet Key Exchange (IKE).

Із трафіком, безпека якого забезпечується IPSec, зв'язане поняття безпечної асоціації (Security Association – SA). SA містить всю інформацію, необхідну для виконання різних мережних сервісів безпеки.

SA являє собою симплексне (односпрямоване) логічне з'єднання, створюване між двома кінцевими точками, для забезпечення безпеки яких використовується один із протоколів IPSec. ESP і AH передають трафік по SA. Весь трафік, переданий по SA, обробляється відповідно до політики безпеки, заданої на кінцях з'єднання.

Опишемо різні аспекти керування SA, визначимо можливі способи керування політикою безпеки, способи обробки трафіку й керування SA.

SA визначає параметри сервісів безпеки, які застосовуються до трафіку. У звичайному випадку при двонаправленому з'єднанні між двома

хостами або між двома шлюзами безпеки потрібно дві SA (по одній на кожний напрямок).

Будемо розглядати SA тільки для одноадресних з'єднань.

Визначено два режими SA: режим транспорту й режим тунелювання. Транспортний режим використовується для створення VPN між двома хостами. В IPv4 заголовок протоколу безпеки транспортного режиму з'являється відразу після IP-заголовка. У протоколі ESP транспортний режим SA забезпечує сервіси безпеки тільки для протоколів більш високого рівня, але не для IP-заголовка. У випадку AH захист поширюється також і на окремі частини IP-заголовка.

Іншим режимом SA є режим тунелювання. Якщо одним з кінців з'єднання є шлюз безпеки, то за стандартами IPSec SA обов'язково повинна виконуватися в тунельному режимі, але багато виробників допускають у цьому випадку як тунельний, так і транспортний режими. Відмітимо, що коли трафік призначено для шлюзу безпеки, наприклад, у випадку ping- або SNMP-команд, шлюз безпеки розглядається як хост, і як правило використовується транспортний режим. Два хосту можуть при необхідності встановлювати тунельний режим.

У тунельному режимі додається зовнішній IP-заголовок, адресами в якому є шлюзи безпеки. Внутрішній IP-заголовок указує на кінцеві хости. Заголовок протоколу безпеки розташований після зовнішнього IP-заголовка й перед внутрішнім IP-заголовком. Якщо AH використовується в тунельному режимі, частини зовнішнього IP-заголовка є захищеними, як і весь тунелюємий IP-пакет, тобто всі внутрішні заголовки захищені, як і всі протоколи більш високого рівня. Якщо застосовується ESP, захист забезпечується тільки для тунелюємого пакета, а не для зовнішнього заголовка.

Коротко підсумуємо:

– ***Хост*** може підтримувати обидва режими, як транспортний, так і тунельний.

– ***Шлюз безпеки*** як правило використовує тільки тунельний режим. Якщо він підтримує транспортний режим, те цей режим як правило використовується тільки тоді, коли небезпечний шлюз є одержувачем трафіку, наприклад, для керування мережею.

Набір реалізованих SA сервісів безпеки залежить від обраного протоколу безпеки, режиму SA, кінцевих точок SA і вибору додаткових сервісів у протоколі. Наприклад, AH забезпечує цілісність вихідних даних і цілісність з'єднання для IP-дейтаграм. "Деталізованість" сервісу визначається ступенем деталізованості SA, для якої використовується протокол.

На кожному мережному інтерфейсі, що підтримує IPSec, повинні створюватися дві бази даних:

– БД Політики Безпеки (SPD).

– БД Безпечних Асоціацій (Security Association Database – SAD).

Перша визначає політики, які застосовуються для обробки всього IP-трафіку. Друга БД містить параметри, які пов'язані з кожною активною безпечною асоціацією. Для обробки трафіку визначається поняття Селектора, що задає множину значень полів протоколів більш високого рівня, що використовуються для визначення відповідності запису в SPD конкретному трафіку.

Для широкого використання IPSec потрібно стандартний, масштабований протокол створення й керування SA. Таким протоколом є протокол Internet Key Exchange – IKE.

Протокол складається з двох фаз – фаза I і фаза II. Кожна фаза складається з обміну декількома повідомленнями. Кожне повідомлення у свою чергу складається з декількох умістів (payload). У результаті виконання фази I створюється IKE SA. У результаті виконання фази II створюється одна або декілька ESP SA або AH SA.

Для опису форматів переданих повідомлень використовується стандарт, називаний "Безпечна Асоціація Інтернет і Протокол Керування

Ключем – Internet Security Association and Key Management Protocol (ISAKMP)". ISAKMP визначає формати пакетів для ведення переговорів про встановлення, зміну й видалення SA.

Поняття домену IPSec

Поняття домену IPSec (Domain of Interpretation – DOI) вводиться для того, щоб можна було згрупувати протоколи, що відносяться до IPSec, які використовують IKE для ведення переговорів про SA. Протоколи безпеки, що відносяться до одного DOI-домену, вибирають протокол безпеки й криптографічні перетворення із загального простору імен і використовують загальні ідентифікатори в протоколі створення SA. Вони також однаково інтерпретують дані, що втримуються в різних повідомленнях.

При описі домену визначаються наступні поняття:

– Схема іменування ідентифікаторів протоколів.

– Можливість визначення умови виконання протоколів і загальні вимоги до політики безпеки на кінцевих точках.

– Синтаксис атрибутів SA.

– Синтаксис умісту повідомлень.

– Можливі типи обміну ключа.

– Можливі типи повідомлень (Notification).

Всі ідентифікатори, використовувані в IPSec, зареєстровані в IANA. Всі дані зберігаються в мережному порядку байтів.

Визначення умов, при яких виконується

У заголовку повідомлень існує поле Situation, у якому втримується інформація, на основі якої Одержувач може зробити вивід про вимоги політики по обробки вхідного трафіку SA. Для IPSec-домену DOI визначені наступні значення:

Умова	Значення
SIT_IDENTITY_ONLY	0x01
SIT_SECRECY	0x02
SIT_INTEGRETY	0x04

Умова SIT_IDENTITY_ONLY

Умова SIT_IDENTITY_ONLY вказує, що безпечна асоціація визначається ідентифікаційною інформацією джерела, що перебуває у вмісті SA. Визначено кілька типів ідентифікацій, переданих у вмісті Identification, що посилається у фазі I IKE.

Якщо Ініціатор не підтримує ні SIT_SECRECY, ні SIT_INTEGRETY, то мітка DOI може не передаватися.

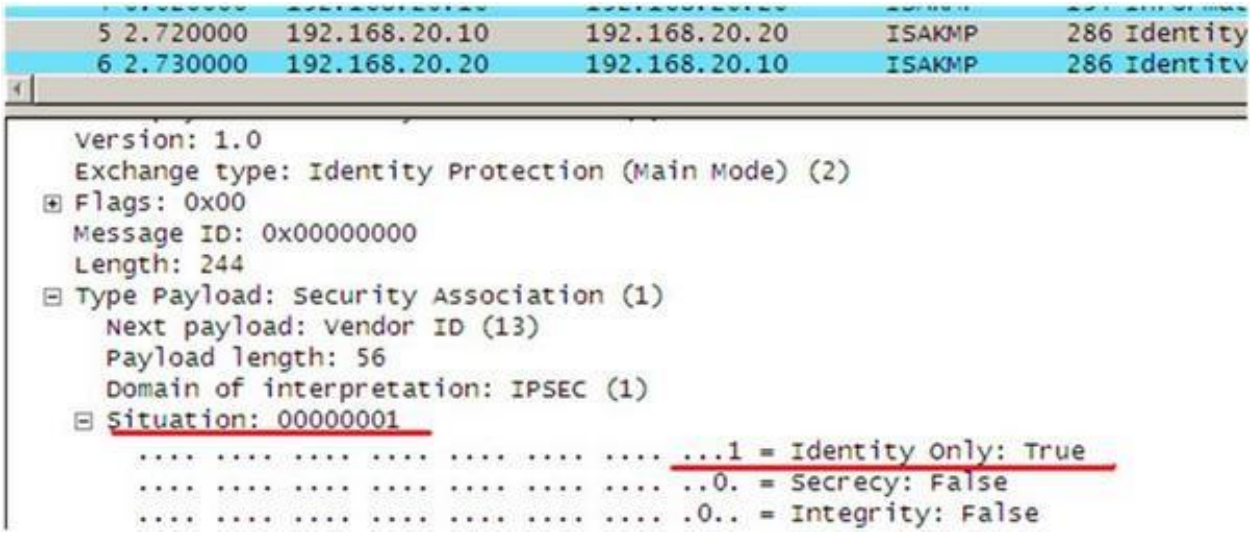

Рисунок 5.1 – Приклад поля Situation

Умова SIT_SECRECY

Умова SIT_SECRECY вказує, що SA встановлюється в оточенні, в якому потрібний захист. Поле Situation містить значення необхідного рівня чутливості.

Якщо Одержувач не підтримує SIT_SECRECY, то він повинен передати SITUATION-NOT-SUPPORTED Notification. У цьому випадку SA встановлено не буде.

Умова SIT_INTEGRETY

Умова SIT_INTEGRETY вказує, що SA встановлюється в оточенні, у якому потрібне забезпечення цілісності. Поле Situation містить значення необхідного рівня цілісності.

Якщо Одержувач не підтримує SIT_INTEGRETY, то він повинен передати SITUATION-NOT-SUPPORTED Notification. У цьому випадку SA встановлено не буде.

Можливі топології IPSec

За допомогою протоколів IPSec можна реалізувати різні топології VPN. Основні топології дозволяють створювати наступні VPN:

– Шлюз безпеки – шлюз безпеки.

– Хост – шлюз безпеки.

– Хост – хост.

Приведемо чотири варіанти топологій VPN, створюваних між хостами й шлюзами безпеки, які реалізують IPSec. Введемо наступні позначення:

Таблиця 5.1

▬	SA(АН абоESP, транспортний або тунельний режим)
⎯	незахищена публічна мережа
Host i	Хост № i
SG i	шлюз безпеки № i
Rtr i	маршрутизатор, що не підтримує IPSec, через який повинен проходити IPSec-трафік
X*	X (хост або шлюз безпеки), що підтримує IPSec

Нижче розглянуті безпечні асоціації які можуть використовувати як АН-, так і ESP-протоколи. Режим (тунельний або транспортний) визначається характером кінцевих точок. Для Host – Host SA режим може

бути як транспортним, так і тунельним. Для SG – SG SA режим швидше за все буде тунельним.

Варіант 1. Створення безпечного з'єднання між двома хостами через відкриту публічну мережу.

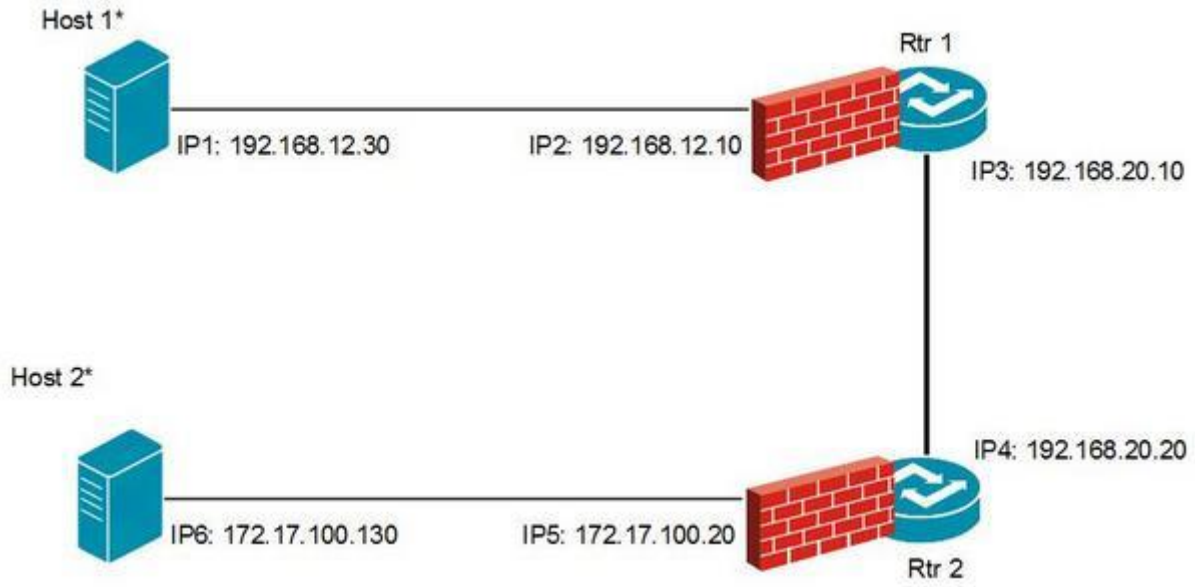

Рисунок 5.2 – Топологія мережі: VPN між двома хостами

Транспортний режим	Тунельний режим
[src:IP1; dst:IP6] [ESP]	[src:IP3; dst:IP4] [ESP] [src:IP1; dst:IP6]
Протокол більш високого рівня	Протокол більш високого рівня

Рисунок 5.3 – Вкладеність заголовків при створенні VPN між двома хостами

У даній топології обидві кінцеві точки IP-з'єднання підтримують IPSec. Ці кінцеві точки можуть реалізовувати керування доступом на прикладному рівні, ґрунтуючись на автентифікації учасників. У транспортному режимі не існує внутрішнього IP-заголовка. У тунельному

режимі внутрішній IP-заголовок існує, але, як правило, IP-адреси у внутрішньому й зовнішньому заголовках збігаються.

У даній топології маршрутизатори (Rtr 1 і Rtr 2) не підтримують IPSec, тобто не є шлюзами безпеки (SG), і не можуть аналізувати трафік, переданий між Host 1 і Host 2. Якщо ці маршрутизатори також виконують функції міжмережевого екрана, то вони повинні пропускати весь IPSec-трафік, як трафік керування SA, так і трафік протоколів AH або ESP.

Трафік між Host 1 і Host 2 захищений сервісами безпеки як у публічній мережі, так і в обох локальних мережах. IP-адреси хостів видні як у публічній мережі, так і в обох локальних мережах.

Варіант 2. Створення віртуальної приватної мережі між двома віддаленими локальними мережами.

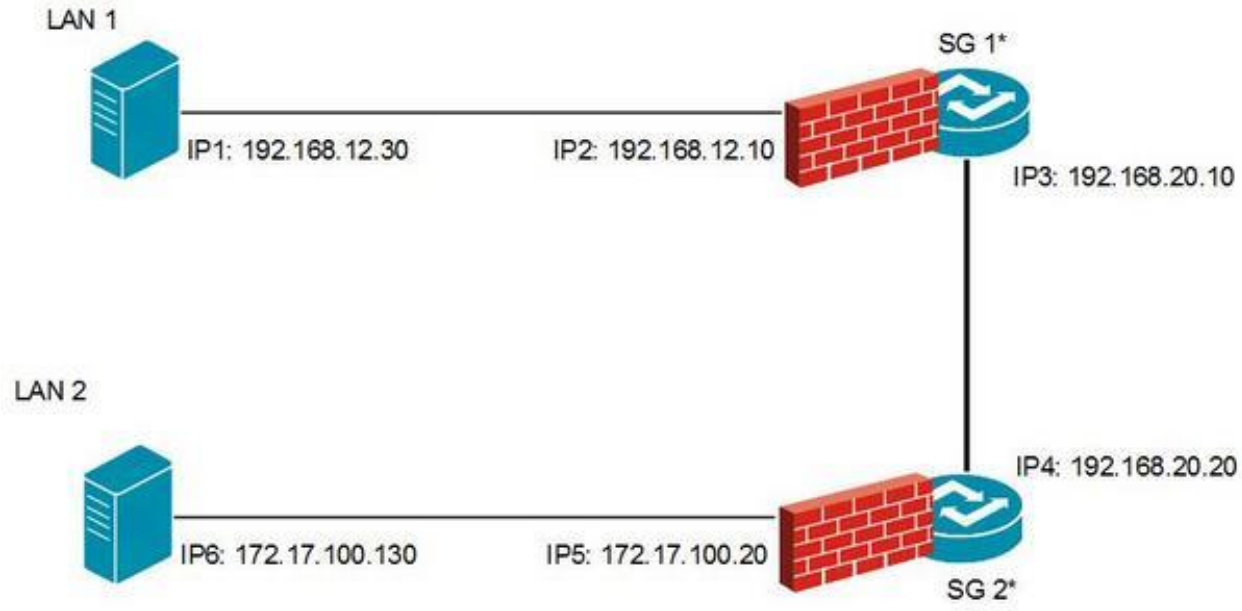

Рисунок 5.4 – Топологія мережі: VPN між двома локальними мережами

У цьому випадку, як правило, використовується тільки тунельний режим. При цьому заголовки в пакеті між SG1 і SG2 будуть виглядати в такий спосіб:

Тунельний режим
[src:IP3; dst:IP4] [ESP] [src: IP1; dst:IP6] [upper]

Рисунок 5.5 – Вкладеність заголовків при створенні VPN між двома локальними мережами

У даній топології хости в локальних мережах не підтримують IPSec, і, як наслідок, трафік у локальних мережах не захищений від внутрішніх (insider) атак. Трафік у публічній мережі захищений. IP-адреси хостів у локальній мережі не видні в публічній мережі.

Варіант 3. Створення безпечного з'єднання між двома хостами з можливістю часткового аналізу й фільтрування трафіку на шлюзах безпеки.

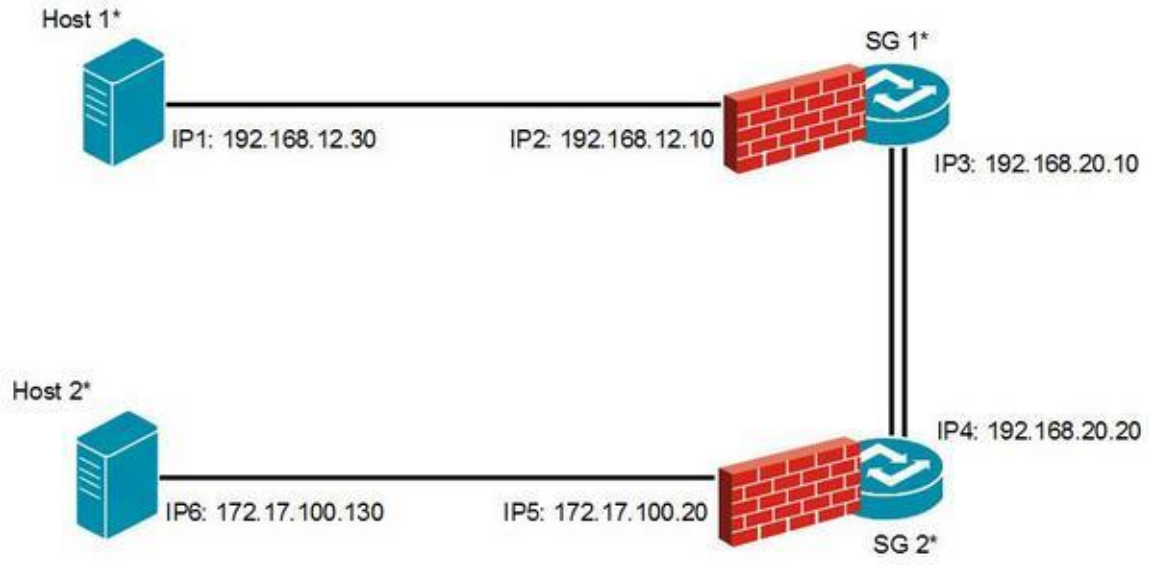

Рисунок 5.6 – Топологія мережі: VPN з можливістю аналізу трафіку на шлюзі безпеки

Створюються дві вкладені SA. Одна між хостами Host 1 і Host 2, інша між шлюзами безпеки SG 1 і SG 2. У цьому випадку трафік буде захищений як у публічній, так і в локальній мережах, і шлюзи безпеки

зможуть частково аналізувати й фільтрувати трафік, переданий і з локальних мереж.

На шлюзах безпеки повинен використовуватися тунельний режим. На хостах треба використовувати транспортний режим.

Варіант 4. Безпечне підключення віддаленого користувача до локальної мережі організації з можливістю часткового аналізу й фільтрування трафіку на шлюзі безпеки (рисунок 5.7).

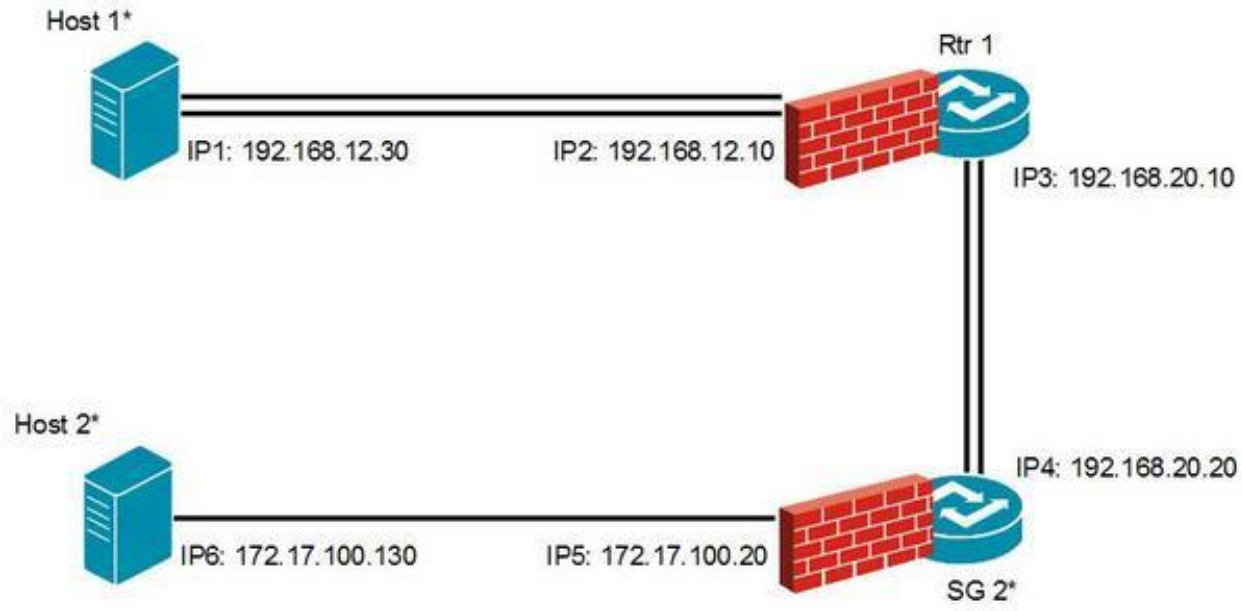

Рисунок 5.7 – Топологія мережі: захищений доступ користувача в локальну мережу

У цьому випадку створюються дві вкладені SA: одна між віддаленим хостом Host 1 і хостом у локальній мережі Host 2 (SA 1), друга між віддаленим хостом Host 1 і шлюзом безпеки SG 2 (SA 2). У результаті трафік захищений як в Інтернеті (SA 2), так і в локальній мережі (SA 1). Віддалений хост (Host 1) використовує Інтернет для досягнення міжмережевого екрана організації (SG 2) і потім одержує доступ до деякого хосту (Host 2) у локальній мережі. Між Host 1 і SG 2

використовується режим тунелювання. Для SA між SG 2 і Host 2 можливий як транспортний, так і тунельний режими.

У даній топології кінцева точка, яка захищається (звичайно портативний переносний комп'ютер) з'єднується зі своєю корпоративною мережею через IPSec-тунель. Кінцева точка використовує даний тунель для доступу в корпоративну мережу, після цього трафік може тунелюватися через локальну мережу, щоб захистити його й у локальній мережі. У цьому випадку існує можливість фільтрування трафіку корпоративним міжмережевим екраном. Кінцева точка повинна мати IP-адресу, відому міжмережевому екрану, щоб він міг пропускати пакети через міжмережевий екран і тунелювати їх далі. Дана IP-адреса може бути статичною або може задаватися динамічно якою-небудь із технологій, аналогічних DHCP. Для підтримки другого варіанта існує механізм, що дає можливість Ініціаторові запитувати IP-адресу, що належить міжмережевому екрану для використання з SA, створюваної в локальній мережі.

Інші топології

Можливі також інші топології. Наприклад, можливе використання разом з IPSec інших протоколів тунелювання, таких як GRE або L2TP.

Ступінь деталізації керування трафіком

IPSec дозволяє управляти деталізацією, з якої надається сервіс безпеки. Наприклад, можна створити єдиний зашифрований тунель між двома локальними мережами, або для кожного TCP- і UDP-з'єднання може бути створений окремий зашифрований тунель між парою хостів. IPSec, що дозволяє вказувати наступні параметри:

– Необхідний рівень деталізації застосовуваного захисту. Варто відмітити, що сильно деталізовані SA звичайно є більше уразливими для аналізу трафіку, чим слабко деталізовані.

Рисунок 5.8 – Приклад веб-інтерфейсу для вказівки ступеня деталізації створення SA

– Використовувані алгоритми в протоколах забезпечення безпеки IP-трафіку.

Рисунок 5.9 – Приклад веб-інтерфейсу для вказівки необхідних алгоритмів у протоколах захисту трафіку

– Використовувані алгоритми в протоколах керування SA.

Рисунок 5.10 – Приклад веб-інтерфейсу для вказівки необхідних алгоритмів у протоколах керування SA

Протокол ESP

Протокол ESP розроблений для забезпечення можливості використання декількох сервісів безпеки в IPv4 і IPv6.

ESP-заголовок вставляється після IP-заголовка й перед заголовком протоколу більш високого рівня (транспортний режим) або перед інкапсульованим IP-заголовком (тунельний режим).

ESP використовується для забезпечення конфіденційності, автентифікації даних, цілісності з'єднання й анти-replay сервісу (забезпечення цілісності деякої послідовності дейтаграм).

Формат пакета ESP

Заголовок протоколу (IPv4, IPv6 або Extension), безпосередньо попередній ESP, містить значення 50 у поле Protocol (IPv4) або Next Header (IPv6, Extension).

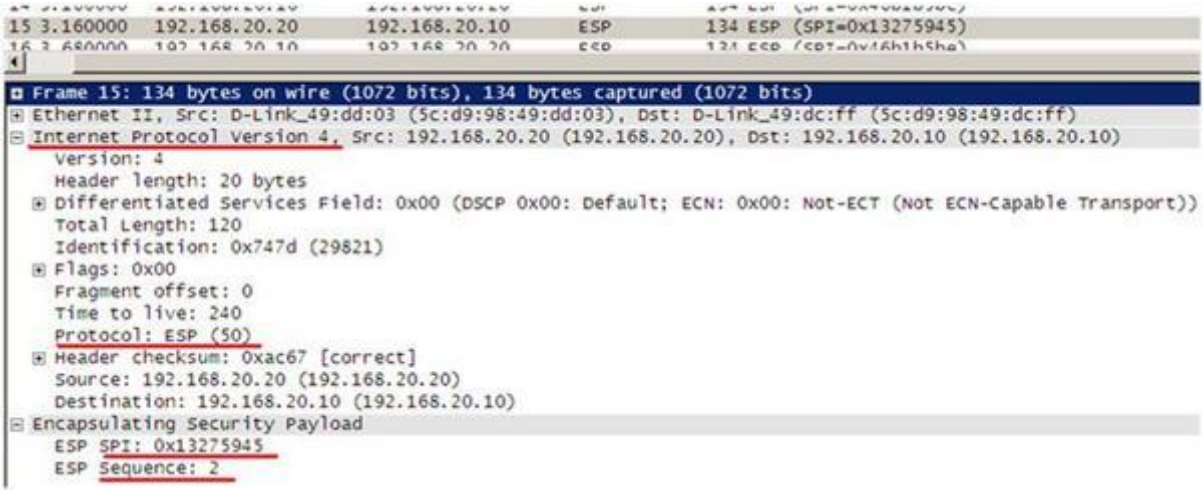

Рисунок 5.11. Приклад вкладеності ESP-пакета

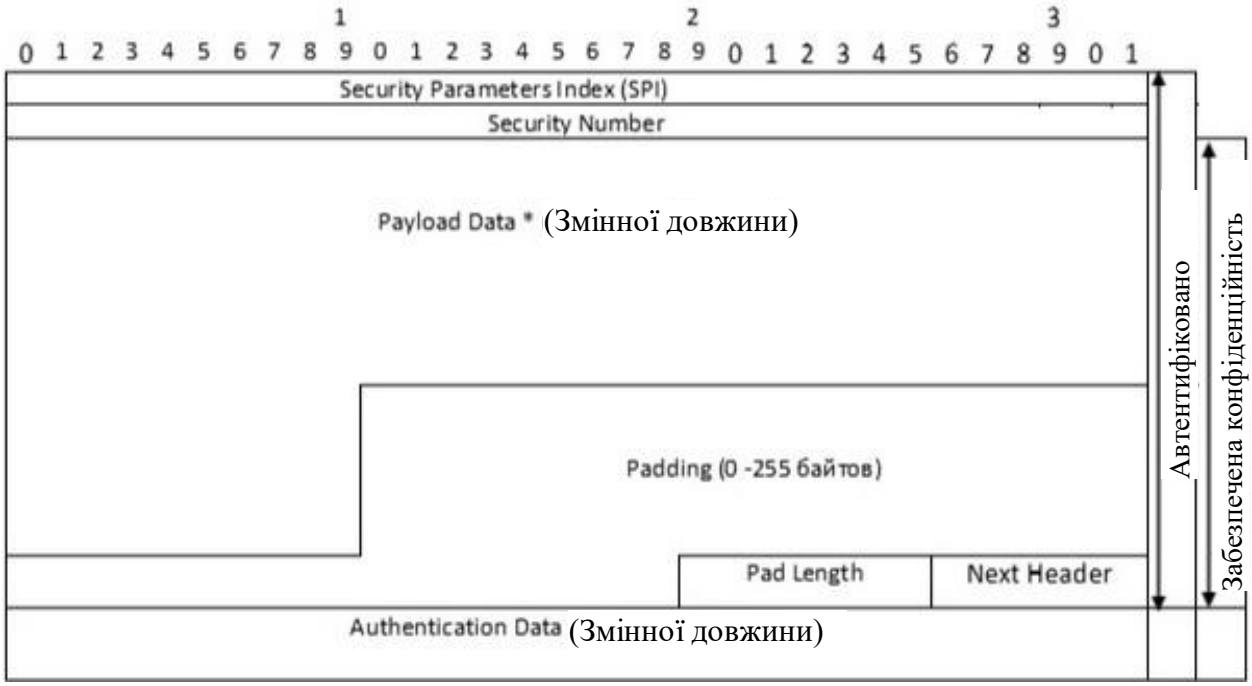

Рисунок 5.12 – Формат ESP-пакета

Дані (Payload Data)

Payload Data є полем змінної довжини, що містить дані протоколу, розташованого вище в стеці, що зазначений у поле Next Header. Довжина даного поля дорівнює цілому числу байтів. Якщо алгоритм, використовуваний для шифрування, вимагає криптографічно-синхронізованих даних, наприклад ініціалізаційний вектор IV, то ці дані також утримуються в цьому полі.

Додавання (Padding)

Використання поля Padding пояснюється декількома факторами.

– Якщо використовуваний алгоритм шифрування вимагає, щоб незашифрований текст був кратний визначеній кількості байтів, наприклад, розміру блоку для блокових алгоритмів, то поле Padding використовується для доповнення незашифрованих даних (що складаються з полів Payload Data, Pad Length і Next Header) до розміру, необхідного алгоритмом.

– Додавання може також вимагатися незалежно від алгоритму шифрування для гарантування того, що отримані зашифровані дані завершуються на 4-байтої границі. Поля Pad Length і Next Header повинні бути в такий спосіб розташовані в 4-байтному слові, щоб гарантувати, що поле Authentication Data прив'язане до 4-байтної границі.

– Додавання може бути використане для маскування реальної довжини вмісту для забезпечення конфіденційності потоку трафіку. Однак варто розуміти, що використання такого додавання збільшує трафік.

Довжина додавання (Pad Length)

Поле Pad Length вказує число байтів додавання, які безпосередньо випливають за ним.

Наступний заголовок (Next Header)

Next Header є 8-бітовим полем, що вказує тип даних, які знаходяться в поле Payload Data, наприклад, заголовок Extension в IPv6 або ідентифікатор протоколу більш високого рівня. Значення даного поля вибирається з безлічі IP Protocol Number, обумовленого IANA.

Автентифікаційні дані (Authentication Data)

Authentication Data є полем змінної довжини, що містить значення перевірки цілісності (Integrity Check Value – ICV), обчислене для ESP-пакета, за винятком самого поля Authentication Data. Довжина поля визначається обраним алгоритмом автентифікації. Поле Authentication Data є необов'язковим і включається в тому випадку, якщо використовується сервіс автентифікації.

Обробка трафіку, виконувана ESP

Розглянемо розташування заголовка ESP щодо заголовків інших протоколів.

Протокол ESP може використовуватися у двох режимах: у транспортному режимі й тунельному. Перший режим застосовується в основному для створення VPN між двома хостами й забезпечує захист для протоколів більш високого рівня, але не для заголовка IP. Відмітимо, що в даному режимі для "in-the-stack" і "in-the-wire" реалізацій може знадобитися реасемблювання вхідних і вихідних IP-фрагментів.

У транспортному режимі ESP-заголовок розташований після IP-заголовка й перед заголовком протоколу більш високого рівня, наприклад, TCP, UDP, ICMP і т.д. Наступні рисунки показують додавання заголовків у транспортному режимі ESP для типового IPv4 пакети.

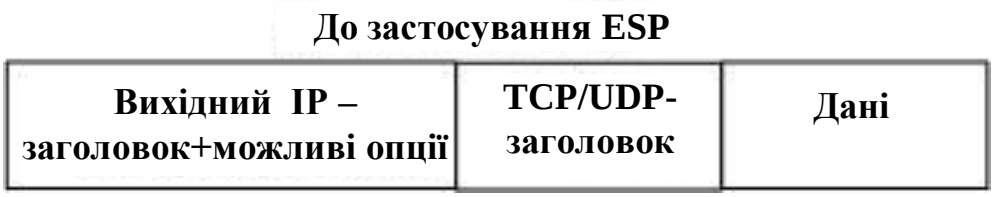

Рисунок 5.13 – Вкладеність заголовків до застосування ESP у транспортному режимі в IPv4

Рисунок 5.14 – Вкладеність заголовків після застосування ESP у транспортному режимі в IPv4

У протоколі IPv6 ESP розглядається як end-to-end вміст, і в такий спосіб він повиннен з'являтися після hop-by-hop, routing і fragmentation заголовків розширення. Заголовки параметрів призначення можуть з'являтися як до, так і після ESP заголовка, залежно від необхідної семантики. Однак, тому що ESP захищає тільки поля після ESP-заголовка, звичайно потрібне розміщення заголовків опцій призначення після ESP-заголовка. Наступні рисунки ілюструють додавання заголовків у транспортному режимі ESP для типового IPv 6-пакета.

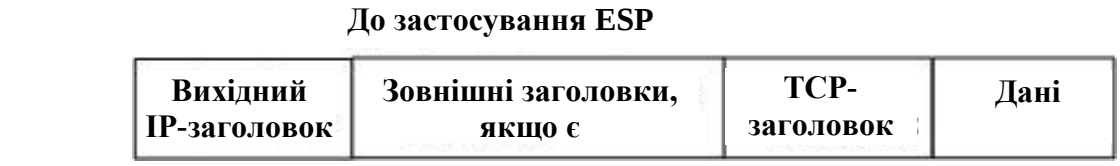

Рисунок 5.15 – Вкладеність заголовків до застосування ESP у транспортному режимі в IPv6

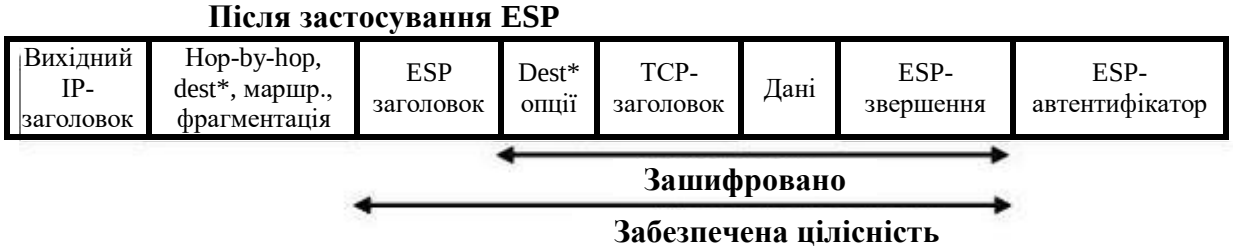

Рисунок 5.16 – Вкладеність заголовків після застосування ESP у транспортному режимі в IPv6

Тунельний режим ESP може бути реалізований як на хостах, так і на шлюзах безпеки. При використанні ESP на шлюзі безпеки для захисту транзитного трафіку повинен застосовуватися тунельний режим. У тунельному режимі внутрішній IP-заголовок містить кінцеві адреси джерела й одержувача, а зовнішній IP-заголовок містить IP-адреси шлюзів безпеки. У тунельному режимі ESP захищає весь внутрішній IP-пакет, включаючи весь внутрішній IP-заголовок. Розташування ESP у тунельному

режимі щодо зовнішнього IP-заголовка є тим самим, що й для транспортного режиму. Наступні рисунки ілюструють додавання заголовків у тунельному режимі ESP для типових IPv 4- і IPv 6-пакетів.

Рисунок 5.15 – Вкладеність заголовків після застосування ESP у тунельному режимі в IPv4

Рисунок 5.18 – Вкладеність заголовків після застосування ESP у тунельному режимі в IPv6

Алгоритми

Визначено алгоритми, обов'язкові для реалізації. Крім них додатково можуть бути реалізовані й інші алгоритми.

1. Алгоритми шифрування

Алгоритми шифрування визначаються при створенні SA і застосовуються для шифрування даних, переданих по SA. У протоколі ESP використовуються симетричні алгоритми шифрування. Тому що IP-пакети можуть приходити в будь-якому порядку, кожний пакет повинен містити всю інформацію, необхідну Одержувачеві для розшифрування. Ці дані,

наприклад ініціалізаційний вектор (IV), можуть передаватися явно в поле вмісту або вони можуть бути отримані із заголовка пакета.

2. Алгоритми автентифікації (забезпечення цілісності)

Алгоритм автентифікації, використовуваний для обчислення Integrity Check Value (ICV), визначається при створенні SA. Для обчислень точка-точка відповідні алгоритми автентифікації використовують MAC із ключем, заснованим на симетричних алгоритмах шифрування (наприклад, DES) або на однобічних геш-функціях (наприклад, MD5 або SHA-1). Для багатоадресних з'єднань однобічні геш-функції використовуються разом з асиметричними алгоритмами створення цифрового підпису.

Обробка вихідного пакета

У транспортному режимі Відправник інкапсулює інформацію протоколу верхнього рівня в ESP-заголовок і зберігає без зміни IP-заголовок (і будь-які IP-заголовки розширення в протоколі IPv6). У тунельному режимі зовнішні й внутрішній IP-заголовки можуть по-різному співвідноситися один з одним.

1. Пошук підходящої SA

ESP застосовується до вихідного пакета після того, як визначено, який SA належить пакет.

2. Шифрування пакета

Відправник виконує наступні дії:

– Інкапсуляція в поле ESP Payload:

– Для транспортного режиму – тільки вихідна інформація протоколу верхнього рівня.

– Для тунельного режиму – вся вихідна IP-дейтаграма.

– Додавання необхідного доповнення (поле Padding).

– Шифрування отриманих даних (Payload Data, Padding, Pad Length, Next Header), використовуючи ключ, алгоритм шифрування, режим алгоритму, зазначені в SA.

Першим виконується шифрування, потім виконується автентифікація (забезпечення цілісності), тому поле Authentication Data не зашифроване. Такий порядок обробки дає можливість Одержувачеві швидко виявити й відкинути повторні або фіктивні пакети, що потенційно знижує ймовірність успішного виконання DoS-атак. Це також допускає можливість паралельної обробки пакетів Одержувачем, наприклад, розшифрування може виконуватися одночасно з перевіркою цілісності. Відмітимо, що, тому що Authentication Data не захищено шифруванням, для обчислення ICV повинен застосовуватися алгоритм забезпечення цілісності із ключем.

3. Обчислення Sequence Number

Перший пакет, що посилається по заново створеної SA, має Sequence Number, рівний 1.

Якщо використовується анти-replay сервіс, відправник перевіряє, що значення лічильника не переповнилося перед створенням нового значення в поле Sequence Number. Інакше кажучи, відправник не повинен посилати пакет по SA, якщо виникає переповнення Sequence Number.

Відправник повторює пакет, якщо він не одержав повідомлення про його одержання. Якщо лічильник переповнився, відправник повинен установити нову SA і обчислити нові ключі.

4. Обчислення значення перевірки цілісності

Якщо для SA потрібно забезпечення цілісності, Відправник обчислює ICV для всього ESP-пакета, за винятком поля Authentication Data. Таким чином, для полів SPI, Sequence Number, Payload Data, Padding(якщо є присутнім) і Next Header обчислюється ICV. Відмітимо, що останні чотири поля є зашифрованими, тому що шифрування виконується до обчислення ICV.

Для деяких алгоритмів забезпечення цілісності рядок байтів, для якої обчислюється ICV, повинен бути кратним довжині блоку обраного алгоритму. Якщо довжина даного рядка байтів не відповідає необхідній

довжині блоку, то повинно виконуватися додавання в кінець ESP-пакета (після поля Next Header) до обчислення ICV. Октети додавання повинні мати нульові значення. Довжина блоку (і, отже, довжина додавання) визначаються зі специфікації алгоритму. Дане додавання не передається разом з пакетом.

5. Фрагментація

Після описаних вище ESP-перетворень при необхідності може виконуватися фрагментація пакета. Таким чином, транспортний режим ESP застосовується тільки до цілих IP-дейтаграмам (не до фрагментів IP). Вхідний IP-пакет, для якого повинно виконуватися ESP-перетворення, може сам бути фрагментований маршрутизаторами, і в такий спосіб фрагменти повинні реасемблюватися перед ESP-перетворенням на стороні Одержувача.

Для транспортного режиму in-the-stack і in-the-wire реалізації можуть, по-перше, реасемблювати пакет, фрагментований локальним IP-рівнем, потім застосовувати IPSec і потім знову фрагментувати пакет, який отримався.

Обробка вхідного пакета

Реасемблювання

Якщо потрібно реасемблювання, то воно виконується до ESP-Обробки.

Пошук підходящої SA

При одержанні пакета, що містить ESP-заголовок, Одержувач визначає підходящу односпрямовану SA, переглядаючи SAD. Для одноадресних SA це визначається на основі значення SPI у заголовку. У записі SAD зазначено, чи варто перевіряти послідовний номер. Також у записі SAD зазначені алгоритми й ключі, використовувані для розшифрування.

Якщо для даного пакета не існує SA, Одержувач відкидає пакет. У цьому випадку дана подія записується в поле із вказівкою SPI, дати й часу

одержання, адрес відправника й одержувача, послідовного номера й, можливо, іншої інформації.

Відмітимо, що трафік керування SA, такий як IKE-пакети, не ідентифікуються SPI.

Перевірка послідовного номера

В основі анти-replay сервісу лежить перевірка коректного значення послідовного номера. Одержувач перевіряє, чи пакет містить послідовний номер, що не є дублікатом послідовного номера іншого пакета, отриманого в даної SA. Така перевірка виконується першою, після того як знайдена відповідна SA, щоб якнайшвидше відкинути дублюючі пакети.

РОЗДІЛ 6. ПРОТОКОЛ SSL/TLS

SSL (англ. Secure Sockets Layer – рівень захищених сокетів) – криптографічний протокол, що має на увазі більш безпечний зв'язок. Він використовує асиметричну криптографію для автентифікації ключів обміну, симетричне шифрування для збереження конфіденційності, коди автентифікації повідомлень для цілісності повідомлень. Протокол широко використовувався для обміну миттєвими повідомленнями й передачі голосу через IP (англ. Voice over IP – VoIP), у таких додатках, як електронна пошта, Інтернет-Факс та інше. У цей час відомо, що протокол не є безпечним. ***SSL повинен бути виключений з роботи на користь TLS*** (див. CVE-2014-3566).

SSL споконвічно розроблений компанією Netscape Communications для додавання протоколу HTTPS у свій веб-браузер Netscape Navigator. ***Згодом, на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що одержав ім'я TLS.***

TLS (англ. Transport Layer Security) – безпека транспортного рівня, як і його попередник SSL (англ. Secure Sockets Layer – рівень захищених сокетів) – криптографічні протоколи, що забезпечують захищену передачу даних між вузлами в мережі Інтернет. TLS і SSL використовують:

– асиметричну криптографію для автентифікації;

– симетричне шифрування для конфіденційності;

– коди автентичності повідомлень для збереження цілісності повідомлень.

Даний протокол широко використовується в додатках, що працюють із мережею Інтернет, таких як веб-браузери, робота з електронною поштою, обмін миттєвими повідомленнями й IP-телефонія (VoIP).

TLS-протокол заснований на специфікації протоколу SSL версії 3.0, розробленою компанією Netscape Communications. Зараз розвитком стандарту TLS займається IETF. Розходження між даним протоколом і SSL 3.0 несуттєві, але важливо помітити, що ***TLS 1.0 і SSL 3.0 несумісні***, хоча в TLS 1.0 передбачений механізм, що дозволяє TLS мати зворотну сумісність із SSL 3.0.

Основна функція протоколу SSL/TLS складається в забезпеченні конфіденційності й цілісності даних прикладного рівня, переданих між двома взаємодіючими додатками, один з яких є клієнтом, а інший – сервером.

Перелічимо завдання протоколу SSL/TLS у порядку їхнього пріоритету:

1. ***Криптографічна безпека:*** SSL/TLS повинен використовуватися для встановлення криптографічно безпечного з'єднання між двома учасниками.

2. ***Інтероперабельність:*** незалежні розроблювачі повинні мати можливість створювати додатки, які будуть взаємодіяти за протоколом SSL/TLS, що дозволить установлювати безпечні з'єднання.

3. ***Розширюваність:*** SSL/TLS визначає загальний каркас, у який можуть бути вбудовані нові алгоритми відкритого ключа й симетричного шифрування. Це рятує від необхідності створювати новий протокол для використання нових алгоритмів, що сполучено з небезпекою появи нових слабких місць, і виключає необхідність повністю реалізовувати нову бібліотеку криптографічних алгоритмів.

4. ***Відносна ефективність:*** криптографічні операції інтенсивно використовують ЦП, особливо операції з відкритим ключем. Для зменшення обчислювального навантаження вводиться поняття сесії, у рамках якої може бути створене декілька TCP-з'єднань. SSL/TLS дозволяє кешувати параметри сесії для зменшення кількості виконуваних

криптографічних операцій при встановленні з'єднання. Це знижує навантаження як на ЦП, так і на трафік.

Протокол складається із двох рівнів. Нижнім рівнем, розташованим вище деякого надійного протоколу (а саме, протоколу TCP) є ***протокол Запису.*** Протокол Запису забезпечує безпеку з'єднання, що заснована на наступних двох властивостях:

– ***Конфіденційність з'єднання.*** Для захисту даних використовується один з алгоритмів симетричного шифрування. Ключ для цього алгоритму створюється для кожної сесії й заснований на секреті, про який домовляються в протоколі Рукостискання. Протокол Запису також може використовуватися без шифрування.

– ***Цілісність з'єднання.*** Забезпечується перевірка цілісності повідомлення за допомогою MAC із ключем. Для обчислення MAC використовуються геш-функції SHA-1 і MD5. Протокол Запису може виконуватися без обчислення MAC.

Протокол Запису використовується для інкапсуляції різних протоколів більш високого рівня. Одним із протоколів більш високого рівня є протокол Рукостискання, що використовує протокол Запису як транспорт для ведення переговорів про параметри безпеки. Протокол Рукостискання дозволяє серверу й клієнтові автентифікувати один одного й домовитися про алгоритми шифрування й криптографічних ключів до того, як прикладний протокол, що виконується на тому ж рівні, почне передавати або приймати перші байти даних.

Протокол Рукостискання забезпечує безпеку з'єднання, що заснована на наступних властивостях:

1. Учасники автентифіковані з використанням криптографії з відкритим ключем (тобто з використанням алгоритмів RSA, DSS і т.д.). Ця автентифікація може бути необов'язковою, але звичайно потрібна принаймні для сервера.

2. Перемовини про поділюваний секрет безпечні, тобто цей загальний секрет неможливо підглянути.

3. Перемовини про поділюваний секрет надійні, якщо виконано автентифікація хоча б однієї зі сторін. У такому випадку атакуючий, розташований у середині з'єднання, не може модифікувати переданий секрет непомітно для учасників з'єднання.

Одна з переваг TLS полягає в тому, що він незалежний від прикладного протоколу.

Визначено наступні криптографічні операції:

– цифровий підпис;

– блокове шифрування;

– шифрування з відкритим ключем.

При блоковому шифруванні кожний блок незашифрованого тексту шифрується, у результаті чого створюється блок зашифрованого тексту. Всі алгоритми блокового шифрування виконуються в режимі CBC, і довжина всіх шифруємих елементів повинна бути кратна довжині блоку алгоритму шифрування.

Протокол Запису

Протокол Запису складається з декількох рівнів. Протокол Запису фрагментує повідомлення на блоки потрібної довжини, здійснює стиск даних, обчислює HMAC і зашифровує їх. На іншому кінці з'єднання отримані дані розшифровуються, перевіряється їхня цілісність, далі вони декомпрессуються, дефрагментуються й передаються протоколам більш високого рівня.

Вище протоколу Запису можуть розташовуватися наступні протоколи:

– протокол Рукостискання;

– Alert-протокол;

– протокол зміни шифрування;

– прикладний протокол, безпека якого забезпечується.

Стан з'єднання

У протоколі вводиться поняття стану з'єднання, що визначає параметри виконання протоколу Запису. Такими параметрами є:

– алгоритм стиску;

– алгоритм шифрування;

– MAC-алгоритм;

– параметри цих алгоритмів, тобто секрети MAC, ключі алгоритму шифрування й ініціалізаційні вектора.

Для кожного напрямку (відповідно читання або запис) параметри з'єднання можуть розрізнятися.

Існує чотири стани з'єднання:

– поточні стани читання й запису;

– очікувані стани читання й запису.

Параметри безпеки для очікуваних станів встановлюються протоколом Рукостискання, а протокол зміни шифрування робить очікуваний стан поточним, у результаті чого відповідні параметри поточного стану скидаються й заміняються параметрами очікуваного стану. Параметри очікуваного стану ініціалізуються порожніми значеннями. Початковий поточний стан завжди визначається без використання шифрування, стиску й MAC.

Визначено наступні параметри стану:

Таблиця 6.1.

Кінець з'єднання	Кожний учасник є або "клієнтом", або "сервером"
Алгоритм симетричного шифрування	Алгоритм, що використовується для симетричного шифрування, і його параметри – довжина ключа алгоритму, довжина блоку алгоритму, ключ шифрування, ініціалізаційний вектор (IV) і ін.

Продовження таблиці 6.1.

MAC алгоритм	Алгоритм, що використовується для перевірки цілісності повідомлення, секрет MAC.
Алгоритм стискування	Алгоритм, що використовується для стискання даних.
Майстер-Секрет	48-байтний секрет, поділюваний обома учасниками з'єднання.
Випадкове число клієнта SecurityParameters.client_random	32-байтне значення, створюване клієнтом у протоколі Рукостискання.
Випадкове число сервера SecurityParameters.server_random	32-байтне значення, створюване сервером у протоколі Рукостискання.
Послідовний номер	Кожний стан з'єднання містить послідовний номер, що обчислюється незалежно для станів читання й запису. Послідовний номер повинен установлюватися в нуль при ініціалізації стану. Послідовні номери не можуть бути більше $2^{64} – 1$. Послідовний номер зростає після створення чергового запису.

З майстер-секрету створюються шість ключів:

– client write MAC secret;

– server write MAC secret;

– client write key;

– server write key;

– client write IV;

– server write IV.

Ключі client write використовуються сервером, коли він одержує повідомлення й клієнтом, коли той посилає їх. Ключі server write використовуються сервером, коли він посилає повідомлення й клієнтом, коли він одержує їх. Після того як параметри безпеки встановлені й ключі створені, очікувані стани з'єднання робляться поточними.

Обчислення ключів

Протокол Запису використовує наступний алгоритм для створення ключів, ініціалізаційних векторів і секретів MAC із параметрів безпеки, створюваних протоколом Рукостискання.

HMAC і псевдовипадкова функція

Для забезпечення цілісності використовується HMAC із геш-функціями MD5 і SHA-1, позначуваними як:

– HMAC_MD5 (secret,data);

– HMAC_SHA (secret, data).

В алгоритмі визначена псевдовипадкова функція PRF, що розширює секрет до потрібної довжини для створення всіх необхідних ключів. Ця функція одержує як вхід секрет, "зерно" (seed – значення, що з однієї сторони є випадковим, а з іншої сторони не є секретним, тобто може стати відомо опонентові) та стандартне значення, і створює вихід необхідної довжини.

Спочатку визначається функція розширення даних P_hash (secret, data), що використовує геш-функцію для розширення секрету до потрібної довжини в такий спосіб:

P_hash (secret, seed) = HMAC_hash (secret, A(1) || seed) ||

HMAC_hash (secret, A(2) || seed) || HMAC_hash (secret, A(3) || seed) ||,

де A (i) визначається в такий спосіб:

A (0) = seed

A (i) = HMAC_hash (secret, A (i – 1))

P_hash може мати стільки ітерацій, скільки необхідно для створення даних необхідної довжини. Наприклад, якщо P_ SHA-1 використовується

для створення 64 байтів даних, то кількість ітерацій повинне бути дорівнює 4, при цьому буде створено 80 байтів даних; останні 16 байтів заключної ітерації будуть відкинуті, щоб залишити тільки 64 байта вихідних даних.

Для одержання ключового матеріалу потрібної довжини секрет, обчислений у протоколі Рукостискання, ділиться на дві половини, одна половина використовується для створення даних за допомогою P_MD5, а інша – для створення даних за допомогою P_ SHA-1.

PRF визначається як результат додавання по модулі 2 результатів виконання P_MD5 і P_ SHA-1.

PRF (secret, label, seed) = P_MD5 (S1, label + seed)

P_ SHA-1 (S2, label + seed),

де Label є фіксованим текстовим рядком.

Відмітимо, що оскільки MD5 створює 16-байтні значення, а SHA-1 створює 20-байтні значення, то кількість ітерацій кожної з функцій буде різним. Наприклад, для створення 80-байтного значення необхідно виконати 5 ітерацій P_MD5 і 4 ітерації P_ SHA-1.

Для створення ключів обчислюється наступне значення:

key_block = PRF (SecurityParameters.master_secret, "key expansion",

SecurityParameters.server_random + SecurityParameters.client_random), де кількість ітерація в PRF визначається сумарною довжиною ключів. Потім key_block розбивається на блоки для одержання необхідних ключів.

Протокол Рукостискання

Протокол Рукостискання складається із трьох підпротоколів, використання яких дозволяє учасникам погодити криптографічні алгоритми, автентифікувати один одного, і повідомити один одному про виникнення тих або інших помилок.

У результаті виконання протоколу Рукостискання будуть створені наступні елементи сесії:

Таблиця 6.2.

Ідентифікатор сесії	Довільна послідовність байтів, обирана сервером для ідентифікації активного або поновлюваного стану сесії.
Сертифікат учасника	X.509 v3 сертифікат учасника. Цей елемент може бути нульовим.
Метод стиску	Алгоритм, використовуваний для стиску даних перед шифруванням.
Набір алгоритмів	Алгоритм симетричного шифрування даних (наприклад, NULL, DES, AES і т.д.), MAC-алгоритм (такий як MD5 або SHA-1) і параметри цих алгоритмів.
Майстер-Секрет	48-байтний секрет, поділюваний клієнтом і сервером.
Поновлювано	Прапор, що визначає, чи може дана сесія використовуватися для створення нового TCP-з'єднання.

Протокол зміни шифрування

Протокол складається з єдиного повідомлення, що зашифроване й стисле, як визначено в поточному стані з'єднання.

Повідомлення про зміну шифрування посилається як клієнтом, так і сервером для повідомлення протилежної сторони про те, що наступні записи будуть захищені алгоритмами й ключами, про які сторони тільки що домовилися. При одержанні даного повідомлення протокол Запису копіює очікуваний стан читання в поточний стан читання. Відразу після посилання даного повідомлення відправник копіює очікуваний стан запису в поточний стан запису. Повідомлення про зміну шифрування посилається при Рукостисканні після того, як параметри безпеки погоджені, але перед тим як посилається заключне веріфікуюче повідомлення.

Alert-протокол

Одним із протоколів, що виконуються вище протоколу Запису, є протокол Alert. Умістом протоколу є або фатальне, або попереджуюче повідомлення. Фатальне повідомлення повинне приводити до негайного розриву даного TCP-з'єднання. У цьому випадку інші з'єднання, що відповідають даної сесії, можуть бути продовжені, але ідентифікатор сесії повинен бути позначений як недійсний для запобігання використання даної сесії для встановлення нових з'єднань. Подібно іншим повідомленням, повідомлення Alert зашифровані й стислі, як визначено в поточному стані з'єднання.

Протокол Рукостискання

Криптографічні параметри сесії створюються протоколом Рукостискання, що виконується вище протоколу Запису. Коли клієнт і сервер починають взаємодіяти, вони погоджують версію протоколу, вибирають криптографічні алгоритми, можуть автентифікувати один одного, використовуючи технологію з відкритим ключем. Для створення поділюваного секрету також використовується технологія з відкритим ключем.

Протокол Рукостискання складається з наступних кроків:

1. Обмін повідомленнями Hello для узгодження алгоритмів, обміну випадковими значеннями й перевірки поновлюємості сесії.

2. Обмін необхідними криптографічними параметрами, які дозволяють клієнтові й серверу погодити премайстер-секрет.

3. Обмін сертифікатами й криптографічною інформацією, що дозволяє клієнтові й серверу автентифікувати один одного.

4. Надання параметрів безпеки на рівень Запису.

5. Можливість клієнтові й серверу перевірити, що вони обчислили ті самі параметри безпеки й що Рукостискання відбулося без втручання зловмисника.

Протокол розроблений для мінімізації ризику атак "зустріч посередині", але захист від атак, при яких зловмисник може блокувати доступ до порту, не передбачуваний.

Клієнт посилає повідомлення ClientHello, на яке сервер повинен відповісти повідомленням ServerHello або фатальною помилкою й розривом з'єднання. ClientHello і ServerHello використовуються для визначення максимального рівня безпеки між клієнтом і сервером.

Client Hello і Server Hello установлюють наступні атрибути: Protocol Version, Session ID, Cipher Suite і Compression Method. Додатково створюються й передаються два випадкових значення: ClientHello.random і ServerHello.random.

Автентифікація й обмін загальним секретом здійснюються в чотирьох повідомленнях: сертифікат сервера, обмін ключа сервера, сертифікат клієнта й обмін ключа клієнта. Загальний секрет повинен бути досить великим; поточні методи розподілу ключа обмінюються секретами, довжина яких перебуває в діапазоні від 48 до 126 байт.

Після повідомлень Hello сервер посилає сертифікат, за допомогою якого клієнт виконує автентифікацію сервера. Додатково може бути відправлено повідомлення обміну ключа сервера, якщо сервер не має сертифіката або його сертифікат може використовуватися тільки для перевірки підпису. Якщо сервер автефікований, він може запросити сертифікат клієнта, якщо того вимагає встановлена політика безпеки на стороні сервера. Після цього сервер посилає повідомлення Server Hello Done, що вказує на те, що фаза Hello-повідомлень рукостискання завершена. Потім сервер чекає відповіді клієнта. Якщо сервер послав повідомлення запиту сертифіката, клієнт повинен послати повідомлення Certificate. Після цього посилає повідомлення обміну ключа клієнта. Вміст цього повідомлення залежить від обраного алгоритму, що вироблено для загального секрету. Якщо клієнт посилав свій сертифікат, то він посилає

повідомлення, що містить цифровий підпис для перевірки всіх повідомлень Рукостискання.

У даній точці клієнтом посилається повідомлення про зміну стану, і клієнт копіює очікуваний стан у поточний стан. Після цього клієнт посилає заключне повідомлення з використанням нових алгоритмом, ключів і секретів. У відповідь сервер посилає своє повідомлення про зміну стану, перетворює очікуваний стан у поточний стан і посилає заключне повідомлення з використанням нових алгоритмів і ключів. Після цього рукостискання вважається виконаним, і клієнт і сервер можуть починати обмін даними прикладного рівня.

*** вказує на необов'язкові або ті, що залежать від ситуації повідомлення, які посилаються не завжди**

Рисунок 6.1 – Послідовність повідомлень при повному Рукостисканні

Коли клієнт і сервер вирішують відновити попередню сесію або дублювати існуючу (замість того щоб вести нові перемовини про параметри безпеки), виконується так зване скорочене рукостискання:

– Клієнт посилає Client Hello, використовуючи Session ID поновлюваної сесії.

– Сервер шукає відповідний ідентифікатор сесії у своєму кеші сесій. Якщо ідентифікатор існує, і сесія позначена як поновлювана, сервер установлює з'єднання з параметрами зазначеної сесії, після чого посилає Server Hello із цим значенням Session ID. Якщо відповідний Session ID не знайдений, сервер створює новий ID сесії, і клієнт і сервер виконують повне рукостискання.

– Після цього й клієнт, і сервер повинні послати повідомлення про зміну стану, потім відразу послати завершальні повідомлення.

– І клієнт, і сервер починають обмін даними прикладного рівня.

Потік повідомлень при скороченому Рукостисканні

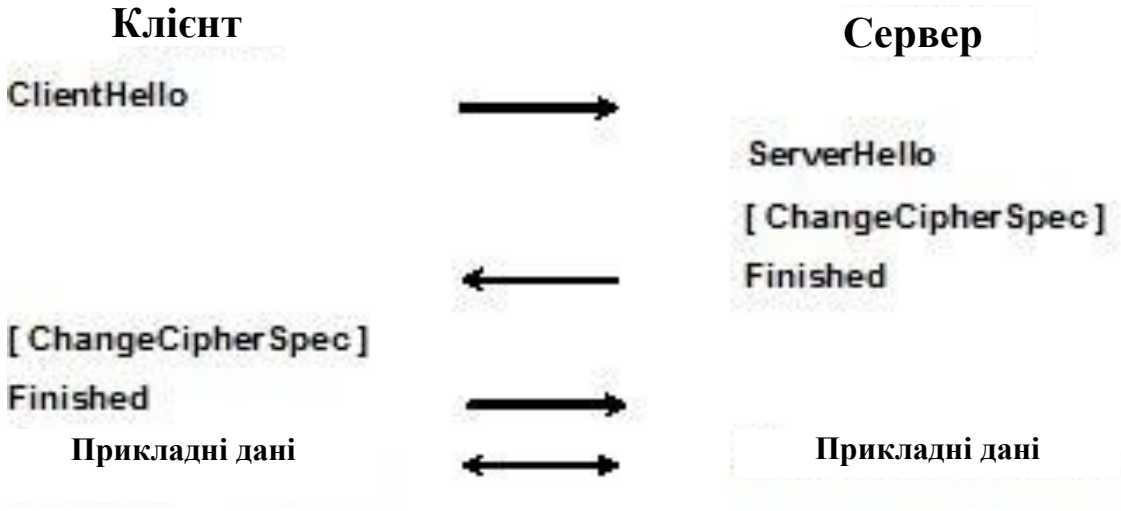

Рисунок 6.2 – Послідовність повідомлень при скороченому Рукостисканні

Варто відмітити, що, тому що Session ID передається без шифрування й забезпечення цілісності, він не містить конфіденційну інформацію. Вміст всього Рукостискання, включаючи Session ID, захищено Finished-повідомленнями, якими учасники обмінюються наприкінці рукостискання.

Список Cipher Suite, переданий від клієнта серверу в повідомленні Client Hello, містить перелік криптографічних алгоритмів, підтримуваних клієнтом, упорядкований по перевагам клієнта. Сервер вибирає по одному алгоритму з кожної категорії, що він підтримує. Якщо такого алгоритму не існує, сервер повертає фатальний Alert і закриває з'єднання.

Після посилання повідомлення Client Hello клієнт чекає повідомлення Server Hello. Будь-яке інше повідомлення, що повертається сервером, за винятком Hello Request, трактується як фатальна помилка.

Сервер посилає Server Hello у відповідь на повідомлення Client Hello, для того щоб вибрати конкретний набір алгоритмів. Якщо для якогось типу алгоритмів клієнт і сервер не мають однакового алгоритму, TCP-з'єднання буде скинуто.

Повідомлення Certificate (сервера)

Сервер повинен посилати сертифікат, якщо метод обміну ключів не є анонімним. Дане повідомлення завжди іде відразу за повідомленням Server Hello.

Тип сертифіката повинен відповідати обраному алгоритму обміну ключа. Звичайно це сертифікат X.509v3. Він повинен містити ключ, що відповідає методу обміну ключа.

Повідомлення серверу обміну ключа посилається сервером тільки тоді, коли повідомлення Server Certificate (якщо воно послано) не містить досить даних для того, щоб клієнт міг здійснити обмін премайстер-секретом.

Дане повідомлення передає криптографічну інформацію, що дозволяє клієнтові передавати премайстер-секрет: премайстер-секрет шифрується або відкритим ключем RSA, або відкритим ключем Діффі-Хеллмана.

Повідомлення Certificate Request

Неанонімний сервер може додатково запросити сертифікат клієнта, якщо це потрібно для політики безпеки сервера.

Повідомлення Server Hello Done

Повідомлення Server Hello Done посилається сервером як ознака закінчення фази Server Hello.

Повідомлення Certificate (клієнта)

Це перше повідомлення, що клієнт посилає після одержання повідомлення Server Hello Done. Воно посилається тільки в тому випадку, якщо сервер запросив автентифікацію клієнта.

Повідомлення Client Key Exchange

Дане повідомлення посилається клієнтом завжди. Воно іде відразу за повідомленням Client Certificate, якщо воно посилалося. У противному випадку це перше повідомлення, послане клієнтом після одержання повідомлення Server Hello Done.

Після одержання даного повідомлення сервер може обчислити премайстер-секрет, що передається або за допомогою RSA шифрування, або обчислюється по алгоритму Діффі-Хеллмана. У кожному разі кожна сторона обчислює той самий премайстер-секрет.

Перевірка цілісності за допомогою сертифіката клієнта

Дане повідомлення використовується для виконання перевірки цілісності переданих і отриманих повідомлень Рукостискання й автентифікації клієнта. Воно посилається тільки в тому випадку, якщо алгоритм відкритого ключа, для якого створений сертифікат клієнта, має можливість підписування. Це означає, що виключенням є сертифікати, створені для відкритого ключа алгоритму Діффі-Хеллмана.

Повідомлення Finished

Повідомлення Finished завжди посилається безпосередньо після повідомлення Change Cipher Spec для перевірки успішного виконання обміну ключа й процесів автентифікації. Повідомлення Change Cipher Spec повинно бути отримане після інших повідомлень Рукостискання й перед Finished-повідомленням.

Finished-повідомлення є першим повідомленням, захищеним за допомогою тільки що обговорених алгоритмів і ключів. Одержувачі Finished-повідомлення повинні переконатися, що його вміст коректний. Після того як одна сторона відправила своє Finished-повідомлення, одержала й перевірила Finished-повідомлення іншої сторони, вона може починати посилати й одержувати прикладні дані по цьому з'єднанню.

Обчислення майстер-секрету

Незалежно від методів обміну ключа використовується наступний алгоритм для перетворення премайстер-секрету в майстра-секрет. Премайстер-Секрет повинен бути вилучений після того, як обчислений майстер-секрет.

master_secret = PRF(pre_master_secret, "master secret",

ClientHello.random+ServerHello.random) [0..47]

Довжина майстер-секрету завжди дорівнює 48 байтам. Довжина премайстер-секрету змінюється залежно від методу обміну ключа.

Додавання додаткових можливостей до протоколу

Розглянемо розширення, які дозволяють додавати нові функціональності в SSL/TLS. Розглянемо загальні механізми розширень для протоколу Рукостискання й конкретні розширення, що використовуються для додавання нових можливостей.

Зараз SSL/TLS використовується в самих різних оточеннях, можливості яких не враховувалися при розробці протоколу. Дані розширення розроблені для того, щоб SSL/TLS міг максимально ефективно функціонувати в нових оточеннях, такі, наприклад, як бездротові мережі.

Бездротові оточення часто мають ряд обмежень, звичайно відсутніх в інших оточеннях. Ці оточення можуть мати обмеження на смугу пропущення, на обчислювальні потужності клієнта, на обсяг пам'яті й т.п.

Дані розширення призначені для забезпечення наступних можливостей:

– Дозволити клієнтам надавати серверу ім'я сервера, з яким вони встановлюють з'єднання. Дана функціональність забезпечує можливість встановлення безпечних з'єднань із хостами, що мають кілька віртуальних серверів на одній мережевій адресі.

– Вести перемовини про максимальну довжину переданих фрагментів. Дана функціональність необхідна через обмеження пам'яті в деяких клієнтів і обмеження смуги пропущення в деяких типах мереж.

– Вести перемовини про використання URL для вказівки сертифікатів клієнта. Дана функціональність потрібна для економії пам'яті клієнта.

– Дозволити клієнтам вказати серверам сертифікати які вони мають в кореневих CA. Дана функціональність необхідна, щоб клієнти з обмеженою пам'яттю могли зберігати тільки невелике число сертифікатів кореневих CA.

– Дозволити клієнтам і серверам вести перемовини про використання урізаних MAC. Дана функціональність дає можливість зменшити трафік, що може бути необхідним в певних типах мереж.

– Дозволити клієнтам і серверам вести перемовини про те, щоб сервер при Рукостисканні посилав клієнтові інформацію про статус сертифіката (наприклад, відповідь OCSP). Дана функціональність дозволяє уникнути посилки CRL і тим самим скоротити трафік і обчислювальне навантаження на клієнта.

Для того щоб підтримувати перераховані вище розширення, вводяться додаткові механізми для повідомлень Hello клієнта й сервера.

Описані розширення можуть використовуватися клієнтами й серверами, що підтримують версію TLS 1.0. Розширення підтримують зворотню сумісність – це означає, що клієнти версії TLS 1.0, які

підтримують розширення, можуть спілкуватися із серверами TLS 1.0, що не підтримує розширення, і навпаки.

Зворотня сумісність досягається в такий спосіб.

– Клієнт запитує використання розширень за допомогою розширеного повідомлення Client Hello, описаного нижче. TLS 1.0 вимагає, щоб сервери приймали розширені повідомлення Client Hello, навіть якщо вони не розуміють розширення.

– Сервер може не посилати ніякої відповіді на розширення, які він не підтримує.

Однак відмітимо, що хоча зворотна сумісність потрібна, деякі клієнти зможуть не встановлювати з'єднання із серверами, які не підтримують необхідні клієнтам розширення.

Як ім'я сервера як правило, підтримується тільки DNS-ім'я.

Сервер, що одержав повідомлення Client Hello, що містить розширення Server Name, може використовувати дану інформацію для вибору сертифіката, що повертається клієнтові, або для якихось інших аспектів безпеки. У цьому випадку сервер повинен включити розширення типу Server Name у розширене Server Hello.

Перемовини про максимальну довжину фрагмента

Колишня версія SSL/TLS указує, що максимальна довжина незашифрованого фрагмента дорівнює 214 байт. Для деяких клієнтів може вимагатися використовувати меншу довжину фрагмента через обмеження пам'яті або обмеження смуги пропущення.

Сервер, що одержав розширений Client Hello з розширенням Max Fragment Length, може прийняти цю довжину й включити розширення Max Fragment Length в Server Hello.

Після того, як сторони успішно домовилися про максимальну довжину фрагмента, відмінної від 214, клієнт і сервер повинні негайно почати фрагментувати повідомлення (включаючи повідомлення

Рукостискання), щоб гарантувати, що не посилають сегменти більшої довжини, чим та, про яку домовилися.

Нова довжина застосовується протягом всієї сесії, включаючи поновлювані сесії.

URL сертифікат клієнта

SSL/TLS вимагає, щоб при виконанні автентифікації клієнта сертифікати клієнта посилали серверу в протоколі Рукостискання. Для клієнтів, що мають обмеження пам'яті, існує можливість посилати URL сертифікат замість самих сертифікатів, щоб вони могли не зберігати свої сертифікати й тим самим не займати пам'ять.

Для ведення переговорів про посилку серверу URL сертифіката клієнти можуть включати розширення типу Client Certificate Url в Client Hello.

Сервер, що одержав розширений Client Hello, що містить розширення Client Certificate Url, може вказати, що має можливість приймати URL сертифікат, вказуючи розширення типу Client Certificate Url в Server Hello.

Вказівка довіреного CA

Клієнти, які мають обмежену пам'ять, можуть зберігати тільки невелику кількість сертифікатів кореневих CA. У цьому випадку вони можуть вказати серверу, якими кореневими сертифікатами вони володіють.

Для цього клієнти можуть включити розширення типу Trusted Ca Keys в Client Hello. Поле Extension Data даного розширення повинне містити Trusted Authorities.

Урізаний HMAC

У даний момент набір шифрування використовує в якості MAC HMAC або з MD5, або з SHA-1 для автентифікації з'єднань рівня запису. Результат обчислення геш-функції використовується як значення MAC.

Однак у деяких обмежених оточеннях може виявитися бажаним використовувати 80-бітні значення MAC.

Для того щоб вести перемовини про використання 80-бітного урізаного MAC, клієнти можуть включити розширення Truncated Hmac у розширений Client Hello.

При одержанні розширеного Hello, що містить розширення Truncated Hmac, сервер може погодитися використовувати урізаний MAC, включаючи розширення Truncated Hmac з порожнім Extension Data у расширенныйServer Hello.

Запит статусу сертифіката

Клієнти, що мають обмеження, можуть захотіти використовувати протокол статусу сертифіката, який повертається як протокол OCSP, для перевірки дійсності сертифікатів сервера, щоб уникнути одержання й перевірки CRL і тим самим зберегти ширину смуги пропускання в обмежених мережах.

РОЗДІЛ 7. БЕЗПЕКА БЕЗДРОТОВИХ З'ЄДНАНЬ

Бездротові мережі (WLAN) стають все більше й більше розповсюдженими. Причиною є те, що вони являють собою недорогий метод з'єднання інформаційних систем, прості в установці й роботі. Деякі організації розраховують витрати на модернізацію кабельних з'єднань у своїх будинках і роблять висновок, що набагато вигідніше використовувати бездротові мережі.

На жаль, незважаючи на те що бездротова технологія сприяє економії засобів, вона веде до виникнення серйозних питань безпеки в організаціях, що використовують даний тип з'єднань. Для запобігання прослуховування мереж і забезпечення коректної автентифікації було розроблено безліч механізмів безпеки, однак дотепер у пропонованих стандартах і в їхніх реалізаціях залишається цілий ряд серйозних уразливостей.

На сьогоднішній день ще не було запропоновано жодного діючого методу захисту для забезпечення повного керування ризиками, пов'язаними з бездротовими мережами. У даному розділі буде розповідатися про ризики безпеки, що пов'язані з використанням бездротових технологій у внутрішній мережі організації, а також визначенні контрзаходів, прийняті організацією для забезпечення контролю над цими ризиками.

Сучасні бездротові технології

У бездротових локальних мережах головним чином використовується група стандартів технології 802.11x (a, b, g і т.д.). Ці стандарти дозволяють з'єднувати робочі станції, або мобільні пристрої каналами із пропускною здатністю до декількох Гбіт/с із використанням бездротової точки доступу, що підключається до кабельної мережі або прямо до іншої робочої станції.

Стандарти передбачають обмін автентифікаційними даними, а також шифрування інформації.

Стандартні архітектури

Для ефективного використання бездротових локальних мереж (WLAN) на підприємстві необхідно забезпечити достатню зону покриття в областях, де співробітники або відвідувачі організації будуть розміщати свої комп'ютери. У приміщеннях радіус дії звичайної бездротової системи стандарту 802.11x WLAN становить, як правило, близько 50 метрів. Поза приміщенням радіус дії може досягати 500 метрів. Отже, точки доступу (AP) повинні розміщатися так, щоб забезпечувати область покриття у відповідних областях.

Наведені тут радіуси дії є приблизними. Реальний радіус дії визначається використовуваним устаткуванням, а також формою й матеріалами, з яких зроблені навколишні фізичні об'єкти.

Ще одним типовим доповненням до архітектури є сервер DHCP, що надає IP-адресу й іншу необхідну інформацію для правильного з'єднання робочої станції в мережі. Ці дані дозволяють завантажувати переносний комп'ютер або мобільний пристрій і з'єднувати його з мережею за допомогою WLAN без яких-небудь додаткових дій. Автентифікація, як правило, проводиться точно в такий же спосіб, як і на будь-який іншій робочій станції в мережі.

DHCP-сервер не обов'язково встановлювати тільки лише для обслуговування адрес у бездротовій мережі. У більшості організацій у внутрішній мережі є DHCP, і WLAN використовує наявний DHCP-сервер за замовчуванням.

Безпека передачі даних

Так як бездротові мережі використовують повітря й простір для передачі й прийому інформації (сигнали є відкритими для будь-якої особи, що перебуває в зоні дії), безпека передачі даних є дуже важливим аспектом безпеки всієї системи в цілому. Без забезпечення належного захисту

конфіденційності й цілісності інформації при її передачі між робочими станціями й точками доступу не можна бути впевненим у тому, що інформація не буде перехоплена зловмисником, і що робітники станції й точки доступу не будуть підмінені сторонньою особою.

Стандарт 802.11x визначає протокол WPA і WPA2 для захисту інформації при її передачі через WLAN. WPA і WPA2 передбачає забезпечення трьох основних аспектів:

– Автентифікація.

– Конфіденційність.

– Цілісність.

WPA і WPA2

WPA і WPA2 (Wi-Fi Protected Access) – являє собою оновлену програму сертифікації пристроїв бездротового зв'язку. Технологія WPA прийшла на заміну технології захисту бездротової Wi-Fi мережі WEP. Плюсами WPA є посилена безпека даних і більш жорсткий контроль доступу до бездротових мереж. Вагомою характеристикою є сумісність між безліччю бездротових пристроїв як на апаратному рівні, так і на програмному. На даний момент WPA і WPA2 розробляються й просуваються організацією Wi-Fi Alliance.

Основні поняття

В WPA забезпечена підтримка стандартів 802.1X, а також протоколу EAP (Extensible Authentication Protocol, розширюваний протокол автентифікації). Варто помітити, що в WPA2 підтримується шифрування у відповідності зі стандартом AES (Advanced Encryption Standard, удосконалений стандарт шифрування), що має ряд переваг над використовуваним в WEP RC4, наприклад набагато більше стійкий криптоалгоритм.

Більш вагомим аспектом при впровадженні WPA є можливість роботи технології на існуючому апаратному забезпеченні Wi-Fi.

Деякі відмінні риси WPA:

– удосконалена схема шифрування RC4;

– обов'язкова автентифікація з використанням EAP;

– система централізованого керування безпекою, можливість використання в діючих корпоративних політиках безпеки.

Автентифікація користувачів

Wi-Fi Alliance дає наступну формулу для визначення суті WPA:

WPA = 802.1X + EAP + TKIP + MIC

Видно, що WPA, по суті, є сумою декількох технологій.

Як згадано вище, у стандарті WPA використовується Розширюваний протокол автентифікації (EAP) як основа для механізму автентифікації користувачів. Неодмінною умовою автентифікації є пред'явлення користувачем свідчення (або інакше мандат), що підтверджує його право на доступ у мережу. Для цього права користувач проходить перевірку за спеціальною базою зареєстрованих користувачів. Без автентифікації робота в мережі для користувача буде заборонена. База зареєстрованих користувачів і система перевірки в більших мережах, як правило, розташовані на спеціальному сервері (найчастіше RADIUS).

Слід зазначити, що WPA має спрощений режим. Він одержав назву Pre-Shared Key (WPA-PSK). При застосуванні режиму PSK необхідно ввести один пароль для кожного окремого вузла бездротової мережі (бездротові маршрутизатори, точки доступу, мости, клієнтські адаптери). Якщо паролі збігаються із записами в базі, користувач одержить дозвіл на доступ у мережу.

Шифрування

Навіть не приймаючи до уваги той факт що WEP, попередник WPA, не має які-небудь механізми автентифікації користувачів як такий, його ненадійність складається, насамперед, у криптографічній слабості алгоритму шифрування. Ключова проблема WEP полягає у використанні занадто схожих ключів для різних пакетів даних.

TKIP, MIC і 802.1X (частини рівняння WPA) внесли свою лепту в посилення шифрування даних мереж, що використовують WPA.

Протокол ***TKIP*** **(*Temporal Key Integrity Protocol*)** – це метод шифрування. Протокол TKIP забезпечує попакетне шифрування, що включає перевірку цілісності повідомлень і механізм повторного шифрування.

TKIP відповідає за збільшення розміру ключа з 40 до 128 біт, а також за заміну одного статичного ключа WEP ключами, які автоматично генеруються й розсилаються сервером автентифікації. Крім того, в TKIP використовується спеціальна ієрархія ключів і методологія керування ключами, що забирає зайву передбачуваність, яка використовувалася для несанкціонованого зняття захисту WEP ключів.

Сервер автентифікації, після одержання сертифіката від користувача, використовує 802.1X для генерації унікального базового ключа для сеансу зв'язку. TKIP здійснює передачу згенерованого ключа користувачеві й точці доступу, після чого вишиковує ієрархію ключів плюс систему керування. Для цього використовується двосторонній ключ для динамічної генерації ключів шифрування даних, які у свою чергу використовуються для шифрування кожного пакета даних. Подібна ієрархія ключів TKIP заміняє один ключ WEP (статичний) на 500 мільярдів можливих ключів, які будуть використані для шифрування даного пакета даних.

Іншим важливим механізмом є перевірка цілісності повідомлень (***Message Integrity Check, MIC***). Її використовують для запобігання перехоплення пакетів даних, зміст яких може бути змінено, а модифікований пакет знову переданий по мережі. MIC побудована на основі потужної математичної функції, що застосовується на стороні відправника й одержувача, після чого рівняється результат. Якщо перевірка показує на розбіжність результатів обчислень, дані вважаються помилковими й пакет відкидається.

При цьому механізми шифрування, які використовуються для WPA і WPA-PSK, є ідентичними. Єдина відмінність WPA-PSK полягає в тому, що автентифікація виробляється з використанням пароля, а не по сертифікату користувача.

WPA2

WPA2 визначається стандартом IEEE 802.11i, прийнятим у червні 2004 року, і покликаний замінити WPA. У ньому реалізоване CCMP і шифрування AES, за рахунок чого WPA2 став більше захищеним, чим свій попередник. З 13 березня 2006 року підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв.

У режимі WPA-PSK/WPA 2-PSK і TKIP або AES використовується загальний ключ (PSK) довжиною 8 – 63 символу.

Автентифікація в WLAN

Автентифікація є ключовим компонентом системи безпеки WLAN. Жодна з опцій, доступних користувачам WLAN, сама по собі не передбачає захист від ризиків, пов'язаних з використанням WLAN. У наступних розділах розглядається кожна з доступних опцій.

Ідентифікатор набору служб

Ідентифікатор набору служб (SSID) – це 32-бітний рядок, використовуваний як мережеве ім'я. Щоб зв'язати робочу станцію із точкою доступу, обидві системи повинні мати той самий SSID. На перший погляд це може здатися рудиментарною формою автентифікації. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися із точкою доступу й з'єднатися з мережею. На жаль, SSID поширюється багатьма точками доступу. Це означає, що будь-яка робоча станція, що перебуває в режимі очікування, може одержати SSID і додати саму себе у відповідну мережу.

Деякі точки доступу можна налаштувати на заборону поширення SSID. Однак, якщо дана конфігурація не буде супроводжуватися

відповідними мірами безпеки передачі даних, SSID як і раніше можна буде визначити за допомогою прослуховування трафіку.

MAC-адреса

Деякі точки доступу дозволяють використовувати MAC-адреси авторизованих робочих станцій для автентифікації (це можливість, передбачена постачальником, тому вона не включена в специфікацію). У даній конфігурації AP настроєна на дозвіл з'єднання тільки по тим MAC-адресам, про які відомо цій точці доступу. MAC-адреса повідомляється точці доступу адміністратором, що додає MAC-адресу в список дозволених пристроїв. На жаль, MAC-адреси повинні передаватися у відкритому виді; у противному випадку мережа функціонувати не буде. Якщо зловмисник прослуховує трафік, він може визначати авторизовані MAC-адреси й налаштувати свою власну систему на використання однієї із цих MAC-адрес для установки з'єднання з AP.

Протокол 802.1X: контроль доступу в мережу по портах

Протокол 802.1X розроблений як надбудова для всіх протоколів контролю доступу 2 рівнів, включаючи Ethernet і WLAN. Протокол призначений для забезпечення узагальненого механізму автентифікації при доступі в мережу й передбачає наступний набір елементів:

– ***Автентифікатор.*** Мережний пристрій, що здійснює пошук інших об'єктів для автентифікації; для WLAN це може бути AP.

– ***Здобувач.*** Об'єкт, якому потрібен доступ. У випадку з WLAN це може бути робоча станція.

– ***Сервер автентифікації***. Джерело служб автентифікації. 802.1X дозволяє централізацію цієї функції, тому даний сервер є, наприклад, сервером RADIUS.

– ***Мережева точка доступу.*** Точка приєднання робочої станції до мережі. По суті, це порт на комутаторі або концентраторі. У бездротовій технології вона є зв'язком між робочої станції й точкою доступу.

– ***Процес доступу через порт (PAE).*** PAE – це процес, що виконує протоколи автентифікації. PAE є як в автентифікатора, так і в здобувача.

– ***Розширюваний протокол автентифікації (EAP).*** Протокол EAP (визначений у стандарті RFC 2284) являє собою протокол, використовуваний при обміні автентифікаційними даними. Поверх EAP можуть працювати й інші протоколи автентифікації більш високого рівня.

Використання протоколу 802.1X дозволяє застосувати більш надійний механізм автентифікації, ніж можливості, доступні в 802.11x. При використанні разом із сервером RADIUS стає можливим централізоване керування користувачами.

Для функціонування 802.1X робоча станція й точка доступу повинні мати між собою зв'язок. Тому робоча станція вже може бути підключена до бездротової мережі перед автентифікацією.

Взаємна автентифікація є необов'язкової відносно 802.1X, і, таким чином, безліч інсталяцій за замовчуванням буде відкрито для атак перехопленням. 802.1X також передбачається одноразова автентифікація (на початку сеансу). Отже, якщо зловмисник заволодіє MAC-адресою легальної робочої станції, вона одержить можливість захопити сеанс і працювати в мережі WLAN під виглядом одного з легальних користувачів.

Питання безпеки бездротових з'єднань

З розширенням застосування WLAN в організаціях виникла необхідність в усвідомленні ризиків, пов'язаних з використанням цих мереж. Ризики варіюються від прослуховування до спрямованих внутрішніх атак і навіть атак, націлених на зовнішні сайти.

Виявлення WLAN

Виявити WLAN дуже легко. Дійсно, саме для цієї мети був розроблений ряд засобів. Однієї з таких утиліт є NetStumber (http://www.netstumber.com/); вона працює в операційних системах сімейства Windows і може використовуватися спільно із супутниковим навігатором (ресивером глобальної системи позиціонування, GPS) для

виявлення бездротових мереж WLAN. Дана утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній WPA/WPA2. Існують і інші засоби, що ідентифікують робочі станції, підключені до точки доступу, а також їх MAC-адреси наприклад, Kismet (http://www.kismetwireless.net/).

Використання зовнішньої антени на портативному комп'ютері уможливлює виявлення мереж WLAN під час обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісного будинку з переносним комп'ютером у руках. Зовнішня антена не є необхідною, однак допомагає розширити діапазон виявлення, яким володіють утиліти.

Прослуховування

Можливо, найбільш очевидним ризиком, що представляється для організації, що використовує бездротову мережу, є можливість проникнення зловмисника у внутрішню мережу компанії. Бездротові мережі по своїй природі дозволяють з'єднувати з фізичною мережею комп'ютери, що перебувають на деякій відстані від неї, як якби ці комп'ютери перебували безпосередньо в мережі. Такий підхід дозволить підключитися до бездротової мережі організації, що розташовується в будинку, людині, що сидить у машині на стоянці поруч із ним.

Даний тип доступу в мережу не завжди доставляє занепокоєння деяким організаціям. Наприклад, у деяких вищих навчальних закладах установлені бездротові мережі, щоб мережні ресурси були доступні студентам і співробітникам у будь-якій точці території університету. Однак це прекрасна можливість для зловмисника перехопити дані, передані у внутрішній мережі.

Навіть ті організації, у яких використовується WPA/WPA2, є уразливими до даного типу прослуховування. Такі засоби, як WPA/WPA2Crack, вимагають обробки декількох мільйонів пакетів, перш ніж зможуть бути визначені ключі шифрування. У сильно завантаженій

мережі це не займе багато часу. Після перехоплення пакетів програма визначає ключі шифрування.

Навіть якщо в організації реалізована надійна автентифікація, що повинні проходити всі користувачі для доступу до секретних файлів і систем, зловмисник може без зусиль добути секретні відомості за допомогою пасивного прослуховування мережі. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Активні атаки

Незважаючи на те, що прослуховування мережі становить серйозну небезпеку, активні атаки можуть бути ще більш небезпечними. Розглянемо основний ризик, пов'язаний з бездротовими мережами: зловмисник може успішно перебороти периметр мережного захисту організації. Більшість організацій розміщають більшу частину засобів безпеки (міжмережеві екрани, системи виявлення вторгнень і т.д.) на лінії мережевого периметра. Системи, розташовані усередині периметра, як правило, захищені набагато менше. Дійсно, на внутрішні системи часто не встановлюються потрібні доповнення, так як ці системи розташовуються в "захищеній" частині мережі.

В більшості організацій використовується деякий метод автентифікації перед наданням доступу до серверів і файлів. Однак якщо на системах не встановлені потрібні відновлення, у зловмисника з'являється можливість виявити ці уразливості, якими він зможе скористатися для виконання несанкціонованих дій.

Не слід думати, що атаки з використанням уразливостей – це єдиний спосіб зловмисного впливу зловмисників. Якщо хакер прослуховує мережу, він може також перехопити паролі й користувальницькі ідентифікатори.

Атаки на внутрішні системи організації – не єдиним методом заподіяння збитку організації. Зрозуміло, втрата конфіденційної інформації вкрай небажана, але якщо плюс до всього постраждає репутація компанії?

Замість проведення внутрішніх атак зловмисник може використовувати мережеве з'єднання для атаки ззовні. Таким чином, організація стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему.

У випадку виявлення зловмисника виникає питання: звідки він діє. Зловмисник прив'язаний до IP-адреси, однак ця IP-адреса фізично може бути ніяк не пов'язана з конкретним місцем розташування.

Зловмисник може розташовуватися де завгодно в радіусі дії бездротової мережі. Останнім часом це являє собою серйозну проблему пошук і припинення діяльності зловмисників. За допомогою атак зсередини зловмисник може обходити стороною механізми захисту більшої частини організацій. Мова йде про ті ж механізми, які використовувалися б для відстеження дій зловмисників.

Можливі юридичні питання

Ще однією потенційною загрозою для організації є ризик, пов'язаний із правовими аспектами й питаннями відповідальності, які можуть виникнути, якщо зловмисник спробує одержати доступ у внутрішню мережу організації. По-перше, необхідно розібратися, чи почала організація належні заходи щодо захисту секретної інформації. Яким чином, наприклад, інспектори можуть розцінити ситуацію, коли зловмисник одержує доступ до інформації про клієнтів у банку? Передбачається ймовірна відповідальність за успішну атаку зловмисника, спрямовану на іншу організацію, здійснену через бездротову мережу веб-сайту організації. Чи може власник бездротової мережі відповістити за заподіяний у такий спосіб збиток? Варто проконсультуватися по даному питанню з головним юридичним консультантом компанії.

Реалізація безпеки бездротових мереж

Реалізація WLAN повинна випереджатися повною оцінкою ризиків, пов'язаних із проектом. Необхідно провести вивчення потенційних погроз, що представляються для компанії. Варто виявити будь-які наявні контрзаходи. Якщо керівництво організації вирішить продовжити

реалізацію, необхідно вжити додаткових заходів для зниження ризиків, що представляються для організації. У наступних розділах розповідається про деякі міри безпеки, які можуть допомогти в керуванні ризиками.

Безпека точки доступу

На самому початку реалізації проекту необхідно налаштувати безпеку точки бездротового доступу. В ідеальному випадку точка доступу дозволяє вказати ключ WPA/WPA2. Переконайтеся, що цей ключ не можна легко вгадати. Хоча такий крок і не запобіжить злому ключа, він зробить процес несанкціонованого визначення ключа трохи складнішим. Якщо можливо, використовуйте MAC-адреси для обмеження набору робочих станцій, яким дозволене підключення. Це ускладнить завдання керування проектом, однак даний підхід допомагає обмежити виявлення робочих станцій точкою доступу. Переконайтеся, якщо можливо, що точка доступу не здійснює поширення SSID.

Більша частина точок доступу, доступних на ринку, надаються деяким інтерфейсом керування. Це може бути веб-інтерфейс або інтерфейс SNMP. По можливості використовуйте HTTPS для керування точкою доступу й запобігайте доступу зловмисника за допомогою використання високонадійних паролів.

Останнє, що необхідно взяти до уваги при розгляді точок доступу, – їхнє розташування. Пам’ятайте, що бездротові сигнали можуть поширюватися на значні відстані. Сигнали можуть елементарно доходити до інших поверхів будинку, автомобільного паркування або зовсім за межі території підприємства. Спробуйте розмістити точки доступу так, щоб їхній діапазон дії якнайменше виходив за межі приміщення або будинку, займаного компанією.

В організаціях рідко вдається повністю обмежити поширення сигналу в такий спосіб. Однак варто пам'ятати, що даний підхід має на увазі максимально можливе обмеження радіуса дії. Якщо можливо запобігти доступу сторонньої людини у внутрішню мережу зі звичайним

адаптером бездротової мережі, що проходить по вулиці за межами підприємства, то необхідно вжити відповідних заходів.

Безпека передачі даних

Навіть незважаючи на серйозні уразливості, що є присутнім в WPA/WPA2, необхідно використовувати цей протокол. Причина в тому, що в особи, що ненавмисно здійснила спробу доступу (наприклад, клієнт інтернет-кафе), не буде можливості одержати доступ до мережі через допущену випадковість. Захист WPA/WPA2 може бути переборений, однак для цього буде потрібно багато зусиль, і немає ніяких причин для того, щоб дозволяти зловмисникові діяти зовсім вільно.

Беручи до уваги, що WPA/WPA2 недостатньо захищає важливу інформацію, рекомендується використовувати інший тип системи шифрування, крім WLAN. Дійсно, якщо розглядати бездротову мережу як наполовину довірений або не довірений сегмент мережі, стає очевидним, що тут потрібно застосувати той же тип захисту, що використовується віддаленими співробітниками для одержання доступу до внутрішніх систем. Варто застосовувати VPN при з'єднанні робочих станцій WLAN із внутрішньою мережею. Більша частина VPN-продуктів передбачає надійні алгоритми шифрування, у яких відсутні недоліки, властиві WPA/WPA2.

Розміщайте WLAN у зоні, що захищається міжмережевим екраном або іншим пристроєм контролю доступу, і використовуйте VPN при з'єднанні із цією системою.

Безпека робочої станції

Існує можливість прямо атакувати робочі станції в мережі WLAN. Якщо зловмисник хоче проникнути в мережу WLAN, то буде використовувати сніффери для виявлення інших робочих станцій. Навіть якщо не вийде проникнути у внутрішні системи або прослухати інформацію, передану в мережі, він зможе атакувати інші робочі станції.

Захист робочих станцій у мережі WLAN не відрізняється від захисту переносних комп'ютерів, розташованих в іншому місці. Необхідно

встановити відповідне антивірусне ПЗ. Якщо ризик великий, на робочих станціях варто застосувати персональні міжмережеві екрани.

Безпека сайту

Якщо мережі WLAN розглядаються як наполовину довірені або мережі без довіри, не існує причин для розміщення WLAN у внутрішній мережі з такими ж правами доступу до секретних систем, якими володіють внутрішні робочі станції. Отже, мережі WLAN необхідно розгортати в окремих сегментах мережі й встановити міжмережевий екран між мережею WLAN і внутрішньою мережею організації.

Поряд із сегментацією мережі варто встановити в WLAN систему виявлення вторгнень для виявлення несанкціонованих відвідувачів. Імовірно, що у вас не вийти виявити, де зловмисник розташовується фізично, однак ви, принаймні, будете знати, що він проникнув у систему, якщо ним будуть здійснюватися спроби виконання якої-небудь активної атаки.

У кожному разі при використанні робочої станції в мережі WLAN необхідно використовувати надійний механізм автентифікації. Стандарт 802.1X передбачає більш надійну автентифікацію, ніж SSID або MAC-адреса, однак він не захищений від перехоплення сеансу з'єднання. Використання надійної автентифікації разом з VPN значно знизить можливість зловмисника одержати доступ до внутрішніх систем.

Нелегальні й несанкціоновані точки доступу також являють собою проблему, що організації повинні дозволяти з метою запобігання неприємностей. Низька вартість точок бездротового доступу дозволяє практично будь-якій людині придбати такий пристрій і встановити його в мережі. В організаціях необхідно періодично проводити перевірку бездротових з'єднань у власних корпоративних мережах.

Для цього можна використовувати такі утиліти як NetStumber або засоби виявлення точок доступу у внутрішній мережі APTools

(http://winfingerprint.sourceforge.net/aptools.php) або FoundScan (http://www.foundstone.com/).

Приклад реалізації бездротової локальної мережі

Керівництво організації вирішило розгорнути WLAN для зниження вартості модернізації кабельних з'єднань у частині будинку. Приміщення, у якому буде діяти зона покриття WLAN, містить у собі їдальню й кімнату відпочинку. Передбачається, що багато співробітників, які не працюють безпосередньо в новому приміщенні організації, захочуть використовувати WLAN, перебуваючи в їдальні або кімнаті відпочинку. На вас була покладена відповідальність за виявлення погроз безпеки, розробку стратегій керування цими ризиками й розгортання системи.

Крок за кроком

– Почніть із того, що розпишіть на папері суть проблеми. Визначте, які служби повинні бути доступні співробітникам на території організації, а також тих, хто може працювати в мережі, перебуваючи в їдальні або в приміщенні для відпочинку.

– Визначте ризики, що представляються для організації через використання WLAN. Чи буде сигнал бездротової мережі доступний поза територією організації? Як розв'язати питання підключення до мережі відвідувачів і позаштатних співробітників?

– Після визначення погроз варто почати визначення контрзаходів, які можуть знизити ризики до контрольованого рівня. Не слід розглядати лише технологічні рішення. Візьміть до уваги також питання, пов'язані з керуванням і виконанням різних операцій.

– Якщо у вас є доступ до точки доступу й бездротовий мережний адаптер, спробуйте застосувати розроблені рішення.

Отже, широкомасштабне розгортання WLAN – це проект, для реалізації якого буде потрібно залучити мережевих і системних адміністраторів, а також співробітників відділу безпеки. Керівництво багатьох організацій використовує низьку вартість бездротових технологій

у порівнянні з модернізацією наявних кабельних мережевих з'єднань типу CAT5. Міри безпеки, які необхідно застосувати в мережі WLAN, підвищать вартість розгортання. Варто врахувати всі питання, пов'язані з керуванням і виконанням операцій, так як може представитися можливість для використання процедур підтримки безпеки WLAN.

РОЗДІЛ 8. СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS-СИСТЕМИ)

Виявлення вторгнень – це ще одне завдання, що виконують співробітники, відповідальні за безпеку інформації в організації, при забезпеченні захисту від атак. Виявлення вторгнень – це активний процес, при якому відбувається виявлення хакеру при його спробах проникнути в систему. В ідеальному випадку така система лише видасть сигнал тривоги при спробі проникнення. Виявлення вторгнень допомагає при примітивній ідентифікації активних погроз за допомогою оповіщень і попереджень про те, що зловмисник здійснює збір інформації, необхідної для проведення атаки. У дійсності, як буде показано в матеріалі лекції, це не завжди так. Перед обговоренням подробиць, пов'язаних з виявленням вторгнень, давайте визначимо, що ж це в дійсності таке.

Периметр захисту мережі являє собою віртуальний периметр, усередині якого перебувають комп'ютерні системи. Цей периметр може визначатися міжмережевими екранами, точками поділу з'єднань або настільних комп'ютерів з модемами. Даний периметр може бути розширений для змісту домашніх комп'ютерів співробітників, яким дозволено з'єднуватися один з одним, або партнерів по бізнесу, яким дозволено підключатися до мережі. З появою в діловій взаємодії бездротових мереж периметр захисту організації розширюється до розміру бездротової мережі.

Система виявлення вторгнень (IDS) призначена для розмежування авторизованого входу й несанкціонованого проникнення, що реалізується набагато складніше.

Визначення типів систем виявлення вторгнень

Існують два основних типи IDS:

– вузлові (HIDS);

– мережеві (NIDS).

Система HIDS розташовується на окремому вузлі й відслідковує ознаки атак на даний вузол.

Система NIDS перебуває на окремій системі, що відслідковує мережевий трафік на наявність ознак атак, проведених у підконтрольному сегменті мережі.

На рисунку 8.1 показані два типи IDS, які можуть бути присутні у мережному середовищі.

Рисунок 8.1 – Приклади розміщення IDS у мережевому середовищі

Вузлові IDS

Вузлові IDS (HIDS) являють собою систему датчиків, що завантажуються на різні сервера організації й керуються центральним диспетчером. Датчики відслідковують різні типи подій і вживають визначені дії на сервері або передають повідомлення. Датчики HIDS відслідковують події, пов'язані із сервером, на якому вони завантажені.

Сенсор HIDS дозволяє визначити, чи була атака успішною, якщо атака мала місце на тій же платформі, на якій встановлено датчик.

Як буде показано далі, різні типи датчиків HIDS дозволяють виконувати різні типи завдань по виявленню вторгнень. Не кожний тип датчиків може використовуватися в організації, і навіть для різних серверів усередині однієї організації можуть знадобитися різні датчики. Варто відмітити, що система HIDS, як правило, коштує дорожче, ніж мережева система, так як в цьому випадку кожний сервер повинен мати ліцензію на датчик (датчики дешевше для одного сервера, однак загальна вартість датчиків більше в порівнянні з вартістю використання мережних IDS).

З використанням систем HIDS пов’язано ще одне питання, що полягає в можливостях процесора на сервері. Процес датчика на сервері може займати від 5 до 15 % загального процесорного часу. Якщо датчик працює на активно використовуваній системі, його присутність негативно позначиться на продуктивності й, таким чином, треба буде встановлювати більш продуктивну систему.

Імовірне виникнення розбіжностей, пов'язаних з керуванням і налаштовуванням, між адміністраторами безпеки (керуючими роботою IDS) і системними адміністраторами. Так як процес повинен постійно перебувати в активному стані, необхідна гарна координація в їхній роботі.

Існує п'ять основних типів датчиків HIDS:

– Аналізатори журналів.

– Датчики ознак.

– Аналізатори системних викликів.

– Аналізатори поводження застосунків.

– Контролери цілісності файлів.

Варто відмітити, що кількість датчиків HIDS збільшується, і деякі виробники пропонують функціональні можливості, що передбачають використання датчиків більш ніж п'яти основних видів.

Аналізатори журналів

Аналізатор журналу являє собою саме те, що відбиває саму назву датчика. Процес виконується на сервері й відслідковує відповідні файли журналів у системі. Якщо зустрічається запис журналу, що відповідає деякому критерію в процесі датчика HIDS, застосовується встановлена дія.

Більша частина аналізаторів журналів налаштована на відстеження записів журналів, які можуть означати подію, пов'язану з безпекою системи. Адміністратор системи, як правило, може визначити інші записи журналу, що представляють визначений інтерес.

Аналізатори журналів по своїй природі є реактивними системами. Іншими словами, вони реагують на подію вже після того, як вона відбулася. Таким чином, журнал буде містити відомості про те, що проникнення в систему виконано. У більшості випадків аналізатори журналів не здатні запобігти здійснюваній атаці на систему.

Аналізатори журналів, зокрема, добре адаптовані для відстеження активності авторизованих користувачів на внутрішніх системах. Таким чином, якщо в організації приділяється увага контролю за діяльністю системних адміністраторів або інших користувачів системи, можна використовувати аналізатор журналу для відстеження активності й переміщення запису про цю активність в область, недосяжну для адміністратора або користувача.

Датчики ознак

Датчики цього типу являють собою набори визначених ознак подій безпеки, що зіставляються із вхідним трафіком або записами журналу. Розбіжність між датчиками ознак і аналізаторами журналів полягає в можливості аналізу вхідного трафіку.

Системи, засновані на зіставленні ознак, забезпечують можливість відстеження атак під час їхнього виконання в системі, тому вони можуть видавати додаткові повідомлення про проведення злочинних дій. Проте, атака буде успішно або безуспішно завершена перед вступом у дію

датчика HIDS, тому датчики цього типу вважаються реактивними. Датчик ознак HIDS є корисним при відстеженні авторизованих користувачів усередині інформаційних систем.

Аналізатори системних викликів

Аналізатори системних викликів здійснюють аналіз викликів між додатками й операційною системою для ідентифікації подій, пов'язаних з безпекою. Датчики HIDS даного типу розміщають програмну спайку між операційною системою й додатками. Коли застосунку потрібно виконати дію, його виклик операційної системи аналізується й зіставляється з базою даних ознак. Ці ознаки є прикладами різних типів поводження, які виявляють собою атакуючі дії, або об'єкти інтересу для адміністратора IDS.

Аналізатори системних викликів відрізняються від аналізаторів журналів і датчиків ознак HIDS тим, що вони можуть запобігати дії. Якщо застосунок генерує виклик, що відповідає, наприклад, ознаці атаки на переповнення буферу, датчик дозволяє запобігти цьому виклику й зберегти систему в безпеці.

Необхідно забезпечувати правильну конфігурацію датчиків цього типу, так як їхнє некоректне налаштовування може викликати помилки в додатках або відмови в їхній роботі. Такі датчики, як правило, забезпечують можливість функціонування в тестовому режимі. Це означає, що датчик відслідковує події, але не вживає ніяких дій, що блокують; цей режим можна використовувати для тестування конфігурації без блокування роботи легітимно використовуваних застосунків.

Аналізатори поводження застосунків

Аналізатори поводження застосунків аналогічні аналізаторам системних викликів у тому, що вони застосовуються у вигляді програмної спайки між додатками й операційною системою. В аналізаторах поводження датчик перевіряє виклик на предмет того, чи дозволено застосунку виконувати дану дію, замість визначення відповідності виклику

ознакам атак. Наприклад, веб-серверу звичайно дозволяється приймати мережеві з'єднання через порт 80, зчитувати файли у веб-каталозі й передавати ці файли по з'єднанню через порт 80. Якщо веб-сервер спробує записати або зчитати файли з іншого місця або відкрити нові мережеві з'єднання, датчик виявить невідповідність нормі поводження сервера й заблокує дію.

При конфігуруванні таких датчиків необхідно створювати список дій, дозволених для виконання кожним застосунком. Постачальники датчиків даного типу надають шаблони для широко використовуваних застосунків. Будь-які "доморослі" додатки повинні аналізуватися на предмет того, які дії їм дозволяється виконувати, і виконання цього завдання повинно бути програмно реалізоване в датчику.

Контролери цілісності файлів

Контролери цілісності файлів відслідковують зміни у файлах. Це здійснюється за допомогою використання криптографічної контрольної суми або цифрового підпису файлу. Кінцевий цифровий підпис файлу буде змінений, якщо відбудеться зміна хоча б малої частини вихідного файлу (це можуть бути атрибути файлу, такі як час і дата створення). Алгоритми, використовувані для виконання цього процесу, розроблялися з метою максимального зниження можливості для внесення змін у файл зі збереженням колишнього підпису.

При початковій конфігурації датчика кожен файл, що підлягає моніторингу, піддається обробці алгоритмом для створення початкового підпису. Отримане число зберігається в безпечному місці. Періодично для кожного файлу цей підпис перераховується й зіставляється з оригіналом. Якщо підписи збігаються, це означає, що файл не був змінений. Якщо відповідності немає, виходить, у файл були внесені зміни.

Робота датчика даного типу сильно залежить від якості контролю над конфігурацією. Якщо організація не здійснює керування датчиком на належному рівні, то датчик, як правило, виявляє всі типи змін, що були

внесені у файл, які, насправді, можуть бути легітимними, але невідомими датчику.

Контролер цілісності файлів не здійснює ідентифікацію атаки, а деталізує результати проведеної атаки. Таким чином, у випадку атаки на веб-сервер сама атака залишиться непоміченою, але будуть виявлені ушкодження або зміна домашньої сторінки веб-сайту. Те ж саме відноситься й до інших типів проникнень у систему, так як в процесі багатьох з них здійснюється зміна системних файлів.

Мережеві IDS

NIDS являє собою програмний процес, що працює на спеціально виділеній системі. NIDS перемикає мережеву карту в системі в нерозбірливий режим роботи, при якому мережевий адаптер пропускає весь мережевий трафік (а не тільки трафік, спрямований на дану систему) у програмне забезпечення NIDS. Після цього відбувається аналіз трафіку з використанням набору правил і ознак атак для визначення того, чи представляє цей трафік який-небудь інтерес. Якщо це так, то генерується відповідна подія.

На даний момент більшість систем NIDS базується на ознаках атак. Це означає, що в системи вбудований набір ознак атак, з якими зіставляється трафік у каналі зв'язку. Якщо відбувається атака, ознака якої відсутня у системі виявлення вторгнень, система NIDS не помітить цю атаку. NIDS-системи дозволяють вказувати трафік, який цікавить, за адресою джерела, кінцевою адресою, портом джерела або кінцевим портом. Це дає можливість відстеження трафіку, що не відповідає ознакам атак.

На ринку почали з'являтися системи NIDS, що базуються на виявленні аномалій. Ці системи здійснюють пошук аномалій у мережевому трафіку для виявлення атак. Корисність використання цих пристроїв на момент написання книги ще не доведена.

Найчастіше при застосуванні NIDS використовуються дві мережеві карти (див. рисунок 8.2). Одна карта використовується для моніторингу мережі. Ця карта працює в "схованому" режимі, тому вона не має IP-адреси, отже, не відповідає на вхідні з'єднання.

У схованої карти відсутній стек протоколів, тому вона не може відповідати на такі інформаційні пакети, як пінг-запити. Друга мережева карта використовується для з'єднання із системою керування IDS і для відправлення сигналів тривоги. Ця карта приєднується до внутрішньої мережі, невидимої для тієї мережі, по відношенню до якої відбувається моніторинг.

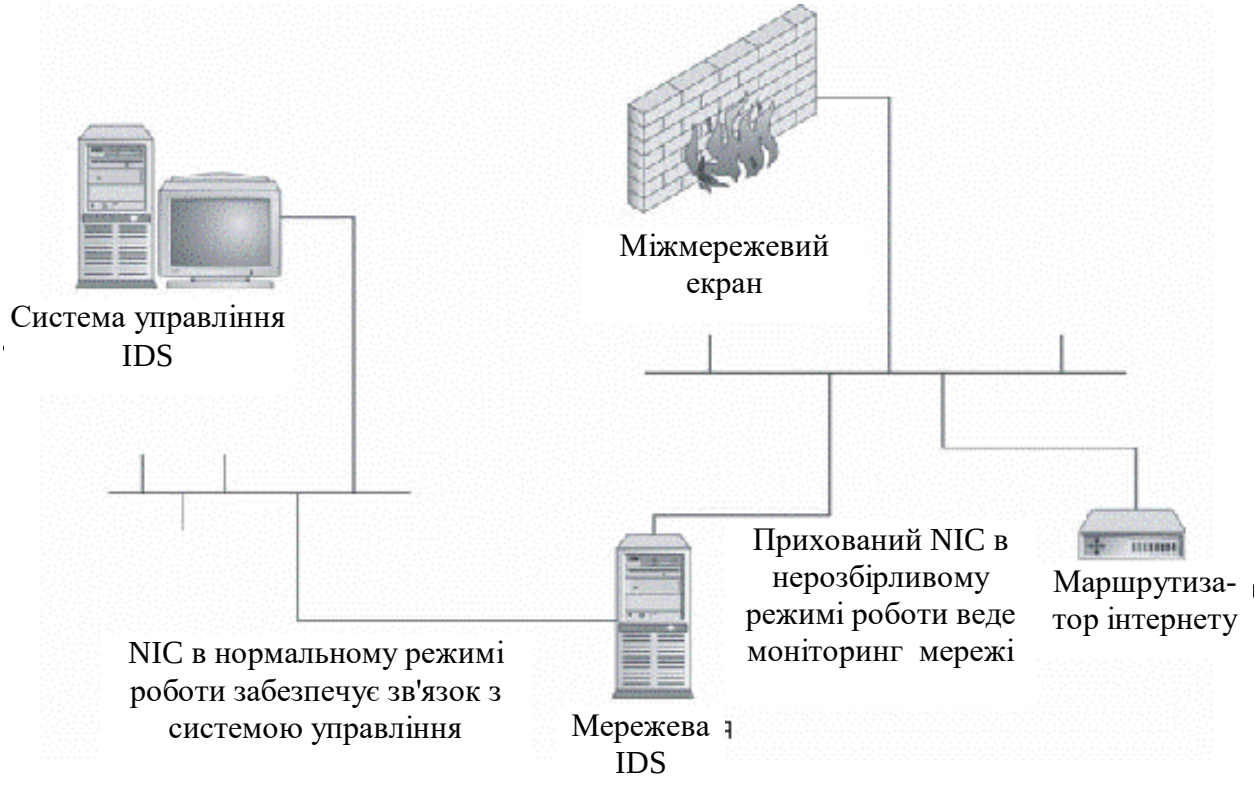

Рисунок 8.2 – Конфігурація NIDS із двома мережними картами

Серед переваг використання NIDS можна виділити наступні моменти:

– NIDS можна повністю сховати в мережі таким чином, що зловмисник не буде знати про те, що за ним ведеться спостереження.

– Одна система NIDS може використовуватися для моніторингу трафіку з більшим числом потенційних систем-цілей.

– NIDS може здійснювати перехоплення вмісту всіх пакетів, що направляються на систему-ціль.

Серед недоліків даної системи необхідно відзначити наступні аспекти:

– Система NIDS може тільки видавати сигнал тривоги, якщо трафік відповідає встановленим правилам або ознакам.

– NIDS може упустити потрібний трафік, який цікавить, через використання широкої смуги пропущення або альтернативних маршрутів.

– Система NIDS не може визначити, чи була атака успішною.

– Система NIDS не може переглядати зашифрований трафік.

– У мережах, які комутуються, (на відміну від мереж із загальними носіями) потрібні спеціальні конфігурації, без яких NIDS буде перевіряти не весь трафік.

Який тип IDS краще?

Чи є один із двох типів IDS більше кращим у порівнянні з іншим? Все залежить від обставин. У пристроїв обох типів є свої переваги й недоліки. У той час як NIDS більш ефективний з погляду вартості (одна система NIDS здійснює моніторинг трафіку великої кількості систем), HIDS більше підходить для організацій, у яких приділяється підвищена увага відстеженню роботи штатних співробітників. Іншими словами, вибір типу пристрою IDS залежить від першочергових цілей, яких необхідно досягти в мережі організації.

Установка IDS

Щоб використовувати IDS по максимуму, необхідно провести великий обсяг процедур планування перед безпосередньою установкою пристрою. Перед створенням відповідної політики потрібно здійснити збір необхідної інформації, провести аналіз мережі й реалізувати завдання по керуванню. Як у більшості комплексних систем, політику необхідно

створити, затвердити й протестувати перед застосуванням. При створенні політики IDS необхідно виконати наступні кроки:

– Визначити цілі створення IDS.

– Вибрати об'єкти моніторингу.

– Вибрати відповідні дії.

– Встановити пороги.

– Застосувати політику.

Визначення цілей застосування IDS

Цілі використання IDS визначають вимоги для політики IDS. Потенційно цілями застосування IDS є наступні.

– Виявлення атак.

– Запобігання атак.

– Виявлення порушень політики.

– Примус до використання політик.

– Примус до проходження політикам з'єднань.

– Збір доказів.

Майте на увазі, що цілі використання пристроїв можуть комбінуватися, і конкретні цілі застосування будь-якої IDS залежать від організації. Набір цілей у жодному разі не обмежується цим списком. IDS дозволяє організації виявляти початок проведення атаки й здійснювати збір доказів або запобігання додаткового ушкодження за допомогою усунення аварійних ситуацій. Зрозуміло, це не єдина ціль, для досягнення якої застосовується IDS. Так як IDS здійснює збір деталізованої інформації з багатьом подіям, що відбуваються в мережі й на комп'ютерах організації, вона також може ідентифікувати дії, що порушують політику, і реальний рівень використання мережних ресурсів.

Розпізнавання атак

Розпізнавання атак є однією з головних цілей використання IDS. Система IDS запрограмована на пошук визначених типів подій, які служать ознаками атак. Як простий приклад приведемо з'єднання через

TCP-порт 80 (HTTP), за яким слідує URL, що містить розширення .bat. Це може бути ознакою того, що зловмисник намагається використовувати вразливість на веб-сервері IIS.

Більшу частину атак ідентифікувати не просто. Наприклад, дотепер в Інтернеті широко поширені атаки з угадуванням пароля. Система HIDS може містити правило, відповідно до якого після трьох невдалих спроб входу через короткі проміжки часу вхід у даний обліковий запис блокується. Для цього HIDS повинна відслідковувати час і число невдалих спроб входу на кожному обліковому записі, фіксувати в журналі, і скидати лічильник у випадку успішного входу або закінчення часу.

Ще більш складним прикладом розпізнавання атак є ситуація, коли зловмисник намагається вгадати паролі на декількох облікових записах і системах. У цьому випадку атакуючий не буде намагатися ввійти в той самий обліковий запис двічі за короткий проміжок часу, а спробує використовувати цей пароль у кожному обліковому записі. Якщо час кожної спроби досить великий, лічильники на окремих облікових записах будуть скидатися, перед тим як зловмисник тричі здійснить невдалий вхід у систему з використанням даного облікового запису. Єдиним способом виявити таку атаку є зіставлення інформації з журналів різних систем. Такий аналіз здійснює система HIDS.

Моніторинг політики

Моніторинг політики – це менш помітний аспект діяльності по виявленню атак. Метою системи IDS, налаштованої на відстеження політики, є відстеження виконання або невиконання політики організації. У найпростішому випадку NIDS можна налаштувати на відстеження всього веб-трафіку поза мережею. Така конфігурація дозволяє відслідковувати будь-яку невідповідність політикам використання Інтернету. Якщо в системі зконфігурований список веб-сайтів, що не відповідає веб-стандартам корпоративного використання, NIDS зафіксує будь-які підключення до таких сайтів.

Система NIDS також перевіряє відповідність конфігураціям маршрутизатора або міжмережевого екрана. В цьому випадку NIDS налаштовується на відстеження трафіку, що не повинен проходити через маршрутизатор або міжмережевий екран. При виявленні такого трафіку визначається порушення корпоративної політики міжмережевих екранів.

Використання IDS для моніторингу політики може зайняти дуже багато часу й зажадати великої кількості дій по конфігуруванню.

Примус до використання політики

Застосування системи IDS як засіб примусового використання політики виводить конфігурацію моніторингу політики на більш високий рівень. При відстеженні політики, IDS налаштовується на виконання дій при порушенні політики. У першому прикладі в розділі "Моніторинг політики" IDS із примусом до використання політики не тільки визначить спробу з'єднання з недоступним веб-сайтом, але й вживе заходів по запобіганню цієї дії.

Обробка інциденту

Система IDS може виявитися корисною після виявлення інциденту. У цьому випадку за допомогою IDS можна зібрати докази. NIDS можна налаштувати на відстеження визначених з'єднань і ведення повноцінного журналу по обліку трафіку. У той же час можна використовувати й HIDS для фіксування всіх записів журналу для визначеного облікового запису системи.

Вибір об'єкта моніторингу

Вибір об'єкта моніторингу залежить від цілей, поставлених перед системою IDS, і від середовища, у якій IDS буде функціонувати. Наприклад, якщо ціль IDS полягає у виявленні атак, і IDS розташована в Інтернеті за межами міжмережевого екрана компанії, то IDS буде потрібно відслідковувати весь трафік, що надходить на міжмережевий екран, для виявлення вхідних атак. Як альтернатива IDS можна розмістити в межах зони, що захищається міжмережевим екраном, для визначення тільки тих

атак, які успішно перебороли міжмережевий екран. Вихідний трафік у цьому випадку може ігноруватися (див. рисунок 8.3). У таблиці 8.1 приводяться приклади об'єктів моніторингу при використанні конкретних політик.

Вибір об'єкта моніторингу визначає розташування датчиків. Датчики можуть бути розташовані поза міжмережевого екраном, усередині мережі, на системах із секретною інформацією або на системах, використовуваних спеціально для збору й обробки даних журналу. Ключовим моментом, про який необхідно пам'ятати при винесенні рішення з приводу розміщення датчика IDS, є те, що датчик повинен мати можливість перегляду подій, які цікавлять, будь то мережний трафік або запис журналу. Якщо події, які цікавлять не переборюють міжмережевий екран, то не рекомендується розміщати датчик NIDS в області, що захищається міжмережевим екраном. Аналогічно, якщо події, які цікавлять фіксуються тільки на головному контролері домену мережі Windows NT, програмне забезпечення HIDS повинне бути розташоване на головному контролері домену, навіть якщо зловмисник фізично розташовується на робочій станції всередині мережі.

Таблиця 8.1 – Приклади інформації, що відслідковується при наявності політики IDS

Політика	**NIDS**	**HIDS**
Виявлення атак	Весь трафік, що надходить на системи, що атакуються потенційно (мережні екрани, веб-сервери, сервери застосунків і т.д.)	Невдалі спроби входу. Спроби з'єднання. Вдалий вхід з віддалених систем.
Запобігання атак	Те ж, що й для виявлення атак	Те ж, що й для виявлення атак.

Продовження таблиці 8.1

Виявлення порушень політики	Весь трафік HTTP, формований на системах клієнтах. Весь трафік FTP, формований на системах клієнтах	Успішні HTTP-з'єднання. Успішні FTP з'єднання. Файли, що завантажуються.
Примус до використання політик	Те ж, що й для виявлення порушень політики	Те ж, що й для виявлення порушення політики.
Примус до відповідності політикам з'єднань	Весь трафік, що порушує примусово використовувану політику з'єднання	Успішні з'єднання із заборонених адрес або по заборонених портах.
Збір доказів	Вміст усього трафіку, формованого на системі-цілі або атакуючій системі	Всі успішні підключення, що виходять із атакуючої системи. Всі невдалі з'єднання з атакуючих систем. Всі натискання клавіш із інтерактивних сеансів на атакуючих системах.

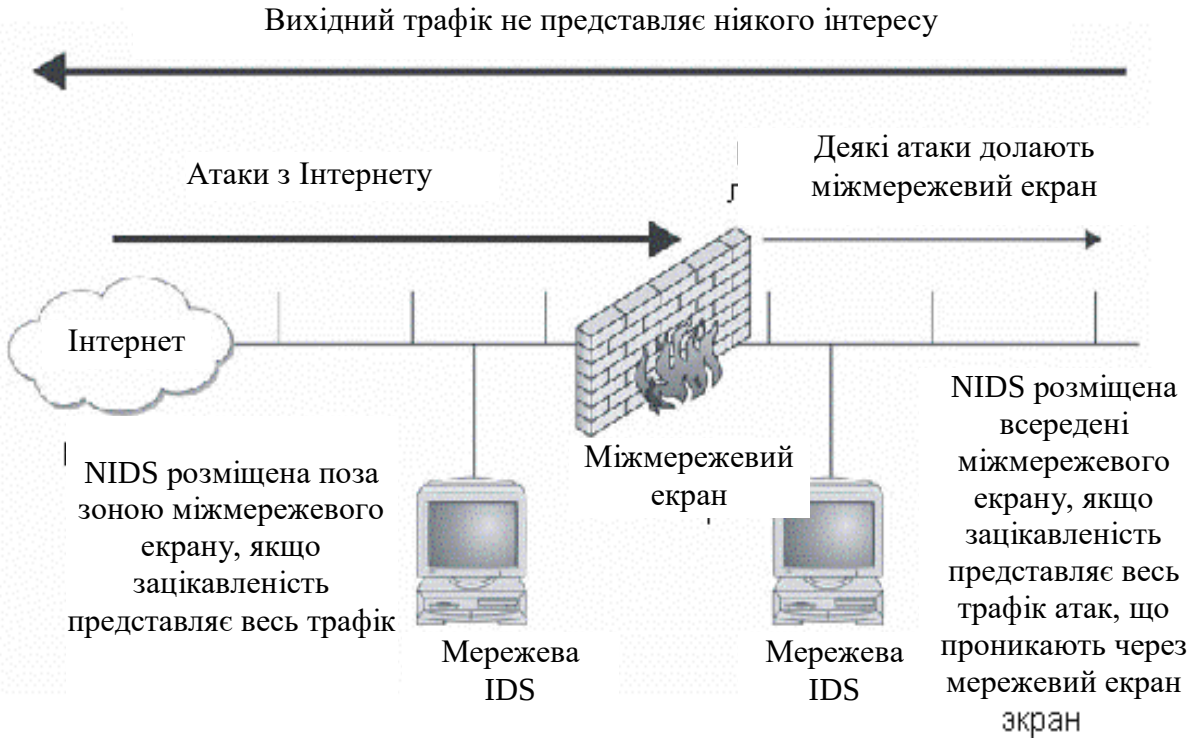

Рисунок 8.3 – Приклад вибору об'єкта моніторингу

При розміщенні датчиків NIDS необхідно керуватися ще одним ключовим правилом. Якщо в мережі використовуються комутатори замість концентраторів, датчик NIDS не буде правильно працювати, якщо він просто підключений до порту комутатора. Комутатор буде відправляти тільки трафік, спрямований на датчик, до того порту, до якого підключений датчик. У випадку з мережею, яка комутується, існують два варіанти використання датчиків NIDS:

– застосування порту, що відслідковує комутатор

– застосування мережевого розгалужувача.

На рисунку 8.4 показані конфігурації обох типів.

При використанні порту може виникнути конфлікт із персоналом по обслуговуванню мережі через те, що цей порт може використовуватися для дозволу проблем, що виникають у мережі. Крім цього, багато комутаторів дозволяють вести моніторинг (деякими виробниками замість цього слова використовується термін "зв'язування") тільки одного порту

одноразово. Порт моніторингу, як правило, не дозволяє здійснювати моніторинг магістралі комутатора. Ця функція не буде працювати в кожного разу, так як магістраль комутатора передає дані зі швидкістю в декілька мегабіт у секунду, і датчик NIDS використовує з'єднання 100 BaseT (швидкість 100 мегабіт у секунду). Таке з'єднання не дозволяє здійснювати передачу даних NIDS, тому в даній конфігурації не представляється можливим переривання з'єднань.

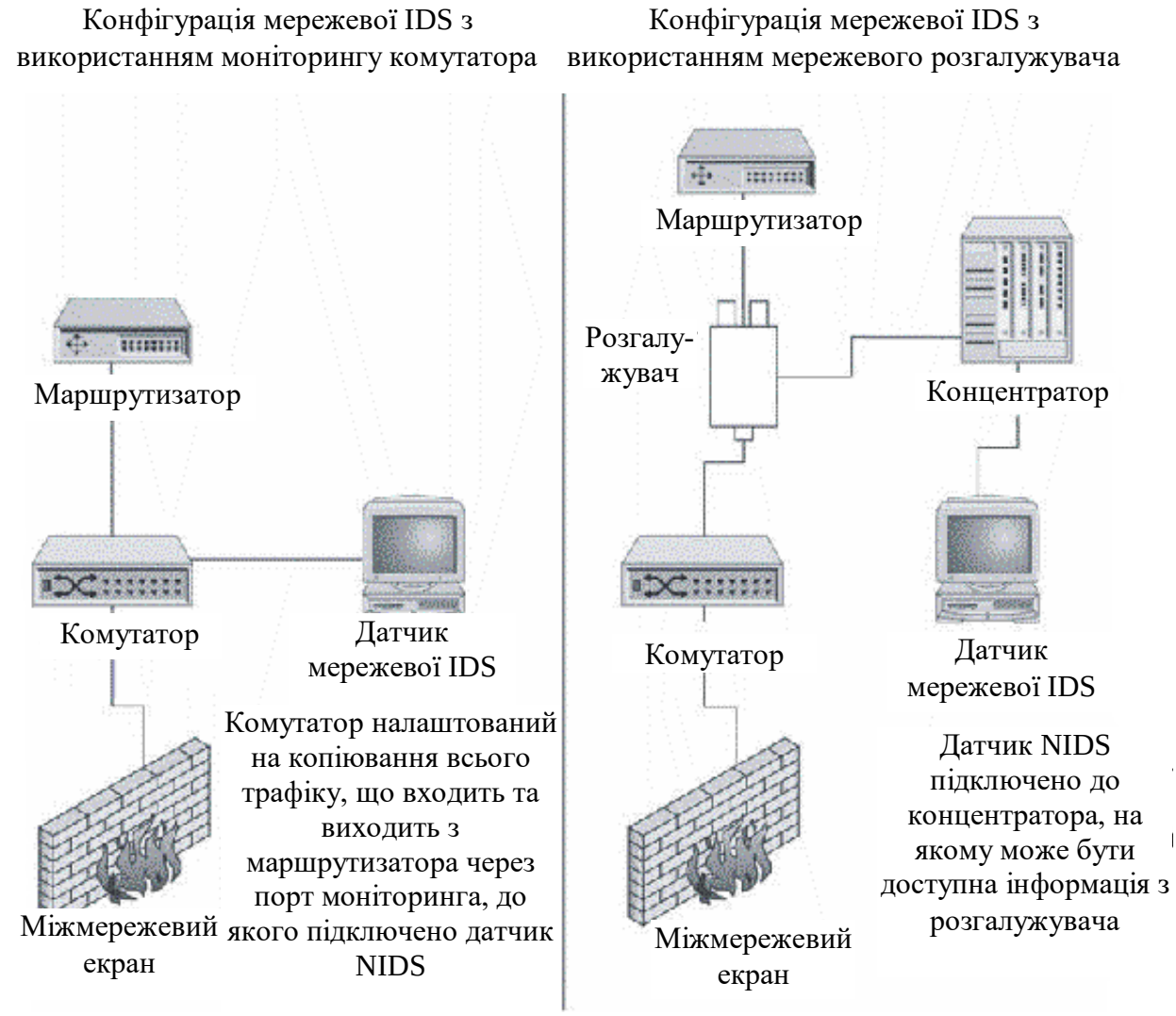

Рисунок 8.4 – Конфігурації датчика мережевої IDS для мережі, що комутується

Розгалужувачі – це пасивні провідні з'єднання між двома пристроями (наприклад, між маршрутизатором і комутатором). Як правило, розгалужувач підключається до концентратора, до якого також приєднаний датчик NIDS. Це дозволяє датчику відслідковувати трафік.

Розгалужувач не дозволяє датчику NIDS здійснювати передачу даних, тому в даній конфігурації переривання з'єднань також неприпустимо.

Вибір відповідних дій

Аналогічно вибору об'єкта моніторингу, вибір відповідних дій залежить від цілей, для яких використовується система IDS. При виникненні події можна вибрати пасивну обробку (відповідна дія, що не перешкоджає діям атакуючого) або активну обробку (відповідна дія, що перешкоджає діям зловмисника). Пасивні відповідні дії не обов'язково мають на увазі дозвіл продовження події, але не допускають виконання безпосередніх операцій самою системою IDS. Цей момент необхідно мати на увазі. Також варто виважено підійти до вибору автоматичної або ручної обробки подій.

Пасивна обробка

Пасивна обробка – це найпоширеніший тип дій, що вживаються при виявленні вторгнення. Причина цьому проста – пасивні відповідні дії забезпечують меншу ймовірність ушкодження легітимного трафіку, будучи, у той же час, найбільш простими для автоматичного застосування. Як правило, пасивні відповідні дії здійснюють збір більшого числа інформації або передають повідомлення особам, що мають право на прийняття більш радикальних заходів:

– ***Запобігання.*** Запобігання спробі атаки є сьогодні найбільше використовуваним методом обробки події атаки. У більшості випадків такий метод обробки подій залишається встановленим за замовчуванням після установки в організації підключення до Інтернету й міжмережевого екрана. Надалі, після виконання всіх дій по налаштовуванню, організації

довіряють захист від атак з Інтернету міжмережевим екранам. Даний тип відповідних дій може використовуватися в більш складних системах IDS. IDS налаштовується на ігнорування атак через неіснуючі служби або служби, щодо яких міжмережевий екран є невразливим. Вагомою підставою для ігнорування атаки служить той факт, що системи не чутливі до розглянутого типу атак; наприклад, це відноситься до атаки Microsoft IIS, спрямованої на веб-сервер Unix, і до атаки Sendmail на сервер Microsoft Exchange. Жодна із цих атак не буде успішної, так як їхні цілі не є вразливими для даних конкретних атак. За допомогою інформації, одержуваної в результаті сканування уразливостей, можна визначити, які події можна безпечно ігнорувати.

– ***Ведення журналів.*** При виникненні події будь-якого типу повинна генеруватися максимально можлива кількість інформації для забезпечення деталізованого аналізу або для допомоги у вживанні подальших заходів. Занесення події в журнал є пасивною відповідною дією, у рамках якої більше не здійснюється ніяких операцій. За допомогою збору основних даних (IP-адреси, дата й час, тип події, ідентифікатори процесу, ідентифікатори користувача й т.д.) IDS ідентифікує подія як щось, що вимагає подальшої уваги.

– ***Ведення додаткових журналів.*** Пасивна обробка подій є більш ефективною, якщо здійснюється збір більшої кількості даних про події що фіксуються у нормальному режимі. Наприклад, якщо звичайний журнал налаштований на збір IP-адрес і номерів портів для всіх з'єднань, то у випадку виявлення події може вироблятися фіксування користувальницьких ідентифікаторів, ідентифікаторів процесів або фіксування всього трафіку, що проходить через з'єднання.

– Ще одним різновидом даного типу обробки події є ***використання виділеного сервера журналів.*** В організації може в різних місцях мережі бути присутнім набір систем ведення журналів, які включаються тільки у випадку виявлення події. Ці виділені сервери журналів здійснюють збір

деталізованої інформації, що потім використовується для ізолювання джерела трафіку, а також як потенційні докази, якщо подія, що відбулася, викличе судовий розгляд.

– ***Повідомлення.*** На відміну від простої констатації того факту, що подія відбулася, повідомлення дозволяють IDS інформувати осіб про подію, що відбулася. Повідомлення може мати всілякі форми, починаючи від мерехтливих вікон і звукових сигналів і закінчуючи поштовими й мобільними повідомленнями. Залежно від обставин той або інший тип більш переважний ніж інший. Наприклад вікна, що мерехтять й сирени не дуже корисні, якщо система IDS веде цілодобовий моніторинг. Поштові повідомлення відправляються у віддалені місця, але можуть не дійти до одержувача вчасно. Вони також можуть викликати великий обсяг мережевого трафіку, у результаті чого зловмисник здогадається про присутність системи IDS. Мобільні повідомлення приходять вчасно (за умови безперебійного функціонування супутника), але можуть не надати досить інформації для вживання відповідних заходів без попереднього перегляду журналів IDS. Налаштовування IDS на відправлення повідомлення при виникненні події може викликати проблеми в поштові або мобільних системах, якщо відбудеться велика кількість подій за дуже малий проміжок часу.

Активна обробка подій

Активна обробка події дозволяє швидко вжити можливих заходів для зниження рівня шкідливої дії події. Однак якщо недостатньо серйозно поставитися до логічного програмування дій у різних ситуаціях і не провести належного тестування набору правил, активна обробка подій може викликати ушкодження системи або повну відмову в обслуговуванні легітимних користувачів:

– ***Переривання з'єднань, сеансів або процесів***. Імовірно, найпростішою дією для розуміння є переривання події. Вона може здійснюватися за допомогою переривання з'єднання, використовуваного

атакуючим зловмисником (це можливо тільки в тому випадку, якщо подія використовує TCP-з'єднання), із закриттям сеансу користувача або завершенням процесу, що викликав неполадку. Визначення того, який об'єкт підлягає знищенню, виконується за допомогою вивчення події. Якщо процес використовує занадто багато системних ресурсів, найкраще завершити його. Якщо користувач намагається використовувати конкретну вразливість або здійснити нелегальний доступ до файлів, то рекомендується закрити сеанс цього користувача. Якщо зловмисник використовує мережеве з'єднання в спробах вивчення уразливостей системи, то варто закрити з'єднання. Дія по знищенню може викликати відмову в обслуговуванні легітимних користувачів. Розберіться в потенційній можливості помилкових сигналів тривоги, перш ніж виконувати відповідну операцію.

– ***Переналаштовування мережі.*** Припустимо, відбулося кілька спроб доступу до комп'ютерів організації з конкретної IP-адреси, отже, є ймовірність того, що з цієї IP-адреси здійснена спроба атаки на інформаційну систему. У цьому випадку може знадобитися переналаштовування міжмережевого екрана або маршрутизатора. Зміна налаштувань може бути тимчасовою або постійною, залежно від IP-адреси й запрограмованих логічних дій (переривання всього трафіку між партнером по бізнесу може негативно позначитися на продуктивності). Нові фільтри або правила можуть заборонити установку будь-яких з'єднань із віддаленим вузлом або заборонити з'єднання лише по конкретних портах.

– ***Обманні дії.*** Найбільш складним типом активної обробки подій є обманні дії. Відповідь обманом спрямована на введення зловмисника в оману за допомогою створення враження успішного й невиявленого проведення атаки. У той же час система-ціль захищається від атаки зловмисника або за допомогою його перенаправлення на іншу систему, або

за допомогою переміщення життєво важливих компонентів системи в безпечне місце.

– Одним з типів обманних дій ***є "горщик з медом".*** Під "горщиком з медом" мається на увазі система або інший об'єкт, що виглядає для зловмисника настільки привабливим, що він не може його пропустити. У той же час за атакуючим ведеться спостереження, і всі його дії записуються. Зрозуміло, інформація в "горщику з медом" не є актуальною, але зовні цей об'єкт виглядає як найбільш важливий компонент інформаційної системи.

Автоматична й автоматизована відповідь

Автоматична відповідь – це набір встановлених операцій, які виконуються при виникненні визначених подій. Такі відповідні дії, як правило, здійснюються в рамках штатної процедури, що визначає конкретні тригери, що ініціюють набір дій. Ці дії можуть варіюватися від пасивних до активних. Автоматичні відповідні дії можуть управлятися людьми або комп'ютерами.

У випадку якщо відповідь на інцидент повністю контролюється комп'ютером без участі людини, такі відповідні дії називаються автоматизованими. Цей тип відповідних дій повинен контролюватися точно визначеним, ретельно продуманим і добре протестованим набором правил. Так як відповідні дії не вимагають участі користувача, вони будуть виконуватися у випадку виявлення відповідності встановленому набору правил. Реалізувати автоматизовані відповідні дії, що примусово знищують мережевий трафік, дуже просто.

У таблиці 8.2 наведені приклади відповідних пасивних і активних відповідних дій з використанням набору політик, що був визначений вище.

Таблиця 8.2 – Приклади відповідних дій, обумовлені політикою IDS

Політика	**Пасивні відповідні дії**	**Активні відповідні дії**
Виявлення атак	Ведення журналів Ведення додаткових журналів Повідомлення	Немає відповідної активної дії.
Запобігання атак	Ведення журналів Повідомлення	Закриття з'єднання. Завершення процесу. Можливе переналаштовування маршрутизатора або міжмережевого екрана.
Виявлення порушень політики	Ведення журналів Повідомлення	Немає відповідної активної дії.
Примусове використання політик	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштовування проксі.
Примусове використання політик з'єднання	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштовування маршрутизатора або міжмережевого екрана.
Збір доказів	Ведення журналів Ведення додаткових журналів Повідомлення	Обманні дії. Можливе закриття з'єднання.

Визначення порогів

Граничні значення забезпечують захист від помилкових спрацьовувань, що підвищує ефективність політики IDS. Граничні

значення можуть використовуватися для фільтрації випадкових подій з метою їхнього відділення від тих подій, які в дійсності являють собою загрозу безпеки. Наприклад, співробітник може підключитися до веб-сайту, не пов'язаного з діловою активністю, перейшовши по посиланню, наданою пошуковою системою. Співробітник може виконувати легітимний пошук, але через некоректно задані параметри пошуку може відобразитися сайт, що не відноситься до роботи. У цьому випадку ця окрема подія не викличе генерацію звіту в системі IDS. Такий звіт просто зайняв би ресурси при вивченні зовсім нешкідливої дії користувача.

Аналогічно, граничні значення, що виявляють атаки, повинні бути налаштовані на ігнорування зондування низького рівня або окремих подій, зв'язаних зі збором інформації. Серед таких подій можна виділити окрему спробу "фінгерингу" (вказівки) співробітника. Програма-вказівник (фінгер), розповсюджена в системах Unix, як правило, використовується для перевірки коректної адреси електронної пошти або для одержання відкритих ключів. Проте, спроби фінгерингу великої кількості співробітників за невеликий проміжок часу можуть бути ознакою того, що зловмисник збирає необхідну інформацію для проведення атаки.

Вибір граничних значень для системи IDS прямо залежить від типів подій і потенційних порушень політики. Неможливо ідентифікувати конкретний універсальний набір граничних значень. Проте, можливо визначити параметри, які необхідно взяти до уваги при налаштовуванні граничних значень. Нижче наведені ці параметри.

– ***Досвід користувача***. Якщо користувач недостатньо досвідчений і допускає безліч помилок, може видаватися занадто багато помилкових сигналів тривоги.

– ***Швидкісні характеристики мережі***. У мережах з низькими швидкостями передачі даних можуть видаватися помилкові сигнали про події, які вимагають одержання визначених пакетів протягом визначеного проміжку часу.

– ***Очікувані мережні з'єднання***. Якщо система IDS налаштована на видачу сигналу тривоги для визначених мережних з'єднань, і ці з'єднання часто мають місце, то буде відбуватися занадто багато помилкових спрацьовувань.

– ***Навантаження на співробітника з адміністрування або безпеки.*** Великий обсяг роботи співробітників, відповідальних за безпеку, може зажадати установку більше високих граничних значень для зниження числа помилкових спрацьовувань.

– ***Чутливість датчика.*** Якщо датчик дуже чутливий, може знадобитися установка більше високих граничних значень, щоб знизити число помилкових спрацьовувань.

– ***Ефективність програми безпеки.*** Якщо програма безпеки організації дуже ефективна, вона може передбачати пропуск деяких атак, пропущених IDS внаслідок наявності в інформаційному середовищі інших засобів захисту.

– ***Наявні уразливості.*** Немає причини для видачі сигналу тривоги у випадку атак на відсутні в мережі уразливості.

– ***Рівень таємності систем і інформації.*** Чим вище рівень таємності інформації, використовуваної в організації, тим нижче повинні бути граничні значення для видачі сигналів тривоги.

– ***Наслідки помилкових спрацьовувань.*** Якщо наслідки помилкових спрацьовувань дуже серйозні, може знадобитися установка більше високих граничних значень для видачі сигналів тривоги.

– ***Наслідки неспрацьовування.*** Навпаки, якщо дуже серйозні наслідки неспрацьовування (або пропущених подій), може знадобитися установка більше низьких граничних значень.

Граничні значення є строго індивідуальними для кожної організації. Можна мати на увазі основні принципи їхнього визначення, але в кожній організації необхідно в окремому порядку розглядати конкретну ситуацію й задавати граничні значення відповідно до наведених вище параметрам.

Застосування системи IDS

Безпосереднє застосування політики IDS повинно ретельно плануватися, як і сама політика. Варто мати на увазі, що до даного моменту політика IDS розроблялася на аркуші паперу з обліком (добре, якщо це так) реальних тестів і досвіду використання. Щоб піддати добре організовану мережу великій небезпеці, у ній досить всього лише встановити неправильно зконфігуровану систему IDS. Отже, після розробки політики IDS і визначення граничних значень необхідно встановити IDS відповідно до кінцевої політики, з мінімальним числом яких-небудь активних дій. Протягом деякого часу при оцінці граничних значень варто уважно стежити за роботою IDS. Таким чином, політика може бути перевірена на практиці без ушкодження легітимного трафіку або переривання легального доступу користувачів до комп'ютерів.

Не менш важливо під час іспитового або початкового строку роботи системи, ретельно проводити вивчення роботи IDS по дослідженню процесів, що відбуваються в системі, щоб оцінити ступінь коректності інформації, що видає IDS.

Помилкове обвинувачення співробітника або зовнішнього користувача внаслідок некоректного визначення факту порушення політики може негативно позначитися на враженні від функціонування системи й поставити в організації питання про ефективність використання програми IDS.

Керування IDS

Концепція виявлення вторгнень – уже не новина в області інформаційної безпеки. Перед прийняттям в організації рішення про використання IDS (будь то комерційна система або некомерційна) керівництво організації повинно чітко визначити цілі застосування програми. Правильне налаштовування й керування IDS вимагає більших зусиль, і ці зусилля треба як можна більш ефективно використовувати для

виявлення атак (за допомогою реалізації гарної програми по забезпеченню безпеки).

Отже, якщо ухвалено рішення про застосування IDS, то для успішної реалізації програми необхідно забезпечити наявність всіх потрібних ресурсів. Якщо цілі програми IDS включають можливість моніторингу в цілодобовому й щоденному моніторингу атак, співробітникам організації знадобиться бути "напоготові" цілодобово сім днів на тиждень. У той же час системним адміністраторам буде потрібно працювати зі співробітниками, відповідальними за безпеку, для визначення успішного або безуспішного проведення атаки й, у випадку успішної атаки, для визначення методу обробки інциденту. В ідеальному випадку процедура по обробці інциденту повинна бути створена й протестована перед застосуванням системи IDS.

Про що може повідомити система IDS

Система виявлення вторгнень може тільки видавати звіти про ті події, на виявлення яких вона налаштована. Конфігурація IDS складається із двох компонентів. Першою з них є ознаки атак, запрограмовані в системі. Другий компонент – будь-яким додаткові, визначені адміністратором, події, що також представляють інтерес. Серед цих подій можуть бути визначені типи трафіку або повідомлень журналу.

За допомогою включення в кінцевий продукт ознак атак постачальник або розроблювач системи по-своєму інтерпретує рівень важливості зазначених подій. Ступінь важливості, що привласнюється визначеним подіям у тій або іншій організації, може бути зовсім інший, ніж той, який передбачив розроблювач. Може знадобитися змінити параметри за замовчуванням для деяких ознак або просто відключити ознаки, не застосовні до організації.

Варто мати на увазі, що система IDS буде видавати попередження тільки про ті події, які вона виявить. Якщо на системі, що відслідковується датчиком HIDS, не заносяться в журнал визначені події, то датчик HIDS не

буде їх розпізнавати. Аналогічно, якщо датчик NIDS не може "бачити" визначений трафік, він не видасть попередження навіть у тому випадку, якщо подія відбудеться.

З умовою правильної конфігурації IDS можна привести чотири типи подій, про які буде повідомляти система IDS:

– Події дослідження.

– Атаки.

– Порушення політики.

– Підозрілі або непояснені події.

Більша частина часу буде приділятися дослідженню підозрілих подій.

Події дослідження

Події дослідження являють собою спроби атакуючого зібрати дані про систему перед безпосереднім проведенням атаки. Ці події можна розділити на п'ять категорій:

– "Сховане" сканування.

– Сканування портів.

– Сканування "троянських коней".

– Сканування уразливостей.

– Відстеження файлів.

Більша частина цих подій відбувається в мережі, в основному, вони виходять з Інтернету й спрямовані на системи із зовнішніми адресами.

Події дослідження виявляють собою спроби збору інформації про системи. Вони не є подіями, що впливають на систему. Деякі комерційні IDS сприймають події дослідження як події високого пріоритету. З обліком того, що ці події не наносять збитку системі, такий підхід можна рахувати нерозумним.

Джерелом подібного трафіку може бути й інша система-жертва, захоплена зловмисником, тому дану інформацію варто повідомляти системним адміністраторам цього вузла.

Сховане сканування. Сховане сканування – це спроби ідентифікації систем, що є присутні у мережі, з метою запобігти виявленню системи, з якої буде проводитися атака. Цей тип сканування буде визначатися датчиками NIDS як половинчасте сканування IP або сховане сканування IP, і, як правило, таке сканування спрямоване на велике число IP-адрес. Відповідною реакцією є ідентифікація джерела й інформування власника системи-джерела про те, що його система, швидше за все, піддалася впливу зловмисника.

Сканування портів. Сканування портів використовується для визначення служб, що працюють в системах мережі. Системи виявлення вторгнень виявляють сканування портів у випадку, коли визначене число портів (відповідне граничному значенню) на одній системі відкривається протягом невеликого проміжку часу. Датчики NIDS і деякі датчики HIDS забезпечують ідентифікацію даного типу сканування й становлять відповідні звіти. Відповідні дії на сканування даного типу ідентичні відповідним діям на сховане сканування.

Сканування "троянських коней". Існує безліч шкідливих програм типу "троянський кінь". Датчики NIDS містять ознаки, що визначають багато які з цих програм. На жаль, трафік, спрямований на "троянські" програми, як правило, визначається кінцевим портом пакета. Ця обставина викликає велику кількість помилкових спрацьовувань системи виявлення вторгнень. У випадку виникнення події "Trojan" варто перевіряти вихідний порт трафіку. Приміром, трафік, що виходить із порту 80, як правило, надходить із веб-сайту.

Одним з найпоширеніших типів "троянського" сканування є сканування BackOrifice. Програма BackOrifice використовує порт 31337, і дуже часто зловмисники здійснюють сканування діапазону адрес для цього порту. Консоль BackOrifice також містить функцію "ping host" (відправлення пінг-запитів на вузли), що здійснює сканування автоматично. Турбуватися не треба, поки не буде зафіксований вихідний

трафік із внутрішньої системи. Знов-таки, у цьому випадку потрібно зв'язатися із власником системи-джерела, так як вона, імовірно, піддалася впливу зловмисника.

Сканування уразливостей. Сканування уразливостей розпізнається системою IDS при виявленні великого набору різних ознак атак. Як правило, таке сканування спрямоване на кілька систем. Рідкі випадки, коли сканування уразливостей виробляється стосовно діапазону адрес без активних систем.

Сканування уразливостей, здійснюване хакерами, неможливо відрізнити від сканування уразливостей, проведеного компаніями, які перевіряють рівень захищеності інформаційних систем (у багатьох випадках у цих компаніях використовуються ті ж самі засоби). Так чи інакше, саме по собі сканування не заподіює системі якої-небудь шкоди, однак якщо атакуючий виконав сканування, у результаті якого виявилися системи з уразливостями до атаки, йому після цього стає відомо, які системи можна атакувати. Для забезпечення відповідності комп'ютерних систем актуальним проблемам безпеки варто контактувати із власником системи-джерела й перевіряти внутрішні системи організації на наявність самих останніх програм безпеки й відновлень.

Як правило, складно відрізнити сканування уразливостей від атаки, так як IDS в обох випадках ініціює ті самі події. Різниця тут полягає в кількості подій. Сканування уразливостей, як правило, супроводжується великим числом різних подій за дуже малий відрізок часу, у той час як при проведенні атак відбуваються події одного типу.

Відстеження файлів. Відстеження файлів або перевірка, як правило, здійснюється внутрішнім користувачем. Користувач намагається визначити, до яких файлів можна здійснити доступ і що ці файли можуть містити. Даний тип розвідки розпізнається тільки датчиком HIDS і тільки в тому випадку, якщо в системі ведеться журнал спроб несанкціонованого доступу. Окремі події подібного роду, як правило, являють собою

безневинні помилки, однак якщо простежується визначена схема, то варто зв'язатися з користувачем і з'ясувати, що ж відбулося.

Атаки

Події атак вимагають найшвидшої відповідної реакції. В ідеальному випадку IDS повинна бути налаштована тільки на ідентифікацію подій високого пріоритету у випадку використання відомої внутрішньої уразливості. У цьому випадку повинна бути негайно застосована процедура обробки інциденту.

Майте на увазі, що IDS не розпізнає різницю між безпосередньою атакою й скануванням уразливостей, що виглядає як атака. Адміністратор системи IDS повинен проводити оцінку інформації, представленою системою IDS, для визначення того, чи є подія атакою. По-перше, необхідно з'ясувати число подій. Якщо протягом короткого проміжку часу спостерігався набір ознак різних атак, то це, швидше за все, сканування уразливостей, а не безпосередня атака. Якщо ж виявлена одна ознака атаки, спрямована на одну або кілька систем, то ця подія може являти собою справжню атаку.

Порушення політики

Більша частина систем IDS поставляється з ознаками наступних подій:

– Загальний доступ до файлів (Gnutella, Kazaa і т.д.);

– обмін миттєвими повідомленнями;

– сеанси Telnet;

– команди "r" (rlogin, rsh, rexec).

У більшій частині організацій використання такого трафіку є порушенням політики безпеки. На жаль, такі порушення політики можуть представляти для організації більшу небезпеку, ніж безпосередні атаки. У більшості випадків подія відбувається в дійсності. Таким чином, відкривається доступ до файлів, і системи налаштовуються на дозвіл виконання команди rlogin.

Вибір методу обробки різних порушень політики залежить від внутрішніх політик і процедур, що мають місце в організації. Проте, необхідно роз'яснити всі моменти системному адміністраторові або відповідальній особі, щоб йому стала ясна суть політик організації.

Підозрілі події

Події, що не відповідають повністю ні одній з інших категорій, заносяться в категорію підозрілих подій. Підозрілою подією називається подія, що не вдалося розпізнати. Наприклад, ключ реєстру Windows NT був змінений з незрозумілої причини. Це не схоже на атаку, але в той же час не ясно, з якої причини змінився ключ. Як інший приклад можна привести пакет із прапорами заголовка, що порушують стандарт протоколу. Це може бути спроба розвідувального сканування, результат несправності мережної карти системи або пакет, при передачі якого виникли помилки. У даних, видаваних системою IDS, не надається досить відомостей для чіткого визначення конкретної ситуації й з'ясування того, що відбулося – помилка або атака.

Не менш підозрілим може виявитися несподіваний мережевий трафік, що з'явився у внутрішній мережі. Якщо робоча станція починає запитувати SNMP-дані з інших систем, то це може бути як наслідком атаки, так і неправильної конфігурації. Підозрілі події необхідно досліджувати настільки, наскільки дозволяють це робити наявні ресурси.

Дослідження підозрілих подій може бути дуже трудомістким завданням. Нерідко представляється розумним пропустити деякі із цих подій або просто передати інформацію мережевому або системному адміністраторові.

Дослідження підозрілих подій

При виникненні підозрілих дій варто виконати процедуру, що складається з наступних кроків, щоб визначити, чи є дана дія вдалим вторгненням або спробою проникнення, або вона носить нешкідливий характер. Отже, потрібно виконати наступні кроки:

– Ідентифікувати систему;

– записувати в журнал відомості про додатковий трафік між джерелом і пунктом призначення;

– записувати в журнал весь трафік, що виходить із джерела;

– записувати в журнал вміст пакетів із джерела.

При виконанні кожного кроку необхідно визначати, чи досить очевидних ознак для з'ясування того, чи є дана дія атакою. У наступних розділах приводиться опис даних кроків.

При дослідженні події необхідно мати на увазі наступний момент. Якщо подія відбувається один раз і більше не повторюється, то дуже важко одержати яку-небудь додаткову інформацію (крім того, звідки надійшов трафік). Одиночні аномалії досліджувати практично неможливо.

1. Ідентифікація систем

Першим кроком при дослідженні підозрілої активності є ідентифікація систем, що беруть участь у дії. Ця процедура може полягати в перетворенні IP-адрес в іменах вузлів. У деяких випадках ім'я вузла знайти не вдається (система не має записи DNS; це клієнт DHCP; віддалений DNS-сервер перебуває в неактивному стані й т.д.). Якщо пошук DNS закінчується невдачею, то варто спробувати ідентифікувати вузол іншими способами, наприклад, пошуком у реєстрі American Registry of Internet Numbers (ARIN) за адресою http://www.arin.net/, в Internic за адресою http://www.networksolutions.com/ або в інших каталогах Інтернету. Утиліти, такі як Sam Spade (перебувають за адресою http://samspade.org/), також допоможуть у цьому випадку. Неможливість ідентифікації джерела або пункту призначення підозрілих дій не є достатнім доказом того, що подія в дійсності є атакою. Аналогічно, успішна ідентифікація систем не є достатнім доказом "необразливості" виявлених дій.

Джерело підозрілого трафіку може не бути безпосереднім джерелом атаки. Спроби проведення атаки на відмову в обслуговуванні, як правило, проводяться з підміненими вихідними адресами, і спроби

несанкціонованого доступу або зондування можуть виходити з інших систем, захоплених зловмисником.

2. Запис у журнал додаткового трафіку між джерелом і пунктом призначення

Одна-єдина окрема подія (наприклад, порушення протоколу IP) може не представляти повну інформацію про трафік між двома системами. Іншими словами, необхідно розуміти контекст підозрілих дій. Гарним прикладом тут служить ознака атаки Sendmail WIZ. Ця ознака ідентифікує спробу використання команди WIZ у програмі Sendmail. Дана подія безпеки ідентифікує будь-яке входження команди WIZ у повідомленні. Якщо команда WIZ є присутнім у тілі повідомлення, то це виразно не спроба вторгнення. Розуміння контексту події допомагає визначати помилкові спрацьовування.

Налаштуйте IDS на відстеження всього трафіку між джерелом підозрілої активності й пунктом призначення. Як приклад використовуйте таблицю 8.3.

Таблиця 8.3 – Приклад конфігурації IDS із записом у журнал усього трафіку між двома системами

Ім'я події	**Дія**	**IP-адреса джерела**	**IP-адреса пункту призначення**	**Протокол**	**Порт джерела**	**Кінцевий порт**
SUS_ACT	Повідомлення, занесення в журнал	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP,UDP і/або ICMP, залежно від типу виявленої активності	Будь-який	Будь-який

Тепер задамося питанням, що ж це все нам дає. По-перше, ми одержуємо подання про інший трафік, що має місце між джерелом і пунктом призначення. Якби пакет WIZ був єдиним трафіком між двома системами, із цього можна було зробити висновок про те, що це схоже на спробу проникнення в систему. Навпроти, якщо спостерігається велике число трафіку SMTP (пошти) між двома системами, то, швидше за все, це звичайний легітимний поштовий трафік.

3. Запис у журнал усього трафіку із джерела

Мається на увазі, що даних, фіксуємих за допомогою запису всього трафіку між двома системами, недостатньо для визначення того, чи є активність легітимною, можна почати збір іншого трафіку, що надходить із джерела. Майте на увазі, що обсяг цього трафіку може бути обмеженим. Якщо джерело підозрілої активності перебуває в деякій віддаленій мережі, то буде спостерігатися тільки трафік, що надходить на ваш вузол. Якщо ж джерело локальне, то можливий збір усього трафіку з даного комп'ютера, що дасть набагато більше широке подання про те, що ж насправді відбувається. Щоб почати збір усього трафіку із джерела, налаштуйте детектор IDS на збір всієї інформації з підозрілого джерела. Приклад такої конфігурації наведений у таблиці 8.4.

Таблиця 8.4 – Приклад конфігурації IDS, призначеної для занесення в журнал усього трафіку, що виходить із визначеної адреси джерела

Ім'я події	**Дія**	**IP-адреса джерела**	**IP-адреса пункту призначення**	**Протокол**	**Порт джерела**	**Кінцевий порт**
SUS_SRC	Повідом-лення, запис у журнал	Джерело підозрілих дій	Будь-який	TCP,UDP і/або ICMP, залежно від типу виявленої активності	Будь-який	Будь-який

Така конфігурація, як правило, генерує деяку інформацію, що не представляє якої-небудь цінності для дослідження. Доти, поки можливо об'єктивно оцінити інформації, даний журнал можна використовувати для складання докладної картини взаємодій, що відбуваються, що мають місце між джерелом і пунктом призначення. Спробуйте вникнути в суть спостережуваної активності. Чи є спостережувана активність веб-трафіком? чи Виходить трафік з підозрілого джерела, або ж його джерелом є ваш вузол?

На даному етапі дослідження повинна бути відома наступна інформація:

– ім'я системи-джерела;

– тип і частота трафіку, обмін яким відбувається між джерелом і пунктом призначення;

– тип і частота трафіку, обмін яким відбувається між джерелом і будь-якими іншими системами вашого вузла.

Ця інформація забезпечує досить докладне подання про природу підозрілого трафіку. Проте, ступінь очевидності що відбувається може не сказати про те, чи є спостережувана активність спробою атаки.

4. Запис у журнал умісту пакетів із джерела

Кінцевим кроком проведеного дослідження є запис у журнал умісту пакетів, що виходять із джерела. Варто помітити, що даний підхід корисний тільки при роботі з текстовими протоколами, такими як telnet, FTP, SMTP і HTTP (до деякої міри). Якщо використовуються двійкові протоколи або протоколи із шифруванням, даний підхід зовсім марний. Для реалізації описаного методу необхідно змінити конфігурацію IDS, як показано в таблиці 8.5.

За допомогою занесення в журнал вмісту пакетів можна скласти повний запис сеансу, а також зафіксувати команди, призначення, що відправляються безпосередньо в пункт.

Після фіксування деяких даних необхідно переглянути знайдену інформацію. Чи позначає сеанс потенційну атаку, або ж все виглядає в межах припустимого? Скомбінувавши ці дані з іншою знайденою інформацією, можна знайти відповідь на це питання. Якщо цього зробити не вдалося, спробуйте знайти людину, у якої є досвід роботи з досліджуваним протоколом.

Таблиця 8.5 – Приклад конфігурації IDS, що здійснює перехоплення вмісту пакетів

Ім'я події	**Дія**	**IP-адреса джерела**	**IP-адреса пункту призначення**	**Прото-кол**	**Порт джерела**	**Кінце-вий порт**
SUS_ACT	Повідом-лення, запис у журнал умісту пакета	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP або UDP	Будь-який	Порт, на який спрямо-ваний підозрі-лий трафік
SUS_ACT	Повідом-лення, запис у журнал умісту пакета	Пункт призначення з підозрілої активності	Джерело підозрілої активності	TCP або UDP	Порт, на який спрямо-ваний підозрі-лий трафік	Будь-який

Розгортання мережної IDS

Даний проект покликаний продемонструвати процес розгортання мережної IDS. Він починається з попередніх етапів, які необхідно виконувати перед безпосередньою процедурою розгортання. При бажанні можете насправді здійснити розгортання датчика мережний IDS.

Крок за кроком

1. Визначте, які дії ви намагаєтеся здійснити за допомогою розгортання датчика IDS. Це допоможе чітко обрисувати цілі застосування IDS.

2. На основі цілей застосування IDS визначите, який мережний трафік потрібно відслідковувати.

3. Тепер вирішіть, яким чином будуть оброблятися різні події, що виявляються IDS. Спробуйте визначити, що буде розумніше – доручити виконання деякої дії системі IDS або операторові, що буде виконувати потрібну процедуру.

4. При відсутності досвіду роботи з датчиком IDS вам доведеться нелегко при першій установці граничних значень. Якщо у вашому огляді є вже функціонуюча система IDS, можете подивитися, які граничні значення встановлені на цій системі для різних ознак атак.

5. Складіть план розгортання IDS. Визначте, кого в організації потрібно задіяти для виконання цього завдання.

6. Якщо ви хочете спробувати здійснити розгортання датчика NIDS, виділіть для цього комп'ютер і встановіть на нього Linux, FreeBSD або іншу версію операційної системи сімейства Unix.

7. Завантажте останню версію програми Snort (безкоштовна IDS) із сайту http://www.snort.org/.

8. Додержуйтеся інструкцій по установці й виконаєте інсталяцію програми Snort. Можна також установити ряд додаткових програмних пакетів для спрощення процесу керування й конфігурації.

9. Підключіть датчик до мережі. Найкраще зробити це за допомогою концентратора. Проте, можна також використовувати порт розгалужувача на комутаторі.

10. Розмістивши датчик на потрібному місці, перегляньте файли журналів, щоб з'ясувати, які події в них фіксуються. Також можна використовувати програму Acid для перегляду файлів журналу через веб-

інтерфейс. Acid – це веб-інтерфейс, використовуваний для аналізу даних програми Snort.

Отже, при наявності деякого досвіду роботи з операційною системою Unix вам буде нескладно розібратися із програмою Snort. Дана вправа допоможе виконати кроки по установці датчика NIDS. Однак якщо ви маєте намір використовувати його як діючий датчик в організації, необхідно заручатися підтримкою мережевих і системних адміністраторів організації. Також не слід думати, що цей проект удасться виконати за один день. Налаштовування датчика й оцінка результатів його роботи потребує деяких часових витрат.

РОЗДІЛ 9. СИСТЕМИ ПРОТИДІЇ ВТОРГНЕННЯМ (IPS-СИСТЕМИ)

Система запобігання вторгнень (англ. Intrusion Prevention System) – програмна або апаратна система мережевої й комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки й автоматично захищає від них.

Системи IPS можна розглядати як розширення Систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковим. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність у реальному часі й швидко реалізовувати дії по запобіганню атак. Можливі міри – блокування потоків трафіку в мережі, скидання з'єднань, видача сигналів операторові. Також IPS можуть виконувати дефрагментацію пакетів, переупорядкування пакетів TCP для захисту від пакетів зі зміненими SEQ і ACK номерами.

Запобігання вторгнень

Запобігання вторгнень стало основним завданням розроблювальних останнім часом продуктів в області виявлення вторгнень. Нові концепції спрямовані на зміну природи IDS за допомогою додавання функцій по запобіганню вторгнень замість тільки виявлення. Багато продуктів, що відповідають цієї концепції, є зовсім новими на ринку. Проте, зазначена функціональність реалізована в ряді продуктів вже зарекомендувала себе.

IDS/IPS-системи використовуються для виявлення аномальних дій у мережі, які можуть порушити безпеку й конфіденційність даних, наприклад: спроби використання уразливостей програмного забезпечення; спроби підвищення привілеїв; несанкціонований доступ до конфіденційних даних; активність шкідливих програм і т.д.

Використання IPS-систем переслідує кілька цілей:

– виявити вторгнення або мережну атаку й запобігти їм;

– спрогнозувати можливі майбутні атаки й виявити уразливості для запобігання їхнього подальшого розвитку;

– виконати документування існуючих погроз;

– забезпечити контроль якості адміністрування з погляду безпеки, особливо великих і складних мереж;

– одержати корисну інформацію про проникнення, які мали місце, для відновлення й коректування факторів, що викликали проникнення;

– визначити розташування джерела атаки стосовно локальної мережі (зовнішні або внутрішні атаки), що важливо при прийнятті рішень про розташування ресурсів у мережі.

У цілому, IPS аналогічні IDS. Головна ж відмінність полягає в тому, що вони функціонують у реальному часі й можуть в автоматичному режимі блокувати мережні атаки. Кожна IPS містить у собі модуль IDS.

IDS, у свою чергу, звичайно складається з:

– системи збору подій;

– системи аналізу зібраних подій;

– сховища, у якому накопичуються зібрані події й результати їхнього аналізу;

– бази даних про уразливості (цей параметр є ключовим, так як чим більше база у виробника, тим більше погроз здатна виявляти система);

– консолі керування, що дозволяє будувати всі системи, здійснювати моніторинг стану мережі, яка захищається, переглядати виявлені порушення й підозрілі дії.

Класифікація:

– Мережні IPS (Network-Based Intrusion Prevention, NIPS): відслідковують трафік у комп'ютерній мережі й блокують підозрілі потоки даних.

– IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS): перевіряє активність у бездротових мережах. Зокрема, виявляє невірно зконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфінг mac-адрес.

– Поведінковий аналіз мережі (Network Behavior Analysis, NBA): аналізує мережний трафік, ідентифікує нетипові потоки, наприклад DoS і DDoS-атаки.

– Система запобігання вторгнень для окремих комп'ютерів (Host-Based Intrusion Prevention, HIPS): резидентні програми, що виявляють підозрілу активність на комп'ютері.

За способами моніторингу IPS-системи можна розділити на дві великі групи: NIPS (Network Intrusion Prevention System) і HIPS (Host Intrusion Prevention System). Перша група орієнтована на мережевий рівень і корпоративний сектор, у той час як представники другої мають справу з інформацією, що зібрана всередині єдиного комп'ютера, а отже можуть використовуватися на персональних комп'ютерах.

Серед NIPS і HIPS також виділяють:

– ***Protocol-Based IPS, PIPS.*** Являє собою систему (або агент), що відслідковує й аналізує комунікаційні протоколи зі зв'язаними системами або користувачами.

– ***Application Protocol-Based IPS, APIPS***. Являє собою систему (або агент), що веде спостереження й аналіз даних, переданих з використанням специфічних для визначених застосунків протоколів. Наприклад, відстеження вмісту SQL-команд.

Що стосується форм-фактора, IPS-системи можуть бути представлені як у вигляді окремого «залізного» рішення, так і у вигляді віртуальної машини або софта.

HIPS

HIPS (Host-Based Intrusion Prevention System, англ. система запобігання вторгнень) – проактивна технологія захисту, побудована на аналізі поводження.

Принцип роботи

В силу того що HIPS є засобом проактивного захисту, програми даного класу не містять бази даних сигнатур вірусів (однак можуть їх задіяти, скажемо HIPS у складі антивірусу може блокувати запуск відомих шкідливих програм незалежно від включення або відключення файлового монітора) і не здійснює їх деактування. HIPS-продукти здійснюють аналіз активності програмного забезпечення й всіх модулів системи й блокування потенційно небезпечних дій у системі користувача. Аналіз активності здійснюється за рахунок використання перехоплювачів системних функцій або установці так званих міні-фільтрів. Слід зазначити, що ефективність HIPS може доходити до 100%, однак більшість програм цього класу жадають від користувача високого рівня кваліфікації для грамотного керування антивірусним продуктом.

Види HIPS:

– ***Класичні HIPS.*** Класичні HIPS-продукти надають користувачеві інформацію про активність того або іншого застосунку, однак рішення про дозвіл/заборону тої або іншої операції повинен приймати користувач, таким чином класичні HIPS-продукти дозволяють користувачеві тонко налаштувати ті або інші правила контролю, але створення правил вимагає високої кваліфікації користувача.

– ***Експертні HIPS***. На відміну від класичних HIPS-продуктів, експертні HIPS можуть самостійно ухвалювати рішення щодо блокуванні тієї або іншої активності, виходячи з правил і алгоритмів, закладених розроблювачем продукту. Для використання експертних HIPS-продуктів користувачеві не обов'язково мати визначену кваліфікацію, однак експертні HIPS-продукти в ряді випадків можуть блокувати легітимну

активність користувальницького програмного забезпечення, або можуть не визнати дану активність програми за шкідливу.

Механізми ухвалення рішення IPS

Ухвалення рішення про вторгнення – ключовий момент у роботі IPS. Вся інформація, що збирається системою, всі підходи до збору інформації, всі алгоритми, використовувані при обробці зібраної інформації, спрямовані на одне – забезпечити більшу виваженість і обґрунтованість прийнятих рішень. Серед питань, пов'язаних з механізмами прийняття рішень, можна виділити наступні:

– По-перше, наскільки повні вихідні дані, з яких джерел вони зібрані?

– По-друге, скільки підходів використовуються при ухваленні рішення і які вони?

– По-третє, наскільки обмежений у ресурсах (часових, обчислювальних, пам'яті, базі даних) хост, відповідальний за прийняття рішення про вторгнення?

– По-четверте, чи передбачена можливість втручання оператора в процес ухвалення рішення?

– І, нарешті, чи існують недетерміновані ситуації, у яких системі потрібне втручання оператора?

Механізми протоколювання, використовувані в IPS, викликають найменше дебатів. Можна говорити про прийняті "де-факто" стандарти протоколювання інформації, використовуваних в IPS. Як правило, кожна IPS підтримує як стандартні механізми передачі інформації – повідомлення syslog, повідомлення SNMP-trap, так і розроблений конкретним виробником захищений канал передачі інформації.

При використанні безлічі модулів IPS у великій розподіленій мережі генерується колосальний обсяг реєструємої інформації, обробка якої вручну не представляється можливої. Відповідно, більшість виробників IPS прагнуть уже сьогодні ввести додаткові засоби

перетворення елементарних подій в "макро-події", що мають зміст для адміністратора безпеки.

Механізми керування IPS: віддалені й централізовані

До питань, які мають першочергове значення при розгляді питань надійності механізмів віддаленого керування системою IPS, а отже, і надійності її функціонування в цілому, відносяться наступні:

– Наскільки надійні використовувані в IPS механізми віддаленого керування й наскільки вони розвинені?

– Чи будуть канали керування успішно функціонувати у випадку проведення DDoS-атаки на мережу?

– Чи може внутрішній зловмисник одержати керування системою IPS і модифікувати логіку її роботи?

До питань, які можуть здаватися не настільки значними, однак саме вони забезпечують зручність і ефективність централізованого керування розподіленою системою модулів IPS, відносяться наступні:

– Чи передбачені в IPS механізми централізованого завдання нових правил реакції IPS з їх наступним вибірним впровадженням на окремі модулі IPS?

– Чи можливо об'єднання окремих IPS у групи й формування групових політик?

Можливість інтеграції IPS з іншими системами

Чи можлива інтеграція даного модуля IPS із системою IPS іншого виробника? Які обмеження? Які можливості інтегрованого рішення? Найчастіше кінцевий користувач був би радий встановити декілька IPS-рішень різних виробників, наприклад, для підвищення надійності, але при цьому необхідно забезпечити погоджену роботу цих систем.

При впровадженні IPS користувачі чекають, що вони одержать гнучке, але одночасно абсолютно надійне рішення, що володіє мінімумом помилкових спрацьовувань, що дозволяє користувачам протистояти всім погрозам, що існують у їхніх мережах, включаючи нові, виникаючі в міру

розвитку мережних сервісів. Природно, що рішення повинне бути зручним у керуванні й гарантувати контроль ситуації у всій інфраструктурі інформаційних систем користувачів. І при цьому, щоб "усе працювало".

Яким чином можна запобігти вторгненням за допомогою системи IDS

Щоб запобігти вторгненню, необхідно або зупинити здійснювану атаку перед її досягненням системи-жертви, або зупинити дію атаки перед виконанням на системі-жертві коду, що використовує уразливість.

Механізм запобігання атаки легше всього розглядати на вузлі, що використовує HIDS. Наприклад, можна використовувати аналізатори системних викликів або поводження застосунку. Якщо виклик застосунку схожий на атаку, аналізатор системних викликів запобіжить виконанню виклику операційною системою. Якщо застосунок намагається виконати неавторизовану операцію, аналізатор поводження застосунку запобіжить її виконанню. В обох випадках HIDS запобігає атаці.

Процес запобігання атаки за допомогою NIDS є більше складним. У стандартній конфігурації NIDS датчик розташовується в тому місці, з якого він може відслідковувати трафік (див. рисунок 8.2, розділ 8). При надходженні через канал зв'язку даних атаки, датчик перехоплює пакет і починає його аналізувати. У деякий момент датчик визначає, що пакет являє собою атаку, і вживає дію. Ця дія, як правило, полягає в закритті з'єднання (тільки якщо атака проводиться через з'єднання TCP) або в переналаштовуванні міжмережевого екрана для блокування подальшого трафіку із джерела.

На жаль, у випадку з NIDS час працює не на користь досягнення цілі. Під час аналізу пакета датчиком пакет продовжує свій рух по мережі. У більшості випадків пакет досягає цілі ще перед закриттям з'єднання або виконанням дій по переналаштуванню міжмережевого екрана. Отже, найчастіше атака випереджає дії датчика по її запобіганню.

Закриття з'єднання або блокування трафіку з атакуючої системи може знизити рівень ушкодження системи, але не запобіжить впливу на неї зловмисника.

Для запобігання за допомогою NIDS успішного проведення атак на систему рішення по пакету повинно прийматися до того, як пакет досягне системи-цілі. Це означає, що архітектуру системи NIDS потрібно змінити таким чином, щоб датчик NIDS був розташований на одному каналу зв'язку із трафіком (як міжмережевий екран), а не просто стежив за минаючим трафіком (див. рисунок 9.1).

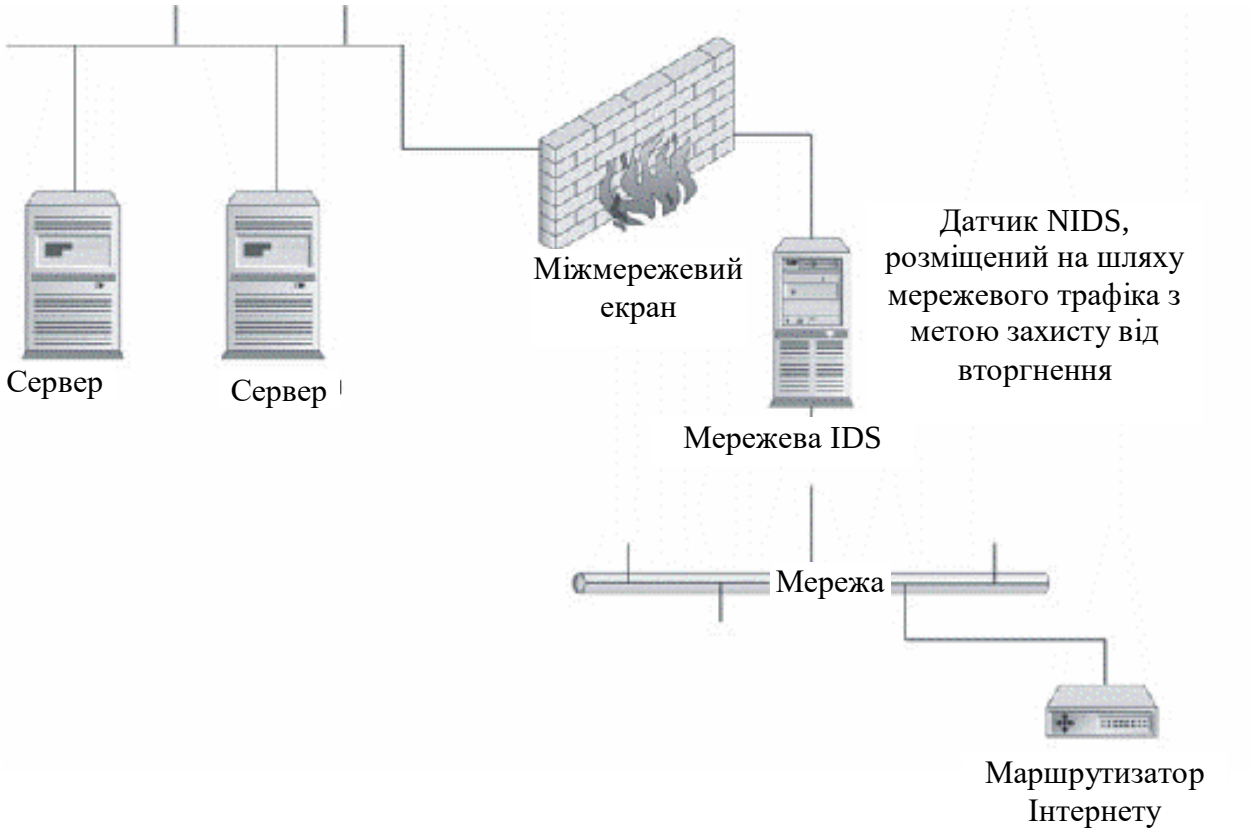

Рисунок 9.1 – Конфігурація, необхідна для запобігання атак датчиком NIDS

Розглянута архітектура не є єдино можливою. Також можливо розташувати датчик NIDS на міжмережевому екрані або реалізувати його тісний взаємозв'язок з міжмережним екраном, щоб останній не пропускав трафік без дозволу датчика NIDS.

Проблеми, пов'язані з виявленням вторгнень

Заміна реактивної природи IDS на превентивну створює деякі проблеми. Дійсно, після цієї зміни виникають два серйозних питання: потенційна можливість відмови в обслуговуванні й недостатній середній рівень доступності.

Відмова в обслуговуванні

При запобіганні вторгнень головним механізмом обробки більше не є повідомлення системи, мережі й системні адміністратори. Тепер "ядром" системи є блокування спроби виконання дії. Коли IDS блокує атаку, вона запобігає виконанню дії, будь то системний виклик, операція застосунку або мережне з'єднання. Дане блокування запобігає атаці. Очевидно, при цьому мається на увазі коректна ідентифікація системою IDS дії як атаки.

Якщо дія, спроба якої була здійснена, насправді не була атакою, а IDS заблокувала її, то, можливо, IDS заблокувала законну дію, що виконувалася в інформаційному середовищі. Внаслідок цього IDS може викликати відмову в обслуговуванні. Якщо дію, що викликала проблему, являло собою деяку аномалію (наприклад, пакет з помилками), то повторна передача пакета або повторна установка з'єднання, як правило, здійснюються успішно. Проте, якщо IDS некоректно ідентифікує легітимні дії або трафік, приймаючи їх за атаки, то, швидше за все, відмова в обслуговуванні буде відбуватися й надалі.

Сучасні датчики IDS видають безліч помилкових сигналів тривоги. Вживання превентивних заходів без повного розуміння характеристик помилкових спрацьовувань і характеристик легітимних дій, як правило, є причиною виникнення проблем.

Доступність

Доступність мереж і систем є важливою властивістю багатьох комп'ютерних систем. Організації затрачають величезну кількість часу й грошей на налаштовування своїх мереж і систем на зниження числа одиночних неполадок. Якщо датчик IDS установлений так, що через нього

повинен проходити весь мережевий трафік, датчик NIDS повинен відповідати високому рівню вимог до доступності інших компонентів мережі. Те ж саме відноситься й до датчиків HIDS, розташованих на вузлі. Чи буде вузол продовжувати функціонувати у випадку збоїв програмного забезпечення датчика, або ж він також буде відключений? В інформаційному середовищі, в якому дуже важливий фактор доступності, необхідно вирішити зазначені питання перед установкою таких систем.

Відповідальність

Мережна IPS має можливість і, більше того, зобов'язана блокувати передачу трафіку, що становить атаку. Разом з тим, мережна IPS не повинна допускати блокування легітимного трафіку. Відповідно, одним із критично важливих показників IPS є кількість помилкових спрацьовувань. Чи можна довірити ухвалення остаточного рішення конкретному пристрою, що володіє обмеженими фізичними й тимчасовими ресурсами (з урахуванням вимог по продуктивності IPS)? Чим забезпечується низька кількість помилкових спрацьовувань і чи можна якось його понизити?

Повнота контролю трафіку

Можливості IPS по контролі трафіку обмежені тими протоколами, засобу аналізу які закладені в програмне забезпечення системи. Разом з тим постійно виникають нові популярні серед користувачів сервіси й механізми мережевої взаємодії, що володіють своїми уразливостями. Який список протоколів, контрольованих IPS? Чи відповідає цей список політиці організації, зацікавленої у впровадженні IPS? Які способи оперативного поповнення списку підтримуваних протоколів?

Гнучкість підходу: можливість модифікації списку погроз

Навіть у самій ефективно зробленій підтримуваній IPS не можуть бути заздалегідь передбачені всі можливі уразливості добре пророблених базових протоколів. Більше того, деякі можливості взаємодії, які не були передбачені в лабораторії, у якій розроблялася IPS, можуть зустрітися на практиці й не бути спробою руйнівного впливу. Чи надає IPS можливість

доробки списку погроз, опису додаткових погроз або виключення зі списку погроз деяких взаємодій по запиті адміністратора?

Повнота бачення/структура IPS

Рівень 1 – мережа

При роботі в реальній мережі нерідко виникають ситуації, коли трафік, що направляється через кілька пристроїв мережних IPS паралельно, не задовольняє критеріям вторгнення, а при розгляді його в сукупності, є вторгненням. Якщо мережні IPS мають можливість взаємодії, або якщо в інфраструктурі мережевий IPS передбачений окремий "центр прийняття рішень", то вторгнення буде успішно виявлено, і мережа залишиться в безпеці. Якщо обміну інформацією або централізований збір не відбувається, а кожний пристрій мережний IPS діє автономно, вторгнення пройде непоміченим. Таким чином, питання "чи передбачений в структурі мережевої IPS механізм централізованого прийняття рішень при роботі декількох IPS" є важливим.

Рівень 2 – існуюча інфраструктура

Якщо припустити, що мережна IPS має механізм централізованого прийняття рішень, то, безсумнівно, інформація від хостової IPS також не буде зайвою при ухваленні рішення про вторгнення. Можливість збору інформації не тільки від мережевих модулів IPS, але й від хостових модулів IPS, дозволяє визначати взаємозв'язки між трафіком, реєструємими мережевими модулями, і станом хостів, реєструємими хостовими модулями. При об'єднанні даних від мережевих і хостових модулів IPS у центрі прийняття рішень з'являється повне подання про стан у мережі й про причинно-наслідкові зв'язки між подіями в різних точках мережі, що сприяє зниженню кількості помилкових спрацьовувань.

Рівень 3 – розвиток інфраструктури

Паралельно з розвитком механізмів IPS інформаційна інфраструктура компаній також еволюціонує. Все більший розвиток мобільних інструментів мережевої взаємодії не може залишатися

непоміченим виробниками IPS. Питання підтримки мобільних пристроїв, контролю їхньої безпеки здобувають все більшу актуальність із кожним роком, якщо не місяцем. У найближчому майбутньому питання "яка підтримка мобільних пристроїв у тому або іншому IPS-рішенні?" може стати ключовим.

Ключові тенденції розвитку систем виявлення вторгнень

Можна виділити наступні найбільш актуальні тенденції розвитку систем виявлення вторгнень:

– ***На рівні виявлення вторгнень.***

Це, по-перше, розширення спектра підтримуваних прикладних протоколів, особливо з урахуванням розвитку індустрії IP-телефонії, технології VoIP і росту популярності сервісу Video-On-demand, практично скрізь використання систем миттєвого обміну повідомленнями й т.п.

По-друге, додавання підтримки мобільних пристроїв і механізмів аналізу взаємодії з мобільними пристроями.

По-третє, більш глибоке пророблення алгоритмів функціонування вже підтримуваних прикладних протоколів, включаючи механізми контролю стану сеансу; як наслідок; підвищення гнучкості визначення факту вторгнення.

І, по-четверте, використання систем запобігання вторгнень для запобігання витоку конфіденційної інформації з організації по різних каналах.

– ***На функціональному рівні.***

Це, по-перше, додавання функцій профілювання трафіку й введення механізмів якості обслуговування на рівні систем запобігання вторгнень.

По-друге, розширення можливостей централізованого керування системами запобігання вторгнень.

По-третє, розвиток засобів перетворення елементарних подій безпеки в "макро"-події, зручні для оператора.

– ***На рівні інфраструктури IPS.*** Тут можливі два моменти.

По-перше, розширення інтеграції хостових і мережевих систем запобігання вторгнень для поліпшення точності виявлення вторгнень.

І, по-друге, розширення можливостей для інтеграції продуктів різних виробників, уніфікація форматів передачі даних і керуючих впливів.

Системи запобігання вторгнень твердо зайняли своє місце на ринку засобів захисту інформації. Їхня необхідність практично не викликає сумнівів, їхня популярність і поширення росте. Разом з тим, індустрія систем запобігання вторгнень приречена на постійний розвиток слідом за розвитком мережевих технологій, технологій передачі інформації й підходів зловмисників до порушення безпеки.

У міру зростання систем запобігання вторгнень будуть збільшуватися їхні можливості по аналізу взаємодії конкретних прикладних протоколів. Разом з тим, буде підвищуватися гнучкість опису поняття "вторгнення", що забезпечить більші можливості по налаштовуванню рішення під конкретне середовище.

Нарешті, структура системи запобігання вторгнень буде прагнути до розподіленої системи з модулями різних типів (і, можливо, що є розробками різних виробників) і єдиним центром прийняття рішень, що одержують інформацію про події й передає керуючу інформацію з використанням стандартизованих протоколів обміну інформацією.

РОЗДІЛ 10. РЕАЛІЗАЦІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ

Комплексні системи мережевої безпеки в організації забезпечують безперервне й надійне функціонування інформаційно-обчислювальної системи.

Створення або модернізація комплексної системи мережевої безпеки в організації необхідна, якщо виконуються наступні дії:

– виробляється реконструкція або модернізація IT-інфраструктури або зміна IT-ландшафту (наприклад, перехід на віртуальні платформи, хмари й т.п.);

– впроваджуються нові критичні бізнес-додатки;

– використовується малоефективна система захисту, що не вирішує основні завдання бізнесу;

– виникають нові законодавчі або галузеві вимоги.

Типова комплексна система мережевої безпеки в організації містить у собі наступні інструменти захисту:

– виявлення й запобігання атак;

– забезпечення безпеки бездротових з'єднань;

– забезпечення криптографічного захисту;

– забезпечення захисту від шкідливого ПЗ;

– автоматичні відновлення;

– забезпечення фізичної безпеки й безпеки web-застосунків;

– керування доступом, журналами аудита;

– моніторинг, аналіз захищеності й подій безпеки;

– контроль цілісності й резервне копіювання;

– організацію віддаленого підключення.

Для того щоб коректно впровадити систему захисту, необхідно здійснити її розробку й знати всі особливості ведення бізнесу. З цією

метою проводиться проектування системи мережевої безпеки в організації, що містить у собі три послідовних етапи:

1. Розробка вимог – це комплекс технічних і організаційних мір, що дозволяють привести інформаційну систему у відповідність вимогам стандарту.

2. Вибір необхідних засобів мережевої безпеки в організації, що забезпечують виконання вимог стандарту.

3. Розробка проектної документації – вся необхідна інформація із впроваджуваного встаткування, технічних засобів і методиці проведення випробувань.

У результаті розробки системи мережевої безпеки в організації формується повний набір проектної документації, необхідний для проведення якісного впровадження засобів мережевої безпеки в організації.

Тепер розглянемо всі наведені механізми й підходи до мережевої безпеки в організації більш докладно.

Концепція "авторитетних рекомендацій" являє собою набір вказівок, які забезпечують належний рівень безпеки. Авторитетні рекомендації (далі – рекомендації) – це комбінація вказівок, ефективність яких доведена при застосуванні у всіляких організаціях. Не всі вказівки придатні для використання в конкретній організації. У деяких компаніях необхідні додаткові політики й процедури, навчання персоналу або контроль за технічною безпекою для досягнення прийнятного рівня керування безпекою.

Адміністративна безпека

Рекомендації з адміністративної безпеки – це ті рішення, які відповідають політикам і процедурам, ресурсам, ступеню відповідальності, потребам у навчанні персоналу й планам по виходу із критичних ситуацій. Ці міри покликані визначити важливість інформації й інформаційних систем для компанії й пояснити персоналу, у чому саме полягає ця

важливість. Рекомендації із забезпечення адміністративної безпеки визначають ресурси, необхідні для здійснення належного керування ризиками й визначення осіб, що несуть відповідальність за керування безпекою організації.

Політики й процедури

Політики безпеки визначають метод, відповідно до якого забезпечується безпека всередині організації. Після визначення політики передбачається, що більшість співробітників компанії будуть її дотримуватися. Варто розуміти, що повного й беззастережного виконання політики не буде. У деяких випадках політика буде порушуватися через вимоги, пов'язані з діловою діяльністю організації. В інших випадках ігнорування політики обумовлено складністю її виконання.

Навіть беручи до уваги той факт, що політика буде виконуватися не постійно, вона формує ключовий компонент програми по забезпеченню безпеки й повинна бути включена в перелік рекомендацій із захисту. При відсутності політики співробітники не будуть знати, що робити для захисту інформації й комп'ютерних систем.

Як рекомендації по безпеці необхідно розглядати наступні політики.

– Інформаційна політика. Визначає ступінь таємності інформації всередині організації й необхідні вимоги до зберігання, передачі, позначенню й керуванню цією інформацією.

– Політика безпеки. Визначає технічні засоби керування й налаштування безпеки, що застосовуються користувачами й адміністраторами на всіх комп'ютерних системах.

– Політика використання. Визначає припустимий рівень використання комп'ютерних систем організації й штрафних санкцій, передбачених за їх нецільове використання. Дана політика також визначає прийнятий в організації метод установки програмного забезпечення й відома як політика прийнятного використання.

– Політика резервного копіювання. Визначає періодичність резервного копіювання даних і вимоги до переміщення резервних даних в окреме сховище. Крім того, політики резервного копіювання визначають час, протягом якого дані повинні бути зарезервовані перед повторним використанням.

Політики самі по собі не формують вичерпних інструкцій з виконання програми безпеки організації. Варто визначити процедури, згідно яких співробітники будуть виконувати певні завдання, і які будуть визначати подальші кроки по обробці різних ситуацій з погляду безпеки.

Усередині організації повинні бути визначені наступні процедури:

– Процедура керування користувачами. Визначає, хто може здійснювати авторизований доступ до тих або інших комп'ютерів організації, і яку інформацію адміністратори повинні надавати користувачам, що запитують підтримку. Процедури керування користувачами також визначають, хто відповідає за інформування адміністраторів про те, що співробітникові більше не потрібен обліковий запис. Анулювання облікових записів важливо з того погляду, щоб доступ до систем і мереж організації мали тільки особи з відповідними діловими потребами.

– Процедури системного адміністрування. Описують, яким чином у цей момент часу застосовується політика безпеки на різних системах, наявних в організації. Ця процедура докладно визначає, як повинна здійснюватися робота з відновленнями і їхньою установкою на системи.

– Процедури керування конфігурацією. Визначають кроки по внесенню змін у функціонуючі системи. Зміни можуть містити в собі відновлення програмного й апаратного забезпечення, підключення нових систем і видалення непотрібних систем.

Ресурси

Для застосування коректних рекомендацій з безпеки необхідно здійснити присвоєння ресурсів. На жаль, не існує формули, яку можна

використовувати для визначення того, скільки ресурсів (грошей або співробітників) повинно бути виділене відповідно до програми безпеки, керуючись лише розмірами організації. У цьому рівнянні занадто багато змінних. Необхідні ресурси обумовлюють розміром організації, діловими процесами організації й небезпеками, що загрожують їй.

Кількість ресурсів повинно визначатися на базі коректної й повної оцінки ризиків, відповідно до алгоритму обробки ризиків. У цьому випадку використовується керування проектом. На рисунку 10.1 показано, яким чином відносяться один до одного ресурси, час і область проекту. Якщо програма безпеки сприймається як проект, то організація повинна виділити досить ресурсів для урівноважування трикутника або розширити час або зменшити область.

Рисунок 10.1 – Трикутна діаграма керування проектом

Персонал

Незалежно від того, наскільки велика або мала організація, деяким співробітникам повинно бути доручене виконання завдань, пов'язаних з обробкою уразливостей і забезпеченням інформаційної безпеки. У невеликих організаціях це може бути покладено на співробітника відділу інформаційних технологій. У великих організаціях можуть існувати цілі відділи безпеки. У рекомендаціях не пропонується яке-небудь певне число

співробітників, однак рекомендується, щоб, принаймні, на одного співробітника були покладені обов'язки по забезпеченню безпеки.

Співробітники відділу безпеки повинні мати наступні навички.

– Адміністрування безпеки. Розуміння щоденного процесу адміністрування пристроїв забезпечення безпеки.

– Розробка політик. Досвід у розробці й підтримці політик безпеки, процедур і планів.

– Архітектура. Розуміння мережевої й системної архітектур і застосування нових систем.

– Дослідження. Перевірка нових технологій безпеки на предмет того, наскільки вони можуть протистояти ризику, що представляється для організації.

– Оцінка. Наявність досвіду збору відомостей про потенційні ризики в організаціях або підрозділах. Оцінка може містити в собі навички проникнення й тестування безпеки.

– Аудит. Наявність досвіду ведення аудита систем або процедур.

Всі ці навички корисні для організації, однак дрібні компанії можуть не мати можливості залучити співробітників, що володіють всіма цими навичками. У цьому випадку найбільш раціональним виходом з положення є залучення адміністратора безпеки або розроблювача політик як співробітник, а для виконання інших функцій варто скористатися послугами сторонніх організацій.

Існують люди, у яких є практично всі перераховані навички. Ці фахівці, як правило, мають більший досвід і, отже, вимагають дуже високої зарплати. Якщо в розглянутій організації бюджет обмежений, і зарплата відповідного рівня не може бути забезпечена, не варто сподіватися на те, що вдасться залучити такого фахівця. Замість цього варто зайнятися пошуком осіб, у яких є загальне поняття про всі перераховані моменти й конкретні навички, які необхідні.

Бюджет

Розмір бюджету безпеки організації залежить від області дії й часових рамок проекту безпеки, а не від розмірів організації. Організації з потужними програмами безпеки можуть мати менший бюджет, ніж дрібні організації, які тільки починають створювати свою програму безпеки.

Розподіл засобів відіграє важливу роль у питаннях, пов'язаних з бюджетом безпеки. Бюджет безпеки повинен бути розділений між капітальними витратами, операціями й навчанням персоналу. У багатьох організаціях допускається помилка, яка полягає в тому, що компаніями встановлюються дорогі засоби безпеки без резервування достатньої кількості засобів на навчання персоналу роботі із цими засобами. В інших випадках організації встановлюють ці засоби, припускаючи, що число співробітників може бути скорочено, або керівництво співробітниками може здійснюватися на різних рівнях. У більшості випадків нові засоби безпеки не дозволяють скоротити штат співробітників. Безсумнівно, даному питанню варто приділити додаткову увагу.

У багатьох організаціях співробітники й керівники думають, що підвищений рівень автоматизації засобів безпеки дозволить скоротити число співробітників, задіяних у забезпеченні безпеки. На жаль, це припущення виправдується дуже рідко. Причина в тому, що нові засоби безпеки не автоматизують процес, виконуваний вручну. У більшості випадків виходить так, що процес у цей момент часу не виконується зовсім. Отже, новий засіб безпеки "надає нову можливість", а не підвищує ефективність системи безпеки. Таким чином, покупка нового засобу, як правило, збільшує навантаження на співробітників і вимагає залучення додаткового персоналу.

Розподіл бюджету, відповідно до рекомендацій, повинен ґрунтуватися на планах проекту безпеки (які, у свою чергу, базуються на ризику, що існує для організації). Для успішного виконання планів проекту безпеки повинні бути виділені всі необхідні засоби.

Відповідальність

Деяка посадова особа в організації повинна відповідати за керування ризиками, пов'язаними з безпекою інформації. З недавнього часу ці обов'язки у великих компаніях прийнято покладати на спеціального співробітника виконавчого рівня – головного фахівця з безпеки інформації (Chief Information Security Officer, CISO).

Навчання

Навчання співробітників є однією найбільш важливою складовою процесу керування погрозами, що представляються для безпеки інформації. Якщо співробітники не будуть мати достатній рівень знань і не будуть працювати спільно, будь-які спроби керування ризиками безуспішні. Рекомендується здійснювати три форми навчання.

– Превентивні міри.

– Примусові міри.

– Заохочувальні міри.

Превентивні міри

Навчання превентивним мірам забезпечує співробітників детальними знаннями про захист інформаційних ресурсів організації. Співробітникам варто розповісти, чому потрібно захищати інформаційні ресурси організації; розуміння причин застосування превентивних мір зробить їх більш сумісними з політиками й процедурами. Якщо співробітники не будуть знати, які цілі забезпечення безпеки, то спробують порушити встановлені політики й процедури.

Крім інформування співробітників про важливість забезпечення безпеки, необхідно надати докладні відомості й підходи до забезпечення відповідності політиці організації. Такі міфи, як, наприклад, "надійні паролі важко запам'ятовувати, тому їх варто записувати на папері", варто розглянути й скорегувати.

Строгі превентивні міри можуть приймати різні форми. В інформаційні програми варто включити як рекламні кампанії, так і

навчання співробітників. Рекламні кампанії повинні містити в собі статті новин і плакати. Для нагадування співробітникам про їхні обов'язки використовуйте електронні повідомлення й спливаючі вікна. Ключовими темами рекламних кампаній повинні бути наступні:

– Розповсюджені помилки співробітників, наприклад, запис на папері або розголошення паролів.

– Розповсюджені випадки недотримання безпеки, наприклад, надання занадто великого обсягу інформації клієнтові.

– Важлива інформація, пов'язана з питаннями безпеки, наприклад, з ким необхідно зв'язуватися у випадку підозри на погрозу безпеки.

– Поточні питання інформаційної безпеки, такі як антивірусний захист і безпека віддаленого доступу.

– Теми, що допомагають співробітникам у роботі, наприклад, захист переносних комп'ютерів у поїздці або захист дітей від зловмисників в Інтернеті.

Заняття по навчанню безпеки повинні бути націлені на різні групи співробітників організації. Всі нові співробітники повинні проходити короткий інструктаж (тривалістю до години). Інших співробітників варто навчати приблизно кожні два роки. У процесі цього навчання надається наступна інформація:

– Чому в організації необхідно забезпечувати безпеку.

– Відповідальність співробітника щодо питань безпеки.

– Детальні відомості про політиків інформаційної безпеки організації.

– Детальні відомості про політиків використання, установлених в організації.

– Пропоновані методи вибору надійних паролів.

– Пропоновані методи запобігання атак соціального інжинірингу, включаючи питання, задані й не задані співробітниками довідкової служби.

Адміністратори повинні одержати базові інструкції з питань безпеки й пройти додаткове навчання відповідно до їх конкретної відповідальності. Тривалість додаткових уроків не повинна перевищувати півгодини, і на цих заняттях необхідно розглянути наступні питання:

– Самі останні методи роботи хакерів.

– Поточні погрози безпеки.

– Поточні уразливості й відновлення безпеки.

Розроблювачі повинні одержати базові інструкції з питань безпеки. Для них варто проводити додаткові заняття залежно від питань, за які вони відповідальні, зокрема, за забезпечення безпеки процесу розробки. Під час цих занять необхідно сконцентруватися на методології розробки й процедурах керування конфігурацією.

Для менеджерів компанії варто періодично влаштовувати презентації про поточний стан справ з наданням актуальних і детальних оцінок погроз і планів по зниженню ризику. У презентації включається обговорення системи виміру й методів визначення ефективності програми безпеки за допомогою цієї системи.

Не слід вважати, що співробітникам відділу безпеки не потрібно проходити інструктаж із забезпечення безпеки. Можна припустити, що як сумлінні співробітники вони й так прекрасно знають про свої обов'язки, однак їм варто періодично надавати інструкції із самих останніх засобів безпеки й методам роботи хакерів.

Примусові міри

Більшість співробітників будуть виконувати превентивні міри й додержуватися політики організації. Проте, деякі співробітники можуть ухилятися від цього (ненавмисно або навіть навмисно), що може нанести організації шкоду. В організаціях варто вживати заходів для захисту від таких співробітників.

Важлива складова процесу "рятування" від таких співробітників є забезпечення поінформованості співробітників про основи політики

організації. Забезпечити цю поінформованість можна за допомогою угод про безпеку. По завершенні проходження співробітником навчання безпеки йому потрібно надати копії відповідних політик і запропонувати підписати угоду про те, що він ознайомився й погодився з політиками організації. Ці підписані документи віддаються на зберігання у відділ кадрів і можуть використовуватися у випадку судового процесу.

Заохочувальні міри

Внаслідок природи питань, пов'язаних з безпекою, співробітники можуть не обтяжувати себе інформуванням відділів безпеки про наявність порушень безпеки. Однак, так як співробітники відділу безпеки не можуть одночасно перебувати в декількох місцях і встежити абсолютно за всім, співробітники є важливою частиною системи оповіщення про небезпеки.

Одним з методів, що використовується тут для збільшення рівня звітності співробітників про аспекти безпеки, є програма заохочень співробітників організації. Заохочення не повинні бути великими. Насправді, краще, якщо заохочення будуть видаватися у вигляді невеликих грошових сум. Співробітників також варто переконати в тому, що такі звіти дуже потрібні організації, і що співробітники не будуть каратися за помилкові оповіщення.

Заохочуватися можуть співробітники, що вносять пропозиції про підвищення рівня безпеки й рішення інших проблем, пов'язаних з безпекою. Успішні заохочувальні програми реалізуються за допомогою запитів у співробітників відповідей на питання через службу новин організації. У такій програмі організація може публікувати отримані рекомендації із вказівкою співробітників, які внесли відповідні пропозиції.

Плани виходу із критичних ситуацій

Навіть у найбільш сприятливих обставинах ніколи не вийде повністю усунути небезпеки, що представляються для інформаційних ресурсів організації. Щоб забезпечити швидке відновлення й зниження

збитку, нанесеного організації в результаті інциденту, необхідно сформулювати плани виходу із критичних ситуацій.

Обробка інцидентів

У кожній організації повинна бути присутньою процедура обробки інцидентів. Вона визначає кроки, які необхідно вживати у випадку взламу захисту або проникнення в систему зловмисника. Без цієї процедури ви можете витратити багато часу на усунення його наслідків. Цей час є для потенційних клієнтів компанії антирекламою й означає втрату засобів і витік інформації.

У процедурі обробки інциденту варто детально визначити, хто відповідає за обробку інцидентів в організації. Без надання чітких інструкцій із цього приводу може бути витрачений зайвий час на пошук винного в події й відповідального за переклад систем в автономний режим і звернення до органів правопорядку.

У рекомендаціях вказується, що періодично потрібно тестувати процедури обробки інцидентів. Споконвічні тести можуть анонсуватися заздалегідь і полягати в спільному діалозі співробітників у форумі й висловленні ними своєї думки із приводу того, яким чином можна обробити той або інший інцидент. Додаткове тестування в "реальному" світі повинно проводитися таким чином, щоб несподівані події симулювали реальні вторгнення зловмисників.

Резервне копіювання й архівація даних

Процедури резервного копіювання повинні виходити з політики резервного копіювання. Процедури визначають час виконання резервного копіювання й указують кроки, які варто виконувати при резервуванні даних і їхньому безпечному збереженні. У процедурах архівації даних вказується періодичність повторного використання резервних носіїв і місця, де повинні розташовуватися носії.

Коли резервний носій потрібно витягти з місця окремого зберігання, необхідно керуватися інструкціями, включеними в процедуру й

що вказують, яким чином здійснюється запит і ідентифікація носіїв, метод відновлення даних і спосіб повернення носія в місце зберігання.

Якщо в організаціях такі процедури відсутні, то існує небезпека неправильної інтерпретації співробітниками політики резервного копіювання. У цьому випадку можливі ситуації, коли резервні носії не будуть вчасно від'єднуватися від сайту або відновлення даних буде відбуватися некоректно.

Відновлення після збоїв

У кожній організації повинні бути присутніми плани відновлення після збоїв для визначення вимог і цілей, що досягаються при виникненні яких-небудь неполадок. Плани детально описують, які обчислювальні ресурси є найбільш критичними для організації, і за допомогою цих планів формуються конкретні вимоги по поверненню цих ресурсів у працездатний стан.

В організаціях необхідно мати плани, що передбачають вихід з різних несприятливих ситуацій, починаючи від втрати одного комп'ютера й закінчуючи виходом з ладу всієї мережі. Крім того, у сценарії відновлення варто включити ключові компоненти інфраструктури, такі як канали зв'язку й устаткування.

Плани відновлення після збоїв можуть не передбачати наявність резервних "гарячих сайтів" з повними копіями всього наявного встаткування. Проте, ці плани повинні бути добре продуманими, а вартість застосування плану – зважена щодо потенційного збитку, що може бути нанесений організації.

Будь-який план відновлення після збоїв необхідно періодично тестувати. Принаймні, один раз у рік повинно проводитися повне тестування. При виконанні цього тесту можливе переміщення співробітників в альтернативні приміщення, якщо це передбачається в плані.

Плани проектів безпеки

Так як забезпечення безпеки є безперервним процесом, безпека інформації варто розглядати як постійно виконуваний проект. Розділимо загальний проект на трохи дрібних, які повинні бути завершені. Відповідно до рекомендацій, відділ безпеки організації повинен затверджувати наступні плани:

– плани вдосконалення;

– плани проведення оцінок;

– плани оцінки уразливостей;

– плани аудита;

– плани навчання;

– плани оцінки політики.

Вдосконалення

Плани вдосконалення випливають із процедур оцінки. Якщо в результаті оцінки визначені деякі небезпечні області, варто створити плани по вдосконаленню для дозволу можливих проблем і внесення відповідних змін у середовище. Плани вдосконалення можуть містити в собі планування установки політики, застосування засобів або внесення змін у систему, або створення навчальних програм. Кожна оцінка, проведена в рамках організації, повинна бути відправною точкою плану вдосконалення.

Оцінка

Відділ безпеки організації повинен розробляти щорічні плани оцінки ризику для організації. У середніх організаціях це може бути план повної оцінки, проведеної один раз у рік. У великих організаціях план може передбачати оцінки по підрозділах, а повні оцінки можуть проводитися рідше одного разу в рік.

Великим організаціям рекомендується відхилятися від концепції щорічних оцінок. На практиці оцінки займають багато часу при їхній організації, виконанні й аналізі. У великих компаніях може бути витрачено

кілька місяців на планування, кілька місяців на виконання й кілька місяців – на аналіз, у результаті чого залишиться зовсім небагато часу на безпосереднє застосування змін, перед тим як наступить час наступної оцінки. У подібних випадках ефективніше виконувати менш масштабні оцінки з більшою частотою, а повні оцінки здійснювати періодично, відповідно до наявних умов.

Оцінка уразливостей

Відділи безпеки організацій повинні регулярно проводити оцінку уразливостей (сканування) систем організації. Відділ безпеки повинен планувати щомісячну оцінку всіх систем усередині організації. Якщо в організації дуже багато комп'ютерів, то їх потрібно згрупувати й вроздріб сканувати щотижня. Необхідна наявність планів до виконання, за допомогою яких адміністратори зможуть внести відповідні корективи в системи.

Аудит

Відділ безпеки повинен розробити плани проведення аудита на відповідність політиці організації. Такі аудити можуть бути розроблені для конфігурації систем, відповідності політиці резервного копіювання або для захисту інформації у фізичній формі. Так як аудити вимагають більших зусиль із боку персоналу, кожний аудит націлений на невелику частину організації. При проведенні аудитів системних конфігурацій із всіх систем можна вибрати зразок. При виявленні значних розбіжностей і невідповідностей у відповідному підрозділі проводиться більш масштабний аудит.

Внутрішній відділ аудита організації повинен мати свої власні розклади й плани аудитів. Аудити, проведені відділом безпеки, не заміняють аудити, здійснювані внутрішнім відділом аудита. Ці аудити спрямовані на визначення того, наскільки добре розуміються й виконуються політики й процедури безпеки, з подальшим усуненням невідповідностей і недоліків.

Навчання

Плани навчання повинні створюватися разом з відділом кадрів. Ці плани містять у собі розклад навчальних занять і плани проведення рекламних кампаній. У розкладі необхідно враховувати, що кожний співробітник повинен проходити навчання один раз у два роки.

Оцінка політики

Кожна політика організації повинна передбачати дати перегляду політики. Відділ безпеки повинен розробляти плани для початку перегляду й оцінки політики в міру наближення дати перегляду. Як правило, щороку потрібен перегляд двох політик.

Технічна безпека

Заходи щодо забезпечення технічної безпеки пов'язані із застосуванням елементів керування безпекою на комп'ютерах і в комп'ютерних мережах. Ці елементи керування є відбиттям політик і процедур організації.

Мережеві з'єднання

Результатом переміщення інформації між організаціями з'явилися комунікаційні можливості між мережами різних організацій. З'єднання з Інтернетом сьогодні доступно практично в будь-якій організації, і більша частина компаній використовує Інтернет у певних ділових цілях. Щоб захистити організацію від небажаних вторгнень, необхідно дотримувати наступних рекомендацій.

Постійні з'єднання

Мережеві з'єднання з іншими організаціями або з Інтернетом повинні захищатися міжмережевим екраном. Міжмережевий екран відіграє роль вогнетривкої стіни між двома кімнатами, що розділяє простір на дві різних ділянки, і при виникненні пожежі в одній з кімнат вогонь не перекинеться на іншу. Аналогічним чином міжмережеві екрани відокремлюють мережі організацій від Інтернету або мереж інших організацій для запобігання поширення збитку. Міжмережеві екрани є

фільтруючими маршрутизаторами, фільтрами пакетів або міжмережевими екранами прикладного рівня, залежно від вимог організації.

Бездротові мережі варто також відокремлювати від внутрішньої мережі організації (для цього рекомендується використовувати міжмережевий екран), так як бездротове з'єднання, по суті, являє собою постійне з'єднання з деякими невідомими об'єктами (це може бути будь-який користувач, що перебуває поблизу й має карту бездротового мережного інтерфейсу).

З'єднання віддаленого доступу

З'єднання віддаленого доступу можуть використовуватися для одержання несанкціонованого доступу до організацій і, отже, ці з'єднання необхідно захищати. Такі з'єднання можуть установлюватися за допомогою телефонного підключення, що комутирується, або через Інтернет. Оскільки вони забезпечують доступ у внутрішню мережу організації як звичайне постійне з'єднання, необхідно використовувати деяку форму двофакторної автентифікації. Мова йде про наступні механізми автентифікації.

– Модеми зворотного виклику. Використовуються разом з механізмом автентифікації і є достатнім засобом автентифікації для телефонних з'єднань. Модеми зворотного виклику налаштовуються на певний номер, що вони набирають перед установкою телефонного з'єднання. Користувач, що намагається підключитися, не може змінити цей номер. Модеми зворотного виклику не підходять для мобільних користувачів .

– Динамічні паролі. Використовуються як механізм автентифікації і є такими, якщо комбінуються з якими-небудь даними, відомими користувачеві.

– Пристрої шифрування. Портативні пристрої шифрування використовуються як механізми автентифікації при їхньому комбінуванні з якими-небудь даними, відомими користувачеві. Пристрій шифрування

повинен бути попередньо оснащено відповідними ключами шифрування й відповідати тому, що має користувач.

Кожний із цих механізмів підходить для автентифікації користувачів через з'єднання віддаленого доступу.

Деякі типи механізмів автентифікації не підходять для віртуальних приватних мереж (VPN). Наприклад, якби для автентифікації використовувався біометричний сканер відбитків пальців, потенційна небезпека обману системи була б набагато вище, так як комп'ютер перебуває за межами фізичного місцеположення, яке захищається.

Захист від шкідливого коду

Шкідливий код (комп'ютерні віруси, троянські програми й хробаки) є однієї з найбільш серйозних погроз для інформації. Число й ступінь складності цих програм продовжує з кожним днем збільшуватися, і також зростає ступінь схильності сучасних застосунків нецільовому використанню цими програмами. Шкідливий код проникає в організації чотирма основними способами:

– Файли із загальним доступом з домашніх і робочих комп'ютерів.

– Файли, що завантажуються із сайтів Інтернету.

– Файли, що надходять в організацію у вигляді вкладень електронної пошти.

– Файли, впроваджувані в системи за допомогою використання уразливостей.

Для контролю цієї небезпеки в організації потрібно розробити ефективну антивірусну програму. Гарна антивірусна програма здійснює контроль за шкідливим кодом у трьох точках.

– Сервери. Антивірусне ПЗ встановлюється на всіх файлових серверах і налаштовується на періодичне виконання повної перевірки наявності вірусів у всіх файлах.

– Робочі станції. Антивірусне ПЗ встановлюється на всіх робочих станціях і налаштовується на періодичне виконання повної перевірки

наявності вірусів у всіх файлах. Крім того, антивірусне ПЗ налаштовується на перевірку кожного файлу, що відкривається.

– Системи електронної пошти. Антивірусне ПЗ встановлюється або на головний поштовий сервер, або на шляху проходження електронної пошти всередині організації. Налаштовується на перевірку кожного файлового вкладення перед безпосередньою доставкою користувачеві.

Системні уразливості усуваються за допомогою регулярного сканування уразливостей і установкою відповідних відновлень.

Установка й налаштування антивірусного програмного забезпечення лише наполовину вирішує проблему шкідливого коду. Для повноти антивірусної програми необхідно забезпечити часті відновлення ознак шкідливого ПЗ й доставку цих відновлень на сервери, робочі станції й системи електронної пошти. Відновлення необхідно одержувати відповідно до рекомендацій виробника програмного забезпечення. Ця дія повинна виконуватися не рідше одного разу на місяць.

Багато виробників антивірусного ПЗ надають автоматизовані механізми завантаження самих останніх ознак вірусів і поширення їх по організації. Це дозволяє здійснювати щоденне завантаження ознак шкідливого ПЗ.

Автентифікація

Автентифікація авторизованих користувачів запобігає одержанню неавторизованими користувачами доступу до корпоративних інформаційних систем. Використання механізмів автентифікації запобігає доступ авторизованих користувачів до тієї інформації, перегляд якої їм заборонений. У цей час головним механізмом автентифікації при внутрішньому системному доступі є паролі. При використанні паролів варто керуватися рекомендаціями, що нижче приводяться:

– Довжина пароля. Мінімальна довжина пароля повинна становити не менш 8 символів.

– Частота зміни пароля. Вік паролів не повинен перевищувати 60 днів. Крім того, паролі не повинні змінюватися протягом дня після планової зміни пароля.

– Історія пароля. Не повинні використовуватися останні десять колишніх паролів.

– Вміст паролів. Паролі не повинні складатися тільки з букв; вони повинні представляти комбінацію букв, цифр і спеціальних символів пунктуації. При зміні паролів система повинна в примусовому порядку накладати ці обмеження.

Паролі завжди зберігаються в зашифрованому виді й недоступні звичайним користувачам. Для систем або інформації особливої таємності паролі можуть не забезпечувати належного захисту. У цих випадках варто використовувати динамічні паролі або двофакторну автентифікацію. Майте на увазі, що автентифікація являє собою комбінацію наступних компонентів:

– Те, що відомо користувачеві, наприклад пароль.

– Те, що є в користувача, наприклад карта доступу.

– Те, що представляє особистість користувача, наприклад відбиток пальця.

Двофакторна автентифікація використовується для зниження уразливості кожного типу автентифікаційних даних. Наприклад, паролі записуються на папері й, отже, можуть бути розкриті. Карти доступу можна украсти, а біометричні засоби автентифікації дорогі й вимагають контрольованого або довіреного доступу між користувачем і комп'ютером.

Всі системи організації варто настроїти на запуск екранної заставки для видалення інформації з екрана й вимога повторної автентифікації, якщо користувача немає за комп'ютером більше 10 хвилин. Якщо співробітник залишить комп'ютер без догляду, не виходячи з мережі, то при відсутності повторної автентифікації зловмисник зможе використовувати цей комп'ютер під виглядом працівника організації.

Відстеження

Відстеження (моніторинг) мереж на предмет наявності підозрілої активності став необхідною й обов'язковою дією. Ця дія включає як аудит, так і моніторинг мережі й системи в реальному часі. Як правило, воно розділяється на аудит й виявлення вторгнень.

Аудит

Аудит – це механізм, що записує дії, що відбуваються на комп'ютері. Журнал містить інформацію про події, що відбулися (вхід у систему, вихід із системи, доступ до файлів і т.д.), про те, хто виконав ту або іншу дію, коли виконана дія, чи була ця дія успішним. Журнал аудита – це матеріал для дослідницьких дій, виконуваних після якої-небудь події. Журнал містить інформацію про те, яким чином здійснене проникнення в комп'ютерну систему, яка інформація зчитана або змінена. Повинно вестися запис наступних подій:

– Вхід/вихід користувачів.

– Невдалі спроби входу.

– Спроби мережевого підключення.

– Спроби віддаленого підключення по телефонній лінії.

– Вхід супервізора/адміністратора/засновника.

– Функції, привілею на виконання яких є в супервізора/адміністратора/засновника.

– Доступ до секретних файлів.

В ідеальному випадку ці події записуються у файл, розташований на захищеній системі – зловмисник не зможе видалити сліди своїх дій.

Журнали аудита корисні в тому випадку, якщо вони регулярно проглядаються. На жаль, журнали аудита – це одні з найбільш складних файлів для перегляду. Людині дуже важко шукати у величезному файлі журналу кілька записів, які можуть означати деяку подію. Отже, в організаціях варто використовувати автоматизовані засоби перегляду журналів аудита. Ці засоби являють собою сценарії, що переглядають

файли журналів на предмет пошуку певних рядків тексту. Рекомендується здійснювати щотижневий перегляд журналів аудита.

Процес відтворення часто утрудняється тим, що часові мітки в різних журналах не відповідають один одному. Щоб спростити процес перегляду журналу, рекомендується синхронізувати годинники на всіх системах за допомогою централізованої системи синхронізації часу, такий як NTP.

Виявлення вторгнень

Системи виявлення вторгнень (IDS) використовуються для моніторингу мереж або систем і оповіщення в реальному часі про подію, що представляє інтерес для осіб, що забезпечують безпеку. Використання вузлової системи виявлення вторгнень допомагає при перевірці журналів аудита, так як дає можливість перегляду файлів журналів. Мережева IDS використовується для моніторингу мережі на предмет атак або трафіку, що відрізняється від нормального потоку даних, звичайно спостережуваного в мережі. Системи IDS обох типів забезпечують безпеку за допомогою видачі попереджень і оповіщень при наявності незвичайної активності в системі, тим самим знижуючи час, що витрачається на обробку інциденту.

Не слід обмежуватися тільки лише застосуванням IDS. IDS яка розгортається, повинна бути тісно пов'язана з політикою використання комп'ютерів і політикою безпеки, а також із процедурами обробки інцидентів, наявними в організації.

Шифрування

Секретна інформація піддається небезпеці при передачі незахищеним способом, наприклад через електронну пошту або телефонні лінії. Секретна інформація піддається небезпеки при зберіганні на незахищеному переносному комп'ютері. Захист інформації забезпечує шифрування.

Якщо рівень таємності інформації того вимагає, інформація повинна шифруватися при передачі по незахищених каналах зв'язку або

через електронну пошту. Використовуваний алгоритм шифрування повинен забезпечувати рівень захищеності, що відповідає ступеня таємності інформації, яка захищається. На лініях зв'язку між комп'ютерами організації повинне застосовуватися шифрування каналу зв'язку. Якщо між комп'ютерами використовуються VPN-з'єднання, то VPN повинні використовувати дуже потужне шифрування для всієї інформації, переданої між двома розташуваннями.

Якщо електронна пошта використовується для передачі секретної інформації всередині організації, шифрування повідомлень не обов'язково. Однак якщо секретні дані передаються за межі внутрішньої мережі організації, необхідно шифрувати повідомлення. Якщо повідомлення передається в іншу організацію, варто заздалегідь розробити процедури, що забезпечують шифрування повідомлення. Деякі правила (такі як HIPAA) вимагають шифрування секретної інформації при її проходженні через відкриті мережі.

При зберіганні на переносних комп'ютерах секретна інформація повинна перебувати в зашифрованому виді. Використовуваний алгоритм шифрування повинен забезпечувати рівень надійності, що відповідає ступеню таємності інформації, яка захищається. Система на портативному комп'ютері повинна вимагати автентифікацію користувача перед тим, як він зможе здійснити доступ до інформації. В ідеальному випадку система повинна забороняти доступ до інформації, якщо користувач комп'ютера недоступний.

При шифруванні будь-яких даних варто використовувати добре відомі й перевірені алгоритми шифрування.

Відновлення систем

Постачальники програмного забезпечення випускають відновлення для усунення уразливостей і помилок у своїх програмах. Ці відновлення дуже важливі з погляду безпеки, так як без них системи будуть перебувати

в стані, уразливому для атаки й проникнення. Проте, відновлення не слід установлювати без їхнього тестування.

У кожній організації повинна бути тестова лабораторія, у якій буде проводитися перевірка нових відновлень різними додатками перед установкою на функціонуючі системи. Адміністратори повинні регулярно перевіряти наявність нових відновлень. Всі відновлення повинні встановлюватися відповідно до процедур контролю за змінами, установленими в організації.

Резервне копіювання й відновлення

Як говорилося в розділі "Адміністративна безпека", резервне копіювання й відновлення є невід'ємними процедурами для забезпечення відновлення після збою. Ніж більше "свіжими" є резервні копії, тим легше відновити всі поточні операції. Інформація на серверах повинна резервуватися щодня. Один раз у тиждень необхідно здійснювати повне резервне копіювання. Резервування даних протягом наступних шести днів повинне доповнювати повне резервування.

Всі резервні копії повинні періодично перевірятися для визначення того, чи успішно створені резервні копії важливих файлів. Повинні бути встановлені регулярні розклади тестування, щоб здійснювалося періодичне тестування всіх носіїв.

Резервне копіювання робочих станцій і портативних комп'ютерів може викликати проблеми в будь-якій організації. Однією з них є великий обсяг даних. Друга проблема полягає в потребі виконання резервного копіювання між різними мережами. Як правило, резервне копіювання робочої станції й портативних комп'ютерів виробляється тільки в тому випадку, якщо інформація є занадто секретною, щоб перебувати на файловому сервері. У цьому випадку резервна система повинна перебувати в одному місці розташування з розглянутим комп'ютером.

Якщо інформація занадто секретна для розміщення на файлових серверах, резервні носії вимагають особливого захисту.

Не менш важливо забезпечити правильне зберігання резервних копій після їхнього створення. Резервне копіювання здійснюється таким чином, щоб організація змогла відновити інформацію у випадку збоїв. Під збоями маються на увазі такі події, як випадкове видалення важливого файлу користувачем або вихід з ладу всього сайту. Для відновлення з першої й другої ситуації пред'являються конфліктуючі вимоги до зберігання резервних копій. Для відновлення важливих користувальницьких файлів резервні копії повинні перебувати під рукою, щоб відновлення можна було зробити швидко. Для захисту від збоїв і інших непередбачених обставин резервні копії повинні зберігатися у відключеному від мережі стані.

Відповідно до рекомендацій, резервні копії потрібно відключати від мережі для максимізації рівня захисту інформації. Резервні копії варто систематизувати, щоб їх можна було швидко знайти й використовувати для відновлення певних файлів. Резервні копії необхідно відключити від мережі протягом 24 годин після створення.

Фізична безпека

Для забезпечення повного захисту необхідно виконувати вимоги фізичної безпеки, поряд із забезпеченням технічної й адміністративної безпеки. Всі заходи щодо забезпечення технічної безпеки не зможуть захистити секретну інформацію, якщо не контролювати фізичний доступ до серверів. Крім того, на доступність інформаційних систем можуть вплинути такі фактори, як електроенергія й кліматичні умови. Відповідно до рекомендацій, фізична безпека забезпечує захист інформаційних систем у наступних областях.

– Фізичний доступ.

– Кліматичні умови.

– Захист від пожежі.

– Електроенергія.

Фізичний доступ

Всі секретні комп'ютерні системи повинні бути захищені від несанкціонованого доступу. Як правило, це реалізується за допомогою змісту систем у єдиному інформаційному центрі. Доступ до інформаційного центра контролюється різними способами. Доступ за допомогою магнітної карти або кодового замка покликаний обмежити число співробітників, які можуть входити в інформаційний центр. Стіни інформаційного центра повинні бути капітальними, щоб виключити доступ через простір над фальш-стелею.

Кліматичні умови

Комп'ютерні системи чутливі до високих температур. Крім того, комп'ютери самі по собі генерують велику кількість тепла. Модулі контролю за кліматом в інформаційному центрі повинні забезпечувати постійну температуру й вологість, а також мати потужність, що відповідає розмірам приміщення й кількості теплоти, виділюваній комп'ютерними системами. Ці модулі налаштовуються на повідомлення адміністраторів про збої або про вихід температури за межі припустимого інтервалу. Якщо навколо кондиціонерів в інформаційному центрі конденсується волога, то із приміщення центру необхідно забрати всі ємності з водою.

Захист від пожежі

В інформаційних центрах не можна використовувати водяні системи пожежогасіння, так як в цьому випадку комп'ютерні системи вийдуть із ладу. Варто використовувати системи пожежогасіння, активна речовина яких засновано не на воді. Система пожежогасіння повинна бути розміщена й налаштована таким чином, щоб вогонь у прилягаючому просторі не зміг ізолювати яку-небудь систему інформаційного центра.

Якщо застосування не водяної системи пожежогасіння вимагає занадто великих витрат, можна використовувати "суху" систему, що відключає електроенергію в інформаційному центрі перед наступною

подачею води. Порадьтеся з пожежним інспектором, щоб з'ясувати, чи можна використовувати цей варіант.

У багатьох інструкціях з боротьби з вогнем говориться про те, що у всіх приміщеннях будинку повинні бути встановлені розпилювальні системи пожежогасіння, незалежно від наявності інших систем. У цьому випадку неводяні системи придушення вогню повинні бути налаштовані на роботу перед розпилювальними системами.

Електроенергія

Для функціонування комп'ютерних систем необхідна електроенергія. Часто відбуваються перепади напруги й короткочасне відключення електроенергії. Такі переривання в електропостачанні можуть вивести комп'ютери з ладу й, отже, привести до втрати даних. Всі важливі комп'ютерні системи повинні бути захищені від короткочасних відключень електроенергії.

Найкраще із цим завданням справляються резервні джерела живлення. Ці джерела повинні забезпечувати електроживлення протягом часу, достатнього для виконання коректного відключення комп'ютерів. Щоб захистити системи від більш тривалих відключень електрики, варто використовувати резервні генератори. У кожному разі повинні бути налаштовані оповіщення, що повідомляють адміністраторам про відключення електроенергії.

Якщо резервний електрогенератор недоступний, варто придбати акумуляторні системи, що дозволяють здійснити коректне відключення систем у випадку тривалої відсутності електроживлення. Це запобіжить виходу комп'ютерів з ладу при раптовому відключенні через "акумулятори, що сіли".

Використання стандарту ISO 17799

Існує багато різних інструкцій, у яких приводяться різного роду рекомендації з тої або іншої тематики (у цьому випадку їхня кількість занадто велика для відбиття в матеріалі цієї книги). Подібні документи

опубліковані багатьма асоціаціями й урядовими агентствами. В 2000 р. Міжнародна організація по стандартизації (ISO) видала міжнародний стандарт для методів безпеки інформації. Документ називається "Інформаційні технології – методи забезпечення інформаційної безпеки" – ISO/IEC 17799 (доступний на сайті американського Національного інституту стандартів http://www.ansi.org/; його вартість – 112 доларів). Документ прямо базується на BS (British Standards Institution) 77910.

Даний документ призначений для використання як стартова точка. Незважаючи на те, що це дуже якісний і корисний документ, кожна організація унікальна й, як правило, вимагає додаткових заходів контролю або ж, навпаки, застосування меншої їхньої кількості, ніж зазначено в стандарті.

Ключові концепції стандарту

ISO 17799 охоплює десять основних областей:

– ***Політика безпеки.*** У даному розділі розповідається про необхідність політики безпеки й регулярного перегляду й оцінки цього документа.

– ***Організаційна безпека***. У даному розділі описується, як варто забезпечувати безпеку інформації. Утримується інформація про роботу зі сторонніми організаціями й керуванні безпекою при цих взаєминах.

– ***Класифікація й контроль майна.*** У даному розділі обговорюється необхідність правильного захисту як фізичних, так і інформаційних ресурсів.

– ***Безпека персоналу.*** У даному розділі обговорюється необхідність контролю ризиків, пов'язаних з найманням на роботу співробітників, а також обговорюється навчання співробітників організації. Крім того, тут уперше зачіпається тема обробки інцидентів.

– ***Фізична безпека й безпека середовища.*** Все фізичне майно повинне бути надійно захищене від розкрадання, пожежі й інших впливів. Даний розділ присвячений саме цій темі.

– ***Керування комунікаціями й операціями***. Розглядається необхідність у документуємих процедурах керування комп'ютерами й мережами, а також обговорюється питання безпеки інформації при її передачі. Тут також згадується необхідність захисту комп'ютерів від шкідливих програм.

– ***Контроль доступу.*** У даному розділі обговорюється контроль доступу до інформації, системам, мережам і додаткам, а також говориться про керування користувачами й про необхідність моніторингу.

– ***Розробка й підтримка систем.*** У даному розділі розглядаються питання безпеки, пов'язані з розробкою проектів. Крім того, тут обговорюються необхідність у шифруванні й керуванні ключами, а також контроль конфігурації системних файлів.

– ***Підтримка безперервності ділових процесів***. Тут розповідається про небезпеку переривання ділових процесів і про різні альтернативні способи підтримки їхньої безперервності.

– ***Відповідність політиці.*** У даному розділі говориться про те, яким чином в організації слід дотримуватися встановленої політики і як повинна проводитися перевірка на відповідність установленій політиці.

Для кожного розділу чітко визначені цілі тих або інших контролюючих дій. Крім того, у введенні приводиться корисна інформація про те, як досягти захищеного стану інформації всередині організації.

Яким чином використовувати цей стандарт

Стандарт ISO 17799 використовується як стартова точка для розробки програм безпеки. При побудові програми безпеки необхідно ознайомитися із цим документом і використовувати його як керівництво при роботі в тій або іншій області. Якщо вже є розроблена програма безпеки, то за допомогою стандарту ISO 17799 можна перевірити, чи не упущені які-небудь важливі питання.

У введенні в документ говориться про те, що деякі міри контролю можуть не знадобитися, і що можуть знадобитися деякі додаткові заходи,

не включені в матеріал стандарту. Точний набір засобів, мір і дій по керуванню, що включається в кожну програму безпеки, визначається в процесі оцінки погроз.

Не використовуйте стандарт ISO 17799 або який-небудь інший рекомендаційний документ як вимоги, відповідність яким повинно бути повним і безумовним. Завжди проводьте оцінку погроз і визначайте дійсні вимоги безпеки для вашої конкретної організації.

Проведення аналізу уразливостей

Цей проект покаже, наскільки розглянута організація відповідає авторитетним рекомендаціям. Майте на увазі, що це трохи інше завдання, ніж оцінка погроз. Ви не будете намагатися виявити погрози, а будете шукати речі, про які раніше могли й не знати.

Послідовність дій

1. Почніть пробляти рекомендації, що приводяться в даному розділі або в стандарті ISO 17799, якщо у вас є цей документ.

2. При роботі з кожним розділом визначте, чи відповідає ваша організація (або остання проведена оцінка погроз) приведеним рекомендаціям.

3. Якщо розглянута організація не відповідає якій-небудь рекомендації, спробуйте зрозуміти причину. Можливо, є інші міри й засоби контролю, або ступінь погрози для організації дуже мала, внаслідок чого неефективно застосовувати засіб, який рекомендується, або метод контролю. Крім того, яка-небудь рекомендація могла попросту раніше ніде не приводитися.

4. Для тих рекомендацій, явна причина застосування яких в організації відсутня, розробіть рекомендацію, що забезпечує відповідний рівень контролів.

Отже, як уже згадувалося вище, цей проект не є повторним проведенням оцінки погроз, а являє собою найменш дорогий спосіб розглянути під іншим ракурсом наявну програму безпеки. Навіть самі

досвідчені співробітники відділу безпеки можуть занадто "зациклюватися" на наявній програмі, і з кожним днем боротися із проблемами, що виникають за підтримкою цієї програми. Зовнішній спостерігач, як правило, може внести "свіжий струмінь" у вигляді рекомендацій, які дозволять удосконалити програму безпеки лише тому, що не будуть скovані щоденним функціонуванням цієї програми. Точно в такий же спосіб може використовуватися й документ із авторитетними рекомендаціями.

РОЗДІЛ 11. БЕЗПЕКА БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ

Безпека електронних платіжних систем

Сучасну практику банківських операцій, торговельних угод і взаємних платежів неможливо представити без розрахунків із застосуванням пластикових карт.

Система безготівкових розрахунків за допомогою пластикових карт називається електронною платіжною системою.

Для забезпечення нормальної роботи електронна платіжна система повинна бути надійно захищена.

З точки зору інформаційної безпеки в системах електронних платежів існують наступні уразливі місця:

– пересилання платіжних і інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом;

– обробка інформації всередині організацій відправника й одержувача повідомлень;

– доступ клієнтів до засобів, акумульованих на рахунках.

Пересилання платіжних і інших повідомлень пов'язана з такими особливостями:

– внутрішні системи організацій відправника й одержувача повинні забезпечувати необхідний захист при обробці електронних документів (захист кінцевих систем);

– взаємодія відправника й одержувача електронного документа здійснюється опосередковано – через канал зв'язку.

Ці особливості породжують наступні проблеми:

– взаємне впізнання абонентів (проблема встановлення взаємної дійсності при встановленні з'єднання);

– захист електронних документів, переданих по каналах зв'язку (проблема забезпечення конфіденційності й цілісності документів);

– захист процесу обміну електронними документами (проблема доказу відправлення й доставки документа);

– забезпечення виконання документа (проблема взаємної недовіри між відправником і одержувачем через їхню приналежність до різних організацій і взаємної незалежності).

Для забезпечення функцій захисту інформації на окремих вузлах системи електронних платежів повинні бути реалізовані наступні механізми захисту:

– керування доступом на кінцевих системах;

– контроль цілісності повідомлення;

– забезпечення конфіденційності повідомлення;

– взаємна автентифікація абонентів;

– неможливість відмови від авторства повідомлення;

– гарантії доставки повідомлення;

– неможливість відмови від вживання заходів по повідомлення;

– реєстрація послідовності повідомлень;

– контроль цілісності послідовності повідомлень.

Отже, як платіжний засіб в електронній платіжній системі використовуються електронні пластикові карти.

Електронна пластикова карта – це носій інформації, що ідентифікує власника й зберігає певні облікові дані.

Розрізняють кредитні й дебетові карти.

Кредитні карти є найпоширенішим видом пластикових карт. До них відносяться карти загальнонаціональних систем США Visa і MasterCard, American Express і ряду інших. Ці карти пред'являють для оплати товарів і послуг. При оплаті за допомогою кредитної карти банк покупця відкриває йому кредит на суму покупки, а потім через якийсь час (звичайно 25 днів) надсилає рахунок поштою. Покупець повинен

повернути оплачений чек (рахунок) назад у банк. Природно, подібну схему банк може запропонувати тільки найбільш заможним і перевіреним зі своїх клієнтів, які мають гарну кредитну історію перед банком або солідні вкладення в банк у вигляді депозитів, цінностей або нерухомості.

Власник ***дебетової*** карти повинен заздалегідь внести на свій рахунок у банку певну суму. Розмір цієї суми визначає ліміт доступних засобів. При здійсненні розрахунків з використанням цієї карти відповідно зменшується й ліміт. Для поновлення або збільшення ліміту власник повинен знову внести гроші на свій рахунок. Для страхування часового розриву між моментом здійснення платежу й моментом одержання банком відповідної інформації на рахунку клієнта повинен підтримуватися незнижуваний залишок.

Як кредитна, так і дебетова карти можуть бути не тільки персональними, але й ***корпоративними.*** Корпоративні карти надаються компанією своїм співробітникам для оплати відрядних або інших службових витрат. Корпоративні карти компанії пов'язані з яким-небудь одним її рахунком. Ці карти можуть мати розділений або нерозділений ліміт. У першому випадку кожному із тримачів корпоративних карт установлюється індивідуальний ліміт. Другий варіант більше пасує невеликим компаніям і не припускає розмежування ліміту.

Пластикова карта являє собою пластину, виготовлену зі спеціальної пластмаси, стійкої до механічних і термічних впливів. За стандартом *ISO 9001* всі пластикові карти мають розміри 85.6×53.9×0.76 мм.

Для ідентифікації власника на пластикову карту наносяться:

– логотип банку-емітента;

– логотип платіжної системи, що обслуговує цю карту;

– ім'я власника карти;

– номер рахунку власника карти;

– термін дії карти й т.п.

Крім того, на карті може бути присутня фотографія власника і його підпис.

Алфавітно-цифрові дані (ім'я, номер рахунку й ін.) можуть бути ембосовані, тобто нанесені рельєфним шрифтом. Це дає можливість при ручній обробці прийнятих до оплати карт швидко перенести дані на чек за допомогою спеціального пристрою – імпринтера, що здійснює "прокатування" карти.

За принципом дії розрізняють пасивні й активні пластикові карти. Пасивні пластикові карти всього лише зберігають інформацію. До них відносяться пластикові карти з магнітною смугою.

Карти з магнітною смугою є поки найпоширенішими – в обігу перебуває понад два мільярди карт подібного типу. Магнітна смуга розташовується на звороті карти й, у відповідності зі стандартом ISO 7811, складається із трьох доріжок. З них перші дві призначені для зберігання ідентифікаційних даних, а на третю доріжку можна записувати інформацію (наприклад, поточне значення ліміту дебетової карти). Однак через невисоку надійність багаторазово повторюваного процесу запису/зчитування запис на магнітну смугу звичайно не практикується.

Карти з магнітною смугою відносно уразливі для шахрайства. Для підвищення захищеності своїх карт системи Visa і MasterCard/Europay використовують додаткові графічні засоби захисту: голограми й нестандартні шрифти для ембосування. Ембоссери (пристрої для тиснення рельєфу на карті) випускає обмежене коло виготовлювачів. У ряді країн Заходу законодавчо заборонений вільний продаж ембоссерів. Спеціальні символи, що підтверджують приналежність карти до тієї або іншої платіжної системи, поставляються власникові ембоссера тільки з дозволу керівного органа платіжної системи.

Платіжні системи з подібними картами вимагають on-line авторизації в торговельних точках і, як наслідок, наявності розгалужених, високоякісних засобів комунікації (телефонних ліній).

Відмінна риса активної пластикової карти – наявність убудованої в неї електронної мікросхеми. Принцип пластикової карти з електронною мікросхемою запатентував в 1974 р. француз Ролан Морено. Стандарт ***ISO 7816*** визначає основні вимоги до карт на інтегральних мікросхемах або чиповим картам.

Карти з мікросхемою можна класифікувати по двох ознаках.

Перша ознака – принцип взаємодії із пристроєм, що зчитує. Основні типи:

– карти з контактним зчитуванням;

– карти з безконтактним (індукційним) зчитуванням.

Карта з контактним зчитуванням має на своїй поверхні від 8 до 10 контактних пластин. Розміщення контактних пластин, їхня кількість і призначення виводів різні в різних виробників і природно, що зчитувачі для карт даного типу розрізняються між собою.

Обмін даними між картою з безконтактним зчитуванням і пристроєм, що зчитує, виробляється індукційним способом. Очевидно, що такі карти надійніші й більш довго використовуються.

Друга ознака – функціональні можливості карти. Основні типи:

– карти-лічильники;

– карти з пам'яттю;

– карти з мікропроцесором.

Карти-лічильники застосовуються, як правила, у тих випадках, коли та або інша платіжна операція вимагає зменшення залишку на рахунку тримача карти на деяку фіксовану суму. Подібні карти використовуються в спеціалізованих додатках з передоплатою (плата за використання телефону-автомата, оплата автостоянки й т.ін.). Очевидно, що застосування карт із лічильником обмежене й не має великої перспективи.

Карти з пам'яттю є перехідними між картами-лічильниками й картами з мікропроцесором. Карта з пам'яттю – це перезаписувана карта-

лічильник, у якій вжиті заходи, що підвищують її захищеність від атак зловмисників. Найпростіші карти з пам'яттю мають обсяг пам'яті від 32 байт до 16 Кбайт. Ця пам'ять може бути організована у вигляді:

– програмувального постійного запам'ятовувального пристрою ППЗП (EPROM), що допускає однократний запис і багаторазове зчитування;

– стираємого електричного програмувального постійного запам'ятовувального пристрою ЕСППЗП (EEPROM), що допускає багатократний запис і багаторазове зчитування.

Карти з пам'яттю можна підрозділити на два типи:

– з незахищеною (повнодоступною) пам'яттю;

– з захищеною пам'яттю.

У картах першого типу немає ніяких обмежень на читання й запис даних. Ці карти не можна використовувати в якості платіжних, тому що їх досить просто "зламати".

Карти другого типу мають область ідентифікаційних даних і одну або кілька прикладних областей. Ідентифікаційна область допускає лише однократний запис при персоналізації й далі доступна тільки для зчитування. Доступ до прикладних областей регламентується й здійснюється тільки при виконанні певних операцій, зокрема при введенні секретного PIN-коду.

Рівень захисту карт із пам'яттю вище, ніж у магнітних карт. Як платіжний засіб карти з пам'яттю використовуються для оплати таксофонів загального користування, проїзду в транспорті, у локальних платіжних системах (клубні карти). Карти з пам'яттю застосовуються також у системах допуску в приміщення й доступу до ресурсів комп'ютерних мереж (ідентифікаційні карти).

Карти з мікропроцесором називають також інтелектуальними картами або смарт-картами. Це по суті мікрокомп'ютери, які містять всі основні апаратні компоненти:

– мікропроцесор з тактовою частотою 5Мгц;

– оперативний ЗП ємністю до 256 байт;

– постійниий ЗП ємністю до 10 Кбайт;

– енергонезалежний ЗП ємністю до 8 Кбайт.

Смарт-карта забезпечує широкий набір функцій:

– розмежування повноважень доступу до внутрішніх ресурсів;

– шифрування даних із застосуванням різних алгоритмів;

– формування електронного цифрового підпису;

– ведення ключової системи;

– виконання всіх операцій взаємодії власника карти, банку й продавця.

Деякі смарт-карти забезпечують режим "самоблокування" при спробі несанкціонованого доступу.

Все це робить смарт-карту високозахищеним платіжним інструментом, що може бути використаний у фінансових додатках, що пред'являють підвищені вимоги до захисту інформації. Саме тому смарт-карти є найбільш перспективним видом пластикових карт.

Важливими етапами підготовки й застосування пластикової карти є ***персоналізація й авторизація***.

Персоналізація здійснюється при видачі карти клієнтові. При цьому на карту заносяться дані, що дозволяють ідентифікувати карту і її власника, а також здійснити перевірку платоспроможності карти при прийманні її до оплати або видачі готівки. Первісним способом персоналізації було ембосування.

До персоналізації відносяться також кодування магнітної смуги й програмування мікросхеми.

Кодування магнітної смуги виробляється, як правило, на тому же устаткуванні, що й ембосування. При цьому частина інформації про карту, що містить номер карти й період її дії, однакова як на магнітній смузі, так і на рельєфі. Однак бувають ситуації, коли після первинного кодування

потрібно додатково занести інформацію на магнітну смугу. У цьому випадку застосовуються спеціальні пристрої з функцією "читання-запис". Це можливо, зокрема, коли PIN-код для користування картою не формується спеціальною програмою, а вибирається клієнтом за своїм розсудом.

Програмування мікросхеми не вимагає особливих технологічних прийомів, але зате має деякі організаційні особливості. Так операції по програмуванню окремих областей мікросхеми рознесені територіально й розмежовані по правах різних співробітників. Звичайно ця процедура розбивається на три етапи:

– на першому робочому місці виконується активація карти (уведення її в дію);

– на другому робочому місці виконуються операції, пов'язані із забезпеченням безпеки;

– на третім робочому місці виробляється властиво персоналізація.

Такі міри підвищують безпека й виключають можливі зловживання.

Авторизація – це процес підтвердження продажу або видачі готівки по карті. Для проведення авторизації точка обслуговування робить запит платіжній системі про підтвердження повноважень пред'явника карти і його фінансових можливостей. Технологія авторизації залежить від типу карти, схеми платіжної системи й технічної оснащеності точки обслуговування.

Авторизація проводиться або "вручну", або автоматично. У першому випадку здійснюється голосова авторизація, коли продавець або касир передає запит операторові по телефону. У другому випадку карта міститься в автоматизований торговельний POS-термінал (Point-Of-Sale – оплата в точці продажу), дані зчитуються з карти, касир вводить суму платежу, а власник карти – PIN-код (Personal Identication Number – персональний ідентифікаційний номер). Після цього термінал здійснює авторизацію, встановлюючи зв'язок з базою даних платіжної системи (on-

line режим), або реалізуючи додатковий обмін даними із самою картою (off-line режим). При видачі готівки процес має аналогічний характер, з тією лише особливістю, що гроші в автоматичному режимі видаються банкоматом, що і проводить авторизацію.

Випробуваним способом ідентифікації власника пластикової карти є використання секретного персонального ідентифікаційного номера PIN. Значення PIN повинно бути відомо тільки власникові карти. З одного боку, PIN повинен бути досить довгим, щоб імовірність угадування за допомогою повного перебору була прийнятно малою. З іншого боку, PIN повинен бути досить коротким, щоб власник міг його запам'ятати. Звичайно довжина PIN коливається від 4 до 8 десяткових цифр, але може досягати 12.

Значення PIN однозначно пов'язане з відповідними атрибутами пластикової карти, тому PIN можна трактувати як підпис власника карти.

Захист персонального ідентифікаційного номера PIN для пластикової карти є критичним для безпеки всієї платіжної системи. Пластикові карти можуть бути загублені, украдені або підроблені. У таких випадках єдиним контрзаходом проти несанкціонованого доступу залишається секретне значення PIN. Тому відкрита форма PIN повинна бути відома тільки законному власникові карти. Вона ніколи не зберігається й не передається в рамках системи електронних платежів.

Метод генерації значення PIN впливає на безпеку електронної платіжної системи. Взагалі, персональні ідентифікаційні номери можуть формуватися або банком, або власниками карт.

Якщо PIN призначається банком, то звичайно використовується один із двох варіантів.

При першому варіанті PIN генерується криптографічно з номера рахунку власника картки. Шифрування проводиться за алгоритмом DES з використанням секретного ключа. Перевага: значення PIN не потрібно зберігати усередині електронної платіжної системи. Недолік: при

необхідності зміни PIN треба міняти або номер рахунку клієнта, або криптографічний ключ. Але банки воліють, щоб номер рахунку клієнта залишався фіксованим. А з іншого боку, оскільки всі PIN обчислюють, використовуючи один ключ, зміну одного PIN при збереженні рахунку клієнта спричиняє зміна всіх персональних ідентифікаційних номерів.

При другому варіанті банк вибирає PIN випадковим чином, зберігаючи це значення у вигляді криптограми. Обрані значення PIN передаються власникам карт по захищеному каналу.

Використання PIN, призначеного банком, незручно клієнтам навіть при невеликій його довжині. Такий PIN важко запам’ятати, і тому власник карти може записати його куди-небудь. Головне – це не записувати PIN безпосередньо на карту або інше видне місце. Інакше завдання зловмисників буде сильно полегшена.

Для більшої зручності клієнта використовують значення PIN, що обрав сам клієнт. Такий спосіб визначення PIN дозволяє клієнтові:

– використовувати той самий PIN для різних цілей;

– задавати в PIN не тільки цифри, але й букви (для зручності запам'ятовування).

Обраний клієнтом PIN може бути переданий у банк замовленою поштою або відправлений через захищений термінал банківського офісу, що негайно його шифрує. Якщо банку необхідно використовувати обраний клієнтом PIN, то це робиться у такий спосіб. Кожну цифру обраного клієнтом PIN складають за модулем 10 (без обліку переносів) з відповідною цифрою PIN, виведеного банком з рахунку клієнта. Одержуване десяткове число називається "зсувом". Цей зсув запам'ятовується на карті клієнта. Оскільки виведений PIN має випадковий характер, те обраний клієнтом PIN неможливо визначити по його зсуві.

Головна вимога безпеки полягає в тому, що значення PIN повинне запам'ятовуватися власником карти й ніколи не повинне зберігатися в будь-якій читабельній формі. Але люди недосконалі й дуже часто

забувають свої PIN. Тому для таких випадків призначені спеціальні процедури: відновлення забутого PIN або генерація нового.

При ідентифікації клієнта за значенням PIN і пред'явленій карті використовуються два основних способи перевірки PIN: неалгоритмічний і алгоритмічний.

Неалгоритмічний спосіб здійснюється шляхом безпосереднього порівняння уведеного клієнтом PIN зі значеннями, збереженими в базі даних. Звичайно база даних зі значеннями PIN клієнтів шифрується методом прозорого шифрування, щоб підвищити її захищеність, не ускладнюючи процесу порівняння.

Алгоритмічний спосіб перевірки PIN полягає в тому, що введений клієнтом PIN перетворять за певним алгоритмом з використанням секретного ключа й потім порівнюють зі значенням PIN, що зберігається в певній формі на карті. Переваги цього методу перевірки:

– відсутність копії PIN на головному комп'ютері виключає його розкриття персоналом банку;

– відсутність передачі PIN між банкоматом або POS-терміналом і головним комп'ютером банку виключає його перехоплення або нав'язування результатів порівняння;

Спрощення роботи зі створення програмного забезпечення системи, тому що вже немає необхідності дій у реальному масштабі часу.

Крадіжки грошей з пластикових карт із використанням банкоматів

Принцип тут такий: скиммер зчитує інформацію з магнітної стрічки Вашої картки, дозволяючи легко виготовити її дублікат. А накладка на клавіатуру дозволяє довідатися PIN, що Ви вводите. У результаті через 2 хвилини після Вашого спілкування з банкоматом, зловмисники мають можливість зняти всі гроші, що залишилися на вашій картці (у межах обмежень на видавані суми банкоматом, але як їх обходити знають усе).

Якщо ви побачите скиммер, відразу дзвоніть в підтримку банку по телефону, зазначеному на картці. Не відходячи від банкомату, тому що зловмисники сидять в одній з недалеко припаркованих автомашин. Такий пристрій ставиться на банкомат на одну ніч або навіть на кілька годин. Зловмисники заздалегідь вивчають відвідуваність банкомату в нічний час, наявність охорони, камер та інші фактори, що визначають співвідношення ризик/заробіток у конкретному випадку.

Дуже часто банкомат вибирається з наступних принципів:

– у спальному районі (великий розмір аудиторії);

– поруч із відділенням банку (нахабність звичайно, але виправдана – банкомат здається надійним);

– на вулиці (варіант установки скиммера на банкомат у приміщенні менш імовірний);

– поруч із місцем де всю ніч витрачаються гроші (McDonalds, торгові центри);

– вуличних камер немає (я не помітив);

– стихійна автостоянка навколо (на ще одну припарковану машину ніхто не зверне уваги).

РОЗДІЛ 12. ЕЛЕКТРОННА КОМЕРЦІЯ: ВИМОГИ ДО БЕЗПЕКИ

Електронна комерція (e-commerce) зустрічається в Інтернеті всюди. Компанії по усьому світі використовують сайти в Інтернеті для пропозиції клієнтам своєї продукції. Деякі із цих спроб виявилися успішними, інші – провалилися. Успішні організації поєднує той факт, що вони усвідомлюють, що займаються електронною комерцією для того, щоб робити гроші. Гроші можна робити, пропонуючи нові послуги через Інтернет, розширюючи наявні послуги, або за допомогою надання наявної послуги за більше низьку ціну.

Організації, що займаються електронною комерцією, піддають себе небезпеці. Вони вкладають кошти в нові технології й у нові методи надання товарів і послуг у надії підвищити ступінь вигоди бізнесу. Ризики, що представляються для організації, мають кілька причин: сторонні люди можуть проігнорувати послугу, можуть не з'явитися нові клієнти, а наявним клієнтам нова послуга може бути не по душі. Так як мова йде про організації, що займаються електронною комерцією, необхідно взяти до уваги повністю новий набір погроз і уразливостей. Ці нові погрози й уразливості спричиняються ризики, які необхідно контролювати.

Говорячи про електронну комерцію, необхідно мати на увазі, що електронні системи обробки замовлень і платежів існують уже тривалий час. Протягом багатьох років між компаніями використовується система Electronic Data Interchange (EDI) для замовлення товарів і здійснення платежів. Великою перевагою, що змушує багато говорити про електронну комерцію, є те, що сьогодні звичайні покупці можуть замовити практично будь-який товар з будь-якого місця, а будь-яка організація може дуже швидко відкрити електронний магазин. Крім того, багато організацій, що займалися раніше продажем товарів через поширювальні мережі, тепер

можуть продавати свою продукцію безпосередньо покупцям і в такий спосіб знижувати вартість ведення бізнесу.

Служби електронної комерції

Які послуги надає електронна комерція? Цей список дуже великий, і деякі служби є зовсім новими й інноваційними. Наприклад, деякі організації продають передплати на джерела інформації. Даний тип послуги став доступний досить давно, але він вимагав чималих засобів, так як при його застосуванні, як правило, потрібна окрема телефонна лінія для замовлень. Зараз будь-яка людина може скористатися цими послугами через Інтернет. Постачальник послуг також може збільшити свій дохід за допомогою надання інформації передплатникам за меншу вартість.

Ще однією послугою, надання якої стало можливим через Інтернет завдяки електронній комерції, є надання бібліотечних послуг для секретної й конфіденційної інформації. Організації можуть підписуватися на службу, що здійснює зберігання й електронний доступ до приналежній їм інформації. Доставка інформації в організацію здійснюється через Інтернет. Наприклад, організація А містить договір з компанією V для зберігання й роботи з електронною інформацією. Компанія V створює центр даних з великим обсягом сховища й забезпечує доставку файлів організації А. Ці файли потім можуть бути розміщені на системах таким чином, щоб співробітники організації А могли безпечно здійснювати доступ до них. Компанія V стягує плату з організації А залежно від обсягу збережених даних.

Інші послуги, надавані за допомогою електронної комерції, пов'язані з функціями, виконуваними організацією, які за допомогою цих послуг можуть виконуватися з меншими витратами. Гарним прикладом тут є поширення інформації. Виробникам, наприклад, потрібно поширювати інформацію про продукти й прайс-аркуші по інформаційних мережах дистрибьютерів і перепродувачів.

Раніше виробникам потрібно було роздруковувати й відправляти інформацію у вигляді твердих копій по звичайній пошті або налаштовувати складні й дорогі приватні мережі, щоб забезпечити підключення розповсюджувачів до систем виробника й одержання інформації. Із залученням можливостей електронної комерції виробник може створити в Інтернеті єдиний сайт і дозволити розповсюджувачам і перепродувачам підключатися до нього через Інтернет і одержувати необхідну інформацію. Даний підхід дешевший й більше реалізується.

Імовірно, найпоширеніша послуга, надавана за допомогою електронної комерції – це покупка товарів. Навіть для цієї традиційної послуги можна спостерігати деякі нововведення. Певні компанії продають через Інтернет електронні книги й MP3-файли. Це теж різновид звичайної послуги із продажу товарів.

Багато сайтів в Інтернеті надають клієнтам можливість отримувати товари: клієнти роблять замовлення, після чого товар пересилається клієнтові.

Приклади служб електронної комерції

Коли ми говоримо про застосування системи безпеки до служб електронної комерції, можна розглядати це питання щодо чотирьох основних аспектів безпеки:

– конфіденційність;

– цілісність;

– доступність;

– відповідальність.

Також доступність є аспектом, пов'язаним з будь-яким типом електронної комерції. Моменти, пов'язані з іншими аспектами, розрізняються залежно від типу пропонованих послуг електронної комерції. Наступні розділи містять приклади того, яким чином можна забезпечити безпеку служб електронної комерції.

Продаж товарів

Допустимо, організації потрібно продавати свою продукцію через Інтернет. Основною концепцією тут є те, що клієнти будуть відвідувати веб-сайт, знайомитися з переліком товарів і замовляти товари з доставкою. Оплата буде проводитися за допомогою кредитної карти, а доставка товарів буде здійснюватися з використанням найбільш економічного методу.

Для даного сценарію можна вивести наступні вимоги безпеки для кожної базової функції безпеки:

– ***Конфіденційність.*** Більша частина інформації не є конфіденційною. Однак номер кредитної карти – це конфіденційні дані. Адреса електронної пошти клієнта й інша особиста інформація також може бути конфіденційною залежно від політики таємності сайту.

– ***Цілісність.*** Клієнт зажадає забезпечення цілісності даних, щоб він зміг одержати те, що йому потрібно. Для змісту інформації в коректному вигляді буде потрібно забезпечити цілісність протягом всієї процедури, а також гарантувати цілісність каталогу, щоб ціни в каталозі відповідали дійсності.

– ***Відповідальність.*** Організації потрібно буде підтверджувати той факт, що особа, яка використовує кредитну карту, дійсно є її власником.

З наведеного прикладу видно, що безпека грає важливу роль в архітектурі даної системи електронної комерції.

Надання конфіденційної інформації

Розглянемо ще одну службу електронної комерції. У даному прикладі організація надає користувачам інформацію за певну плату. Ця інформація є власністю організації, і керівництво організації хоче контролювати те, яким чином інформація поширюється. Організація фактично продає доступ до даних окремих користувачів або інших організацій на основі підписки.

Ґрунтуючись на даному сценарії, можна скласти список вимог до безпеки базових служб:

– ***Конфіденційність.*** Прайс-аркуші, замовлення й звіти про дефекти являють собою конфіденційні дані. Крім того, на кожного розповсюджувача повинно бути накладене обмеження на те, які прайс-аркуші й замовлення він може переглядати.

– ***Цілісність.*** Прайс-аркуші необхідно захищати від несанкціонованої зміни. Кожне замовлення повинено бути коректне у будь-якому місці системи.

– ***Відповідальність.*** Виробникові буде потрібно довідатися, який розповсюджувач запитує прайс-аркуш або розміщає замовлення; це необхідно для надання коректної інформації.

Доступність

Доступність у даному розділі розглядається як окрема тема, так як це ключове питання, пов'язаний з роботою служб електронної комерції. Якщо сайт недоступний, то бізнес компанії стоїть на місці. Все навіть більш серйозно, так як доступність сайту впливає безпосередньо на довіру клієнта надаваним послугам.

Питання взаємин "компанія-клієнт"

Перевірка доступності починається з питань, пов'язаних з організацією, якій потрібно підтримувати ділові відносини з рядовим населенням або конкретною клієнтурою. Існує кілька питань, пов'язаних з доступністю. Перше питання: коли клієнтові знадобиться користуватися послугою? Відповідь: у будь-який момент, коли це йому буде потрібно. Це не грає ролі, коли в організації припускають наявність певного числа клієнтів, це має значення лише тоді, коли клієнтам потрібно відвідати сайт і виконати ділові операції. Тому сайт повинен працювати в будь-який час.

Також варто мати на увазі, що при цьому повинен бути в активному стані весь сайт цілком, а також система обробки платежів і інші компоненти сайту, які можуть знадобитися клієнтові. Можете уявити, що

відчує клієнт, що знайшов ваш сайт, визначив, який товар йому потрібно придбати, і в підсумку виявив, що його замовлення не може бути оброблено через неприступність платіжної системи. Швидше за все, цей клієнт дістанеться вашим конкурентам.

Хоча це не питання безпеки, у цілому проблема доступності передбачає такі ділові питання, як можливість прийому й обробки замовлень, що вводяться в систему. При побудові сайту необхідно забезпечити достатній обсяг інфраструктури для очікуваного навантаження. Цей момент дуже добре ілюструється на прикладі телевізійної комерційної компанії. Компанія починає з команди людей, які тільки що закінчили роботу над створенням веб-сайту електронної комерції. Вони дивляться на екран і чекають першого замовлення. Перше замовлення не змушує себе довго чекати, і всі з полегшенням зітхають. Потім замовлення починають надходити все частіше й частіше, і незабаром їхня кількість уже досягає декількох сотень тисяч. По реакції персоналу видно, що вони не очікували такого потоку замовлень, і що вони просто не зможуть їх обробити. Кілька великих компаній не змогли забезпечити обробку ряду замовлень і практично припинили через це свою роботу.

Питання взаємин "компанія-компанія"

Електронна комерція, реалізована між компаніями, відрізняється від випадку "компанія-клієнт". Електронна комерція між компаніями, як правило, реалізується між двома організаціями, що встановили певні взаємини. Одна організація звичайно отримує продукцію або користується послугами іншої. Так як між цими організаціями встановлені взаємини, питання безпеки можуть оброблятися поза каналом зв'язку (це означає, що організаціям не прийдеться вирішувати питання безпеки при виконанні транзакції).

З іншого боку, питання доступності стають більш критичними. Організації реалізують даний тип електронної комерції для прискорення

процесу обробки замовлень і для зниження загальних витрат, що мають місце при обробці паперових замовлень і рахунків. Отже, якщо одній організації потрібно зробити замовлення, інша організація повинна мати можливість прийняти його й обробити. Деякі взаємини між компаніями передбачають проведення транзакцій у певний час дня, в інших випадках потрібно проводити транзакції в будь-який час.

Всесвітній час

Доступність систем електронної комерції підкоряється концепції всесвітнього часу. Дана концепція визначає глобальну природу Інтернету й електронної комерції як такий. Традиційні комерційні відносини залежать від людей. Люди відкривають магазини й чекають клієнтів. Магазин відкритий протягом годин, яких клієнти найімовірніше виходять за покупками.

Після введення систем замовлень по електронній пошті почала проглядатися концепція всесвітнього часу. Клієнти можуть замовляти товар по телефону, не виходячи з будинку. Внаслідок цього в організаціях, що приймають замовлення по електронній пошті, співробітникам доводиться протягом тривалого часу відповідати на телефонні дзвінки. Деякі компанії із системою замовлень по електронній пошті підтримують роботу системи замовлень протягом 24 годин на день.

Те ж саме відноситься й до Інтернету. Інтернет є у всіх точках земної кулі. Отже, незалежно від місцевого часу в певному місці земної кулі обов'язково буде середина дня. Деякі організації можуть націлювати свою продукцію на локальних споживачів. Але це не означає, що в продукції компанії буде зацікавлені тільки локальні клієнти. Замовлення можуть надходити із всіляких точок планети. Для розширення ринку продукції організації, комерційний сайт повинен підтримувати обробку замовлень, що виходять із різних місць.

Зручність клієнта

В остаточному підсумку доступність спричиняє зручність клієнта. Наскільки зручною представляється клієнтові організація обробки замовлення й доставки товару? Якщо сайт недоступний, коли клієнтові потрібно зробити замовлення на товар, то клієнт, швидше за все, відчує незручність.

Те ж відноситься й до випадку, коли клієнт хоче перевірити стан замовлення або відстежити доставку придбаного товару. Якщо дана можливість заявлена, але не надана, або клієнт одержав менше користі, ніж очікував, то він перестане довіряти такій організації.

Зручність або незручність клієнта може швидко вирости. Інформація поширюється через Інтернет безліччю способів, включаючи сайти з оглядами компаній і продуктів, списки електронної пошти, у яких користувачі обговорюють всілякі теми, чат-портали й системи новин, що дозволяють проводити дискусії у вигляді форумів. Організації, що якісно надають свої послуги, часто згадуються на таких сайтах і форумах. Користувачі рекомендують один одному користуватися послугами тих або інших компаній. Не менш часто в обговореннях фігурують організації, що надають послуги неякісно або не в повному обсязі, тому якщо одному клієнтові не сподобалося, як його обслужила та або інша компанія, його негативна думка дійде до сотень і тисяч інших користувачів. Таким чином, число потенційних клієнтів організації буде знижуватися.

Збитки внаслідок простою

Після обговорення питань, пов'язаних з доступністю, стає ясно, що ціна, що платять компанії за час, протягом якого послуги не надаються по тим або інших причинах, велика. Збитки мають місце незалежно від причини, по яким сайт електронної комерції не працює. Може відбутися програмний або апаратний збій, хакер здійснить атаку на відмову в обслуговуванні, або недостатньо якісно буде функціонувати устаткування.

Збитки від часу простою можна виміряти, взявши середнє число транзакцій за певний період часу й зіставивши його з доходом від середньостатистичної транзакції. Однак даний спосіб не визначає загальний обсяг збитків компанії, так як є потенційні клієнти, які навіть не відвідали сайт, довідавшись про його неробочий стан від друзів або від знайомих по листуванню. З цієї причини сайт електронної комерції повинен бути побудований в обхід одиничних точок збою. Кожний комерційний сайт повинен передбачати процедури відновлення устаткування й програмного забезпечення, що дозволяють забезпечити його безперервне функціонування в процесі відновлення систем.

Рішення проблеми доступності

Ми обговорили безліч питань, пов'язаних з доступністю, але тепер залишилося розібратися, яким же чином вирішити всі ці проблеми? Скажемо відразу: ніяк. Не можна повністю гарантувати доступність сайту електронної комерції. Знаючи це, можна говорити про міри, що вживаються для керування ризиком неприступності сайту.

Перед тим як застосовувати будь-які з рішень по забезпеченню керування, необхідно вирішити, наскільки коштовна доступність сайту. Рішення по запобіганню збоїв і відновленню можуть дуже швидко стати дорогими, і керівництву організації спочатку варто з'ясувати величину збитків від неприступності сайту.

Одним з методів зниження ризику простою сайту є забезпечення надмірності. Почнемо з комунікаційної системи. Інтернет-архітектура сайту електронної комерції повинна передбачати, принаймні, два з'єднання із провайдером. Для більших сайтів може знадобитися кілька провайдерів або навіть декілька продубльованих каналів зв'язку.

На комп'ютерних системах перебувають веб-сервер електронної комерції, програмні додатки й сервер бази даних. Кожна із цих систем є точкою збою. Якщо важливо забезпечити доступність сайту, кожна із цих систем повинна бути надлишковою. Для сайтів, через які проходить

великий обсяг трафіку, можна використовувати комутатори прикладного рівня для балансування навантаження, встановлені перед веб-серверами для приховання одиничних збоїв від клієнтів.

При використанні систем обходу збоїв не слід забувати про компоненти мережевої інфраструктури, такі як міжмережеві екрани, маршрутизатори й комутатори. Кожен із цих пристроїв являє собою одиничну точку збою мережі, що може з легкістю вивести сайт із ладу. Ці компоненти також варто налаштувати на обхід збоїв при забезпеченні підвищеного ступеня доступності.

Реалізація безпеки клієнтської сторони

Безпека клієнтської сторони має на увазі безпеку комп'ютера клієнта при його з'єднанні із сервером електронної комерції. Ця частина системи містить у собі комп'ютер клієнта й програму-браузер, а також з'єднання із сервером (див. рисунок 12.1).

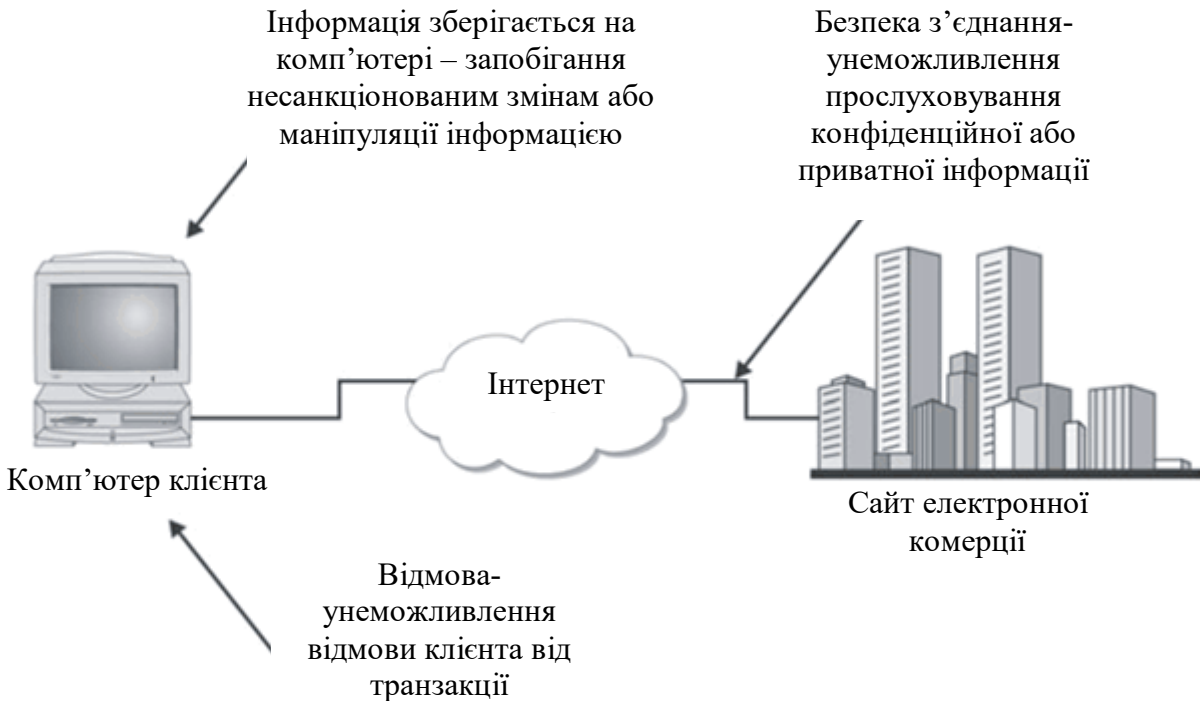

Рисунок 12.1 – Компоненти системи безпеки на стороні клієнта

Із цією частиною системи зв'язані кілька питань:

– Захист інформації при передачі між комп'ютером клієнта й сервером.

– Захист інформації, що зберігається на комп'ютері клієнта.

– Захист того факту, що певний клієнт зробив певне замовлення.

Безпека з'єднань

Безпека з'єднань для застосунків електронної комерції охоплює безпеку інформації, переданої між системою клієнта й сервером електронної комерції. Це можуть бути такі секретні дані, як відомості кредитних карт або паролі на сайті. Ця інформація є такими ж конфіденційними даними, переданими із серверу на комп'ютер клієнта, як і файли клієнта.

Єдиним реальним рішенням даної проблеми є шифрування. Більша частина стандартних веб-браузерів забезпечує можливість шифрування трафіку. Це рішення використовується за замовчуванням у випадку застосування HTTPS замість HTTP. При використанні HTTP між клієнтом і сервером установлюється з'єднання за допомогою протоколу захищених сокетів (SSL). Весь трафік, що проходить через це з'єднання, шифрується.

Шифрування HTTPS захищає інформацію з того моменту, як вона залишає комп'ютер клієнта, і до того моменту, як досягає веб-серверу. Використання HTTPS стало необхідним, оскільки користувачі почали усвідомлювати небезпеку того, що зловмисник може одержати доступ до номера кредитної карти в Інтернеті. Реальність даної ситуації полягає в тому, що сума відшкодування збитку клієнтам у випадку розкрадання номера кредитної карти становить не більше 50 дол.

Зберігання інформації на комп'ютері клієнта

Протоколи HTTP і HTTPS не зберігають стан. Це означає, що після завантаження в браузер веб-сторінки сервер не запам'ятовує, що тільки що в даний браузер була завантажена дана сторінка. Для реалізації комерційної діяльності через Інтернет з використанням веб-браузерів і веб-

серверів сервери повинні фіксувати інформацію про те, що робить клієнт (це інформація про клієнта, дані про те, які товари він замовляє, а також будь-які паролі, які клієнт використовує для доступу до захищених сторінок). Один із способів, за допомогою якого на веб-сервері можна реалізувати дану функціональність (і даний метод є найпоширенішим), є застосування елементів cookies.

Cookie – це невеликий фрагмент інформації, що зберігається на клієнтській системі веб-сервером. До цієї інформації може звертатися тільки той веб-сервер, що розмістив елемент cookie на даному комп'ютері; крім того, термін дії елемента cookie повинен минати по закінченню певного часу (як правило, менше року). Елементи cookie можуть зберігатися у відкритому або зашифрованому виді. Ці елементи можуть бути постійними (не видалятися, після того як клієнт закриває браузер) або тимчасовими (елементи cookie не записуються на диск, але залишаються в пам'яті, поки браузер відкритий).

Cookie можуть використовуватися для запису будь-якої інформації для веб-серверу. На одному сайті вони застосовуються для відстеження замовлення під час вибору клієнтом різних елементів. На іншому сайті cookie використовуються для відстеження автентифікаційних даних клієнта, щоб йому не довелося здійснювати вхід на кожну сторінку.

Ризик використання елементів cookie обумовлює можливістю клієнта (або іншої особи, що має доступ до комп'ютера) переглянути дані, записані в цьому елементі. Якщо cookie містить паролі або інші автентифікаційні дані, це дозволить неавторизованій особі одержати доступ до сайту. Якщо елемент cookie містить інформацію про замовлення клієнта (наприклад, кількість товарів і їхня вартість), клієнт зможе змінити вартість елементів.

При розміщенні замовлення необхідно перевіряти ціни, якщо вони зберігаються в елементі cookie.

Керування ризиком тут здійснюється за допомогою використання шифруємих і тимчасових елементів cookies. Якщо інформація замовлення клієнта або автентифікаційні дані утримуються в тимчасовому елементі cookie, то вони не записуються на системний диск системи клієнта. Зловмисник як і раніше зможе одержати доступ до даної інформації за допомогою розміщення системи-посередника між клієнтом і сервером і в такий спосіб перехопити дані в елементах cookie (і змінити їх). Якщо елементи cookie піддаються шифруванню, даний тип перехоплення даних стає неможливим.

Відмова від виконаної операції

Ще одним ризиком, пов'язаний із клієнтською стороною електронно-комерційних взаємин, є потенційна можливість клієнта відмовитися від транзакції. Очевидно, що якщо клієнт насправді не ініціював транзакцію, організація не дозволить її провести. Однак як організація визначить, чи є клієнт тим, за кого він себе видає? Тут приходить на допомогу автентифікація.

Тип автентифікації, використовуваної для підтвердження особистості клієнта, залежить від ризику допущення помилки. На випадок покупки товару за допомогою кредитної карти є певні процедури виконання транзакції із кредитною картою без надання самої карти. Ці процедури передбачають надання клієнтом правильної поштової адреси для покупки товару.

Якщо сайт електронної комерції надає послугу, що вимагає підтвердження особистості для доступу до певної інформації, кредитна карта може в цьому випадку не підійти. В організації кращим виявляється використання ідентифікатора користувача й пароля або навіть двофакторної автентифікації. У кожному із цих випадків умови надання послуги, що відправляються клієнтові, повинні в деталях описувати вимоги до захисту ідентифікаторів і паролів. Якщо для доступу до інформації клієнта використовується правильний ідентифікатор і пароль,

то мається на увазі, що доступ до інформації здійснюється легітимним користувачем. Якщо пароль загублений, забутий або виявлений зловмисником, необхідно негайно сповістити про це організації.

Реалізація безпеки серверної частини

Коли мова йде про безпеку серверної частини, ми говоримо лише про фізичний сервер електронної комерції й про програмне забезпечення веб-серверу, що на ньому працює. У наступних розділах даної лекції ми розглянемо безпеку застосунку й бази даних. Сам по собі сервер електронної комерції повинен бути доступний з Інтернету. Доступ до системи може бути обмежений (якщо сервер електронної комерції призначений для роботи з невеликим колом користувачів), або система може бути відкрита для всіх користувачів.

З безпекою серверу зв'язані два питання:

– безпека інформації, збереженої на сервері;

– захист самого серверу від вторгнення зловмисників.

Інформація, що зберігається на сервері

Сервер електронної комерції відкритий для доступу з Інтернету, отже, сервер має часткову довіру, але не більше того. Система із частковою довірою або зовсім без довіри не повинна містити секретної інформації. Якщо сервер використовується для прийому платежів по кредитних картах, номера кредитних карт, то ця інформація поповинна негайно переноситися в систему, що безпосередньо обробляє транзакції (яка розташована в більше захищеній частині мережі). Жоден номер кредитної карти не повинен перебувати на сервері.

Якщо інформація повинна зберігатися на сервері електронної комерції, її необхідно захищати від несанкціонованого доступу. Це можна реалізувати за допомогою використання елементів керування доступом до файлів. Крім того, якщо секретні файли не зберігаються в структурі каталогів на веб-сервері або FTP-сервері, то доступ до них через браузер або FTP-клієнт здійснити набагато складніше.

Захист серверу від атак

Сервер електронної комерції, як правило, являє собою веб-сервер. Як уже говорилося раніше, даний сервер доступний з Інтернету й, отже, відкритий для атак. Можна вжити певних заходів, щоб захистити сам сервер від успішного проникнення зловмисника.

– розташування серверу;

– конфігурація операційної системи;

– конфігурація веб-серверу.

Давайте більш детально розглянемо кожний із цих аспектів.

Розташування серверу

Коли мова йде про розташування серверу, необхідно в першу чергу розглядати його фізичне розташування й місце розташування в мережі. З фізичної точки зору, даний сервер представляє більшу важливість для організації. Отже, він повинен розташовуватися усередині захищеної області, наприклад у центрі обробки даних. Якщо керівництво компанії зволіло розташувати сервер у сусіднім приміщенні, необхідно забезпечити захист серверу, відгородивши його від інших клієнтів.

При розташуванні серверу в сусідньому приміщенні рекомендується переглянути наявні в цьому приміщенні процедури безпеки.

Мережне розташування серверу також необхідно взяти до уваги. На рисунку 12.2 показане розташування серверу в демілітаризованій зоні (DMZ). Міжмережний екран варто налаштувати на дозвіл доступу до серверу електронної комерції тільки через порт 80 (для HTTP) і 443 (для HTTPS). Для відкритого доступу до серверу електронної комерції не потрібні додаткові служби й, отже, їх необхідно блокувати на міжмережному екрані.

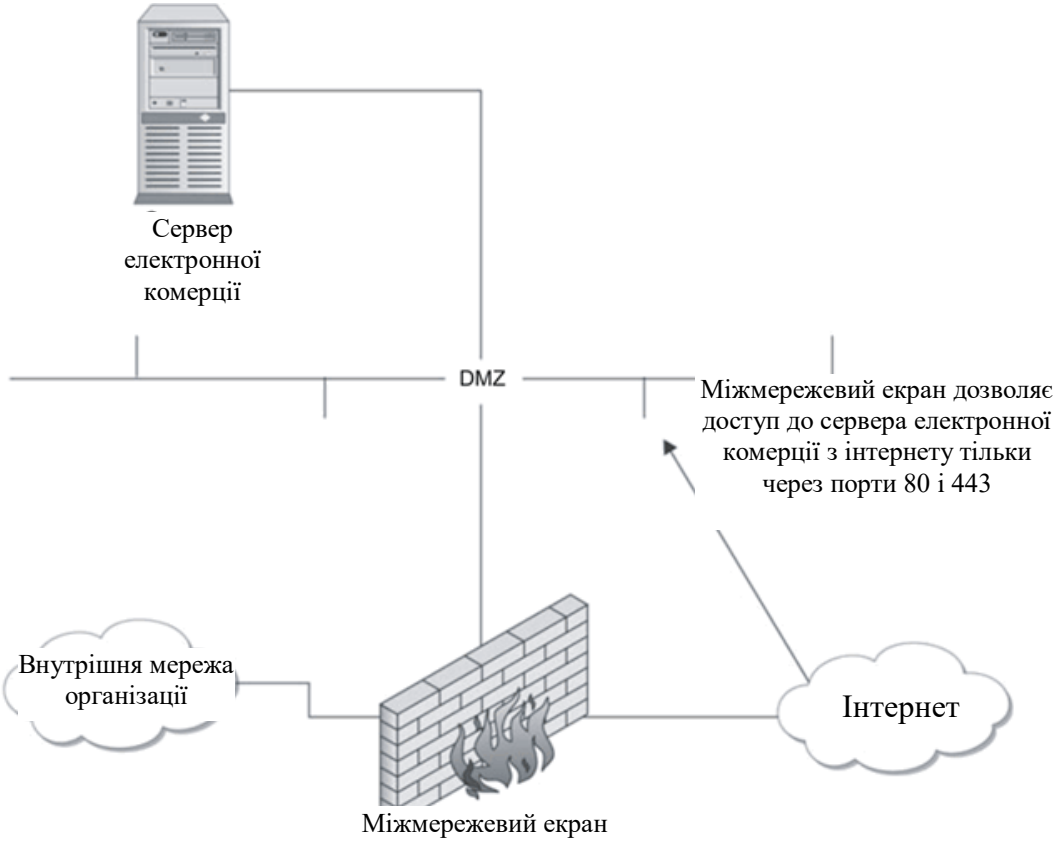

Рисунок 12.2 – Правильне мережеве розташування серверу електронної комерції

Якщо продуктивність серверу електронної комерції є життєво важливим фактором, і очікуваний трафік серверу дуже великий, корисно реалізувати подвійне базування серверу (див. рисунок 12.3).

В цьому випадку один мережевий інтерфейс підтримує вхідний трафік і передає відповідні пакети клієнтові. Даний інтерфейс розташовується в демілітаризованій зоні. Другий мережевий інтерфейс призначений для передачі запитів застосунків або на сервер застосунків (переважно), або прямо в базу даних. Цей інтерфейс розташовується в другій DMZ або в мережі серверу застосунків. Дана мережа відділяється від внутрішньої мережі організації міжмережевим екраном. У жодному разі не слід використовувати один інтерфейс для Інтернету й для внутрішньої мережі.

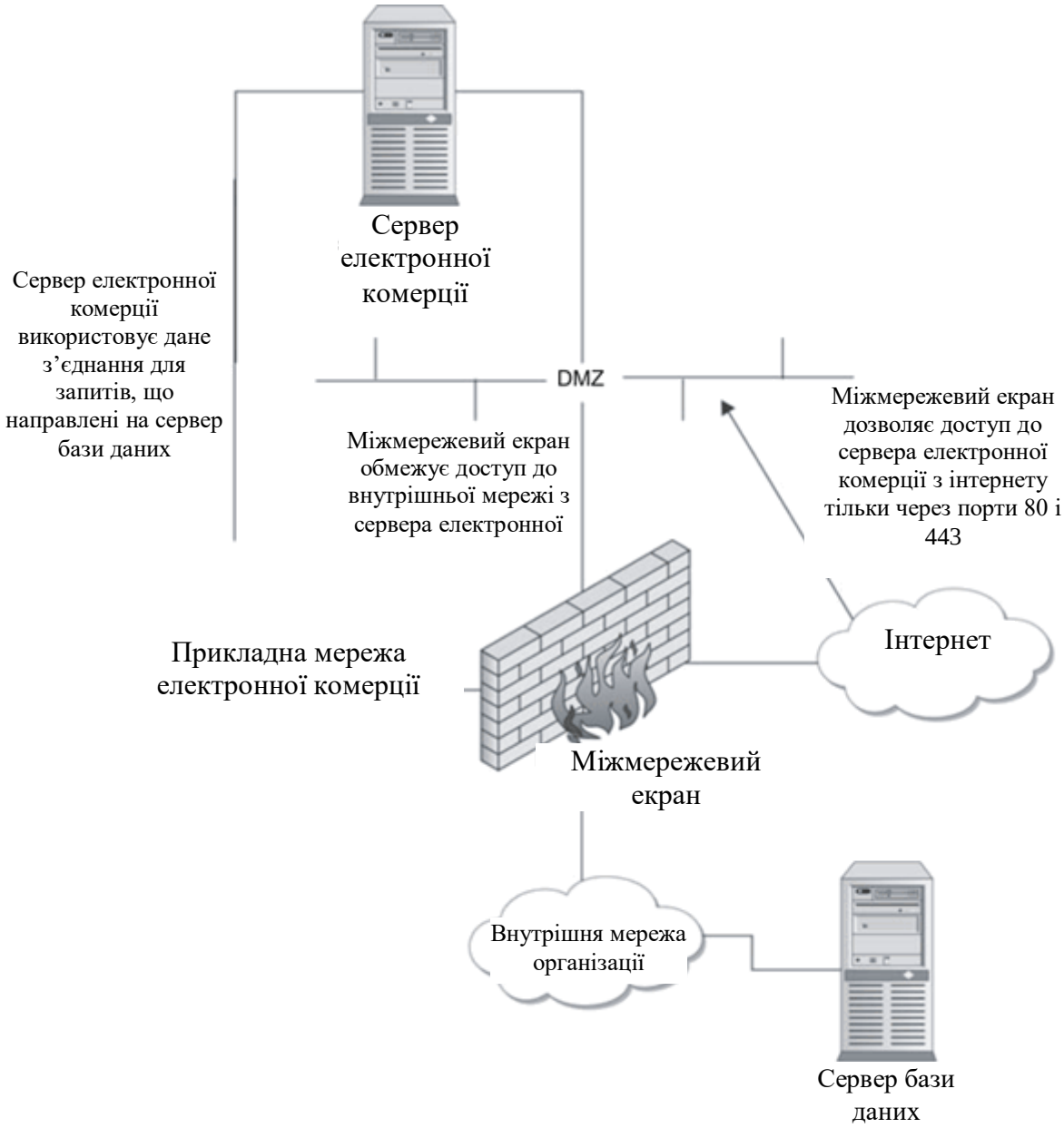

Рисунок 12.3 – Розташування серверу електронної комерції при необхідності використання двох мережевих інтерфейсів

Конфігурація операційної системи

Операційна система серверу електронної комерції повинна бути настроєна з урахуванням питань безпеки. Вибір операційної системи залежить від ряду факторів, включаючи експертизу адміністраторів організації.

При виборі операційної системи необхідно взяти до уваги такі фактори, як вимоги до продуктивності й забезпечення відказостійкості. Крім того, рекомендується вибирати операційну систему, з якої знайомі системні адміністратори.

Першим кроком у безпечному налаштуванні серверу є видалення або відключення всіх служб, що не є життєво важливими. Система являє собою веб-сервер і, отже, на ній повинно працювати програмне забезпечення веб-серверу. Чи потрібно в системі служба DNS? Найімовірніше, ні, тому її варто відключити. Перегляньте служби, що працюють у системі, і визначите, які з них є необхідними для функціонування системи. Відключіть всі служби, які не є обов'язковими.

Наступним кроком є установка відновлень системи. Перевірте наявність останніх відновлень для обраної операційної системи й завантажте їх. Після завантаження відновлень настройте систему на відповідність політиці організації щодо довжини пароля й частоти його заміни, аудита й інших вимог.

При завантаженні відновлень для обраної операційної системи не завантажуйте тільки поточний компонент відновлення. Деякі виробники відокремлюють відновлення безпеки від основного пакета. Якщо відновлення

безпеки не будуть завантажені в окремому порядку, то відновлення системи відбудеться некоректно.

Перед тим як система буде оголошена готовою для роботи, необхідно просканувати її на наявність уразливостей. Сканери уразливостей можуть бути платними або безкоштовними, але вони обов'язково повинні бути самими останніми. Перевірте систему й переконайтеся, що всі необов'язкові служби відключені й завантажені всі необхідні відновлення. Це сканування підтвердить, що система в цей момент не містить уразливостей. Сканування необхідно проводити щомісяця з використанням самих останніх відновлень, щоб забезпечити

відсутність уразливостей у системі. Виявлені уразливості необхідно негайно усувати.

Конфігурація веб-серверу

Веб-сервер сам по собі є останнім компонентом безпеки серверу. На ринку є безліч різних веб-серверів, і вибір серверу залежить від використовуваної платформи й переваг адміністраторів і розроблювачів. Як у випадку з операційними системами, веб-сервери налаштовуються з обліком (або без) аспектів безпеки. Конкретні вимоги до конфігурації веб-серверу виходять за рамки даної книги, однак є деякі загальноприйняті конфігурації, які необхідно реалізовувати, незалежно від використовуваного веб-серверу.

По-перше, програмне забезпечення серверу повинно оновлюватися й доповнюватися відповідно до рекомендацій виробника.

Веб-сервер у жодному разі не повинен функціонувати з використанням кореневого або адміністраторського облікового запису. Якщо зловмисник успішно проникне на веб-сервер, він одержить привілеї, ідентичні встановленим для веб-серверу. Якщо веб-сервер функціонує з використанням кореневого облікового запису, зловмисник одержить привілеї кореневого облікового запису. Щоб уникнути цього створіть окремого користувача – власника веб-серверу й реалізуйте роботу серверу через цей обліковий запис.

Кожний веб-сервер вимагає, щоб адміністратор визначив кореневий каталог серверу. Цей каталог інформує про те, де шукати файли документів і сценарії, а також обмежує набір файлів, до яких здійснюється доступ через браузер. Кореневий каталог веб-серверу в жодному разі не повинен збігатися із системним кореневим каталогом і не повинен містити файли конфігурації й безпеки, необхідні для операційної системи (див. рисунок 12.4).

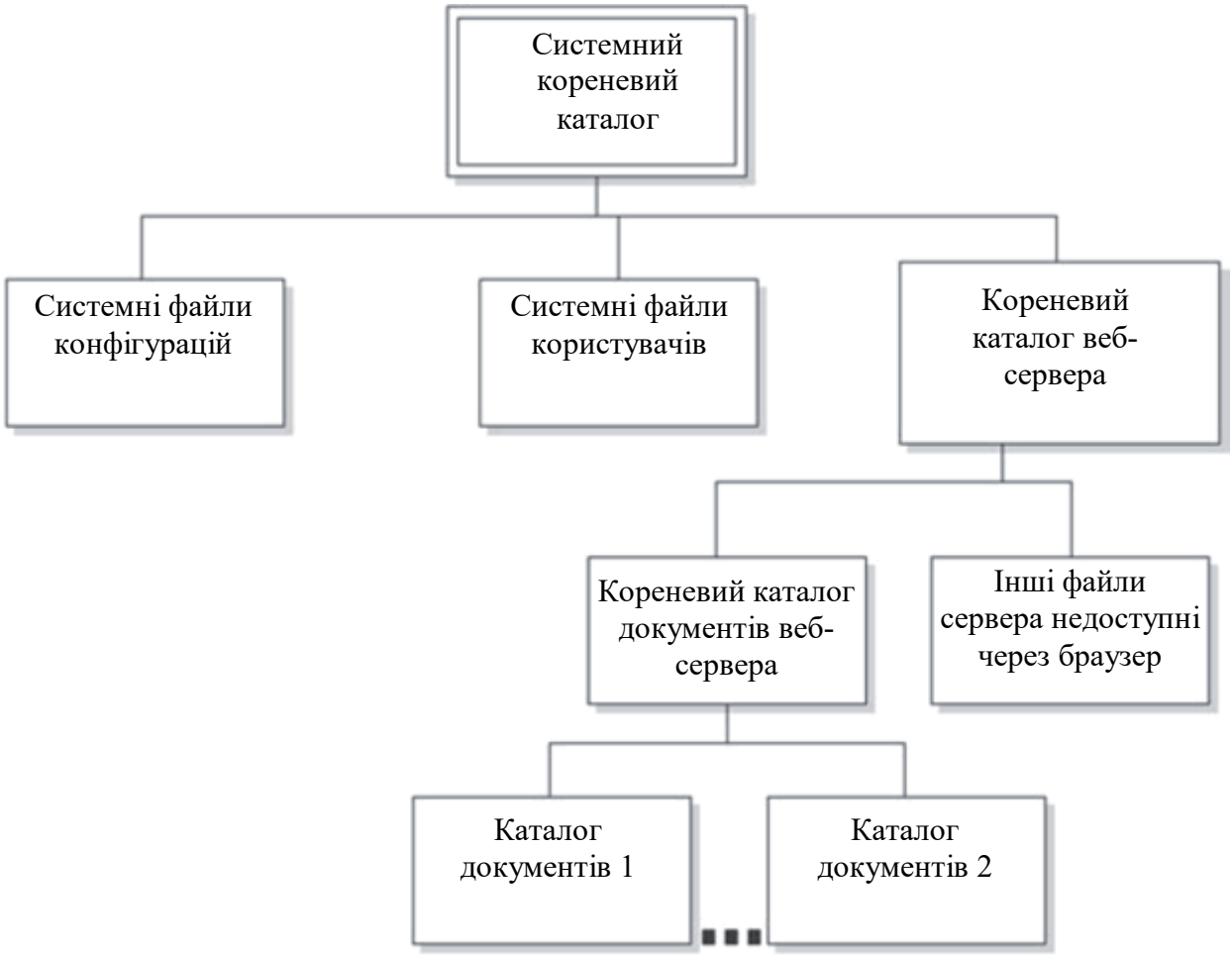

Рисунок 12.4 – Коректна структура кореневого каталогу веб-серверу

Більша частина веб-серверів співставляється зі сценаріями CGI (CGI – загальний шлюзовий інтерфейс; дана технологія використовується для створення сценаріїв на веб-сервері). Деякі сценарії, наявні за замовчуванням, містять дуже серйозні уразливості, які дозволяють зловмисникам одержувати доступ до файлів або до самої системи. Будь-які сценарії, що поставляються з веб-сервером, які не використовуються веб-сайтом, повинні бути вилучені, щоб запобігти їх запуску зловмисником з метою одержання доступу до системи.

Сценарії CGI не повинні бачити звичайні користувачі, тобто веб-сервер потрібно налаштувати на приховання списків каталогів, якщо в браузері не зазначений файл. Якщо в браузері зазначений сценарій CGI або

Perl, сервер потрібно налаштувати на виконання сценарію, а не на відображення коду. Звичайно даний аспект настроюється у файлі httpd.conf у наступних рядках:

AddType application/ x-httpd-cgi .cgi

AddType application/ x-httpd-cgi .pl

Як у випадку з операційною системою, веб-сервер необхідно просканувати на наявність уразливостей, перш ніж вводити в роботу. Отут можливе використання того ж сканера, за допомогою якого здійснювалося сканування операційної системи, однак необхідно, щоб він забезпечував тести, спеціалізовані для веб-серверу. Як тільки система буде введена в роботу, необхідно почати виконання сканування відповідно до розкладу, що використовувались при скануванні операційної системи.

Реалізація безпеки застосувань

Безпека застосувань електронної комерції є, можливо, найбільш важливим компонентом системи безпеки. Застосування передбачає процедури по проведенню операцій, таких як зміна сторінок і відновлення програмного забезпечення.

Правила розробки застосування

Почнемо обговорення безпеки застосування з розробки самого застосування. При розробці застосування електронної комерції організація повинна виконати ті ж кроки проектування, що й при розробці будь-якої великомасштабної й комплексної системи, а саме:

– визначення вимог;

– системне проектування;

– розробка;

– тестування;

– реалізація.

Всі ці кроки повинні бути викладені в посібнику з розробки, наявному в організації.

Вимоги безпеки варто включити в етап визначення вимог проекту. Ці вимоги містять в собі наступне:

– визначення секретної інформації;

– захист вимог для секретної інформації;

– вимоги автентифікації для доступу або виконання операцій;

– вимоги до аудита;

– вимоги доступності.

Якщо ці вимоги визначені, то при проектуванні системи можна буде виявити потенційні проблеми. Вся секретна інформація повинна певним чином захищатися. Це спричиняє наявності компонентів застосунку, що вимагають HTTPS замість HTTP. Для секретної інформації потрібно не тільки шифрування при передачі. Деякі дані, наприклад приватні відомості про клієнта, вимагають захисту при записі на комп'ютер клієнта в елементах cookie. При проектуванні необхідно приймати це в розрахунок, і в цьому випадку використовувати шифрування елементів cookie.

Необхідно також згадати ще одне питання, пов'язане із секретною інформацією. Інформація може стати секретною через метод, за допомогою якого вона використовується в застосунку. Наприклад, деякі додатки передають інформацію між програмами з використанням URL (універсального покажчика ресурсів, що представляє собою адресу веб-сайту в адресному рядку браузера). Якщо відображається довгий URL зі знаком питання "?", що відокремлює різні значення, то застосунок передає параметри іншим сценаріям або програмам. Клієнт може поміняти ці параметри й змінити функціонування програм. Деякі сайти електронної комерції записують обрані покупцями товари в адресах URL. Ця інформація містить код товару, кількість і вартість. Якщо в базі даних не здійснюється перевірка даних, клієнти можуть змінювати ціну товарів. Був випадок, коли клієнт помітно зменшив ціну, і організація фактично продала товар по дуже низькій ціні. Беручи до уваги цей приклад, стає

ясно, що вартість товарів є дуже важливою інформацією. Якщо для передачі цієї інформації між сценаріями або програмами використовується URL, значення вартості (принаймні) повинні перевірятися в базі даних перед обробкою замовлення.

В інформаційних системах може зберігатися така секретна інформація, як номера кредитних карт. Як уже говорилося раніше, у жодному разі не рекомендується зберігати настільки значиму інформацію на самому веб-сервері. При проектуванні системи необхідно розробити механізм окремого збереження цієї інформації: або зберігати ці дані на сервері бази даних, або видаляти їх після використання. При ухваленні рішення про те, зберігати або не зберігати інформацію про кредитні карти, варто керуватися думкою на цей рахунок клієнтів компанії. Деякі фахівці з маркетингу говорять, що клієнт воліє, щоб процедури електронної комерції були більш простими й швидкими, і що повторне введення номерів кредитних карт може змусити клієнтів звернутися до іншого сайту. Із цієї причини даний аспект перетворюється у вимогу. Якщо так і є, номера кредитних карт повинні зберігатися в тому місці, в якому ризик успішного проведення атаки невеликий.

Організація може запобігти даній проблемі за допомогою залучення зовнішньої партнерської організації для обробки транзакцій із кредитними картами. При цьому інформація про покупку повинна передаватися партнерові. Необхідно ретельно забезпечити коректність передачі інформації.

Правильні методи програмування

Будь-який застосунок електронної комерції вимагає деяких зусиль по роботі з кодом сценаріїв або програм. Як правило, це особливі програми, розроблені спеціально для конкретного середовища й ситуації. Програми являють собою основне джерело системних уразливостей, причинами яких є помилки, допущені при програмуванні. Самою значною

помилкою є переповнення буфера. Знизити ризик прояви цієї проблеми можна в такий спосіб:

– вказівка обмеженого розміру даних, що вводяться користувачем;

– передача неперевірених уведених користувачем даних командам оболонки.

Якщо програміст указує обмеження розміру даних, що вводяться користувачем, то він, як правило, визначає конкретний розмір змінних. Якщо зловмисник про це знає, то зможе ввести такі дані, які викличуть переповнення буфера, з наступним одержанням доступу до файлів або операційної системи.

Друге питання є частковим випадком першої проблеми. Якщо програми викликають команди оболонки, то дані, що вводяться користувачем, не повинні наосліп передаватися команді оболонки – вони повинні перевірятися на відповідність даній команді.

Багато які із цих помилок можна усунути, перед тим як сайт буде введений у роботу, якщо відповідний код ретельно перевірити. На жаль, деякі програмні проекти передбачають досить часу для виконання цієї дії. Принаймні, члени групи розробки повинні бути проінструктовані з питань безпеки щодо цих типів помилок перед початком програмування.

Загальнодоступність вихідного коду

Сканери уразливостей повинні виявити проблеми, пов'язані з переповненням буфери, у широко відомих програмах і сценаріях, перед тим як сайт буде уведений у роботу. Даний крок є життєво необхідним, так як дані уразливості добре відомі в співтоваристві хакерів і можуть використовуватися для проведення атак, спрямованих на сайт. Уразливості до переповнення буфера в спеціально розробленому коді невідомі зловмисникам і не можуть бути легко виявленими. Проте, якщо атакуючий сильно зацікавлений у проникненні на сайт електронної комерції, він буде використовувати будь-яку доступну інформацію, щоб знайти уразливість.

Однією з дій, які може почати хакер, є перевірка сценаріїв через веб-сайт. Правильна конфігурація веб-серверу повинна обмежувати можливості хакера по виконанню цих дій, однак якщо на сайті є сценарії, у конфігурації може бути допущена помилка, що дозволить зловмисникові переглянути ці сценарії. Ще одним способом запобігання перегляду сценаріїв є написання всього застосунку на компилюємій мові (C або C++) замість інтерпретуємих мов (CGI і Perl).

Керування конфігурацією

Як тільки застосунок написаний і протестований, він здається в роботу й відкривається для широкої громадськості. Якщо до даного моменту дотримувалися рекомендації з безпеки, то можна вважати, що був прийнятий ряд обережностей для захисту сайту. Однак на цьому робота над питаннями безпеки не закінчується. Залишився ще один важливий компонент безпеки, який необхідно взяти до уваги – керування конфігурацією. Керування конфігурацією можна розділити на дві частини.

– Контроль за санкціонованими змінами.

– Виявлення несанкціонованих змін.

Контроль санкціонованих змін здійснюється за допомогою процедур і політик. Тільки певні співробітники допускаються до внесення змін у програми або веб-сторінки. Перед установкою програмних відновлень їх необхідно тестувати у системі розробки або контролю якості. Зміни, внесені у веб-сторінки, повинні проходити контроль якості для виявлення орфографічних і граматичних помилок.

Розробка й тестування повинні здійснюватися на окремій системі, що імітує робочу систему. На робочій системі не повинні здійснюватися які б то не було дії по розробці або відновленню програмного забезпечення.

Визначення несанкціонованих змін повинно проводитися для кожної системи, що представляється широкій громадськості дані, пов'язані з організацією. Головним прикладом тут, без сумніву, є сайт електронної

комерції. Кожний програмний компонент (сценарій або скомпільована програма) і кожна статична веб-сторінка повинна постійно перевірятися на наявність несанкціонованих змін. Найчастіше це реалізується за допомогою використання криптографічної контрольної суми. При розміщенні файлу на робочій системі для нього необхідно згенерувати контрольну суму. Періодично варто повторно генерувати контрольну суму й зіставляти її з оригіналом. Якщо контрольні суми виявилися різними, необхідно видати відповідне повідомлення й перевірити систему на проникнення зловмисника. У позаштатних ситуаціях програма, що виконує перевірку, може перезавантажувати копію вихідного файлу. Для запобігання фіктивної тривоги необхідно здійснювати відновлення контрольної торби в рамках процедури керування конфігурацією.

Реалізація безпеки серверу бази даних

Для завершення роботи над системою безпеки необхідно, крім усього іншого, забезпечити захист серверу бази даних, що містить інформацію про всі комерційні транзакції. Усередині мережі організації повинна бути присутня база даних, у яку записується вся інформація про клієнтів, замовлення, доставку й транзакціях. Ця база містить великий обсяг секретної інформації. Інформація в базі даних може бути конфіденційною по своїй природі, що вимагає деякого захисту конфіденційності, або вона є секретною й необхідно забезпечити її коректність, що спричиняє вимогу до забезпечення цілісності. Сервер може являти собою ключовий компонент у системі електронної комерції й вимагати захисту доступності.

Беручи до уваги таємність інформації в базі даних, необхідно перевірити наступні аспекти:

– розташування серверу бази даних;

– яким чином сервер бази даних з'єднується з веб-сервером або сервером застосунків;

– яким чином веб-сервер захищений від внутрішніх користувачів.

Розташування бази даних

Як у випадку з веб-сервером, фізичним розташуванням системи повинно бути місце, доступ до якого контролюється. Для цієї мети добре підходить інформаційний центр. Хоча сервер бази даних може бути розташований у сусідньому приміщенні, таємність інформації з бази даних спричиняє той факт, що вона повинна перебувати в області, повністю контрольованою організацією.

Найкращим розташуванням серверу бази даних є внутрішня мережа організації. Немає ніяких причин для того, щоб надавати доступ до серверу бази даних ззовні організації, тому даний сервер не потрібно підключати до Інтернету. Ця система користується повною довірою, а також не представляє яких-небудь додаткових ризиків для внутрішньої мережі, розташовуючись усередині її.

У деяких випадках сервер бази даних є настільки секретним, що розташовується в окремій частині мережі. Цей сегмент мережі захищається внутрішнім міжмережевим екраном, і проходження трафіку через міжмережевий екран у значній мірі обмежено.

З'єднання із сервером електронної комерції

Сервер бази даних повинен з'єднуватися із сервером електронної комерції таким чином, щоб можна було здійснювати обробку транзакцій. Як правило, дане з'єднання здійснюється через з'єднання SQL (див. рисунок 12.5). В ідеальному випадку сервер бази даних ініціює з'єднання із системою в демілітаризованій зоні. Це ідеальна ситуація, так як система в демілітаризованій зоні не є довіреною частиною мережі й не повинна з'єднуватися із внутрішньою або довіреною частиною мережі. Однак тут потрібно, щоб сервер електронної комерції зберігав інформацію про транзакції (а також запити) до того, як сервер бази даних ініціює з'єднання. Ця обставина може привести до затримки транзакцій або надання клієнтові інформації. У більшості випадків цей варіант неприйнятний.

Єдиною альтернативою є ініціювання SQL-з'єднання сервером електронної комерції, що веде до виникнення ряду питань, пов'язаних з безпекою. По-перше, сервер електронної комерції повинен мати ідентифікатор і пароль до серверу бази даних, щоб виконати дану дію. Цей ідентифікатор і пароль повинні додаватися в програмі або записані у файлі системи. Якщо ідентифікатор і пароль перебувають у системі електронної комерції, зловмисник може заволодіти ними й одержати доступ до серверу бази даних. Так як сервер бази даних містить секретну інформацію, це вкрай неприпустимо.

Один зі способів уникнути цієї ситуації – зробити так, щоб ідентифікатор і пароль, використовувані сервером електронної комерції, був прив'язаний до ідентифікатора з більшими обмеженнями. Ідентифікатор буде мати можливість доступу для відправлення інформації про транзакцію в одну таблицю (доступ запису), однак не буде мати права доступу для читання таблиць з бази даних. Дана конфігурація придатна для деяких застосунків, однак вона не дозволяє серверу електронної комерції одержувати інформацію для подання клієнтові. При необхідності ідентифікатору можна привласнити право доступу для читання несекретної інформації в базі даних, наприклад інформації каталогу, щоб здійснювати відповідний запит даних і відображати їхньому клієнтові.

Як бути у випадку, якщо інформація, яку потрібно представити клієнтові, є секретною? Це дуже серйозна проблема. Наприклад, клієнт банку запитує дані про баланс на своєму рахунку? Як обробити такий запит? У найкращому разі, ідентифікатор і пароль, що перебувають на сервері електронної комерції, можуть бути скомбіновані з деяким видом автентифікації, через яку проходить клієнт. Таким чином, якщо зловмисник проникне на сервер електронної комерції, він не зможе одержати доступ до секретної інформації про клієнтів.

Даний ризик можна знизити ще більше, розділивши функціональність серверу електронної комерції між веб-сервером і

сервером застосунків. Веб-сервер представляє інформацію клієнтові й приймає дані, що вводяться клієнтом. Сервер застосунків обробляє інформацію, отриману від клієнта, запитує сервер бази даних і передає інформацію веб-серверу для подання клієнтові (див. рисунок 12.5).

Рисунок 12.5 – Переглянута архітектура електронної комерції, у якій використовується сервер застосунків

Захист внутрішнього доступу

Всі питання безпеки, які ми обговорювали дотепер, були пов'язані із зовнішніми погрозами. На жаль, це не єдині погрози, що підлягають обов'язковому розгляду. У співробітників організації є доступ до внутрішньої мережі, у якій перебуває сервер бази даних, і, отже, вони мають можливість безпосередньо атакувати його без необхідності долати міжмережевий екран і веб-сервер.

Одне з рішень даної проблеми вже було згадано раніше. Сервер бази даних можна перенести в окрему мережу й захистити внутрішнім міжмережевим екраном. Однак це не єдине рішення проблеми. Сервер необхідно сканувати на наявність уразливостей згідно тому ж розкладу, що рекомендується для веб-серверу. Програмне забезпечення серверу необхідно оновити й доповнити, перш ніж уводити сервер в експлуатацію, а ідентифікатори й паролі повинні контролюватися згідно тому, як це визначено в політиці безпеки. Крім цього, базу даних необхідно налаштувати на аудита спроб доступу до неї.

Бази даних надають зловмисникові можливість одержання доступу до інформації без необхідності доступу в базову операційну систему. Для того щоб правильно відслідковувати систему на предмет спроб доступу й використання уразливостей, необхідно стежити як за системними журналами, так і за журналами баз даних.

Беручи до уваги таємність інформації, що втримується в базі даних, варто здійснювати контроль санкціонованого доступу до системи. Система не повинна перебувати в загальному користуванні, і, крім того, у даній системі повинні бути заборонені які-небудь дії по розробці.

Розробка архітектури електронної комерції

Давайте тепер узагальнимо всі обговорені аспекти. На рисунку 12.6 представлена схема всього сайту електронної комерції в цілому. Тут зображені архітектурні компоненти, що забезпечують повноцінний сайт із високим ступенем доступності й більшим обсягом минаючого трафіку.

Залежно від кількості трафіку й установлених вимог безпеки деякі з компонентів можуть не бути необхідними.

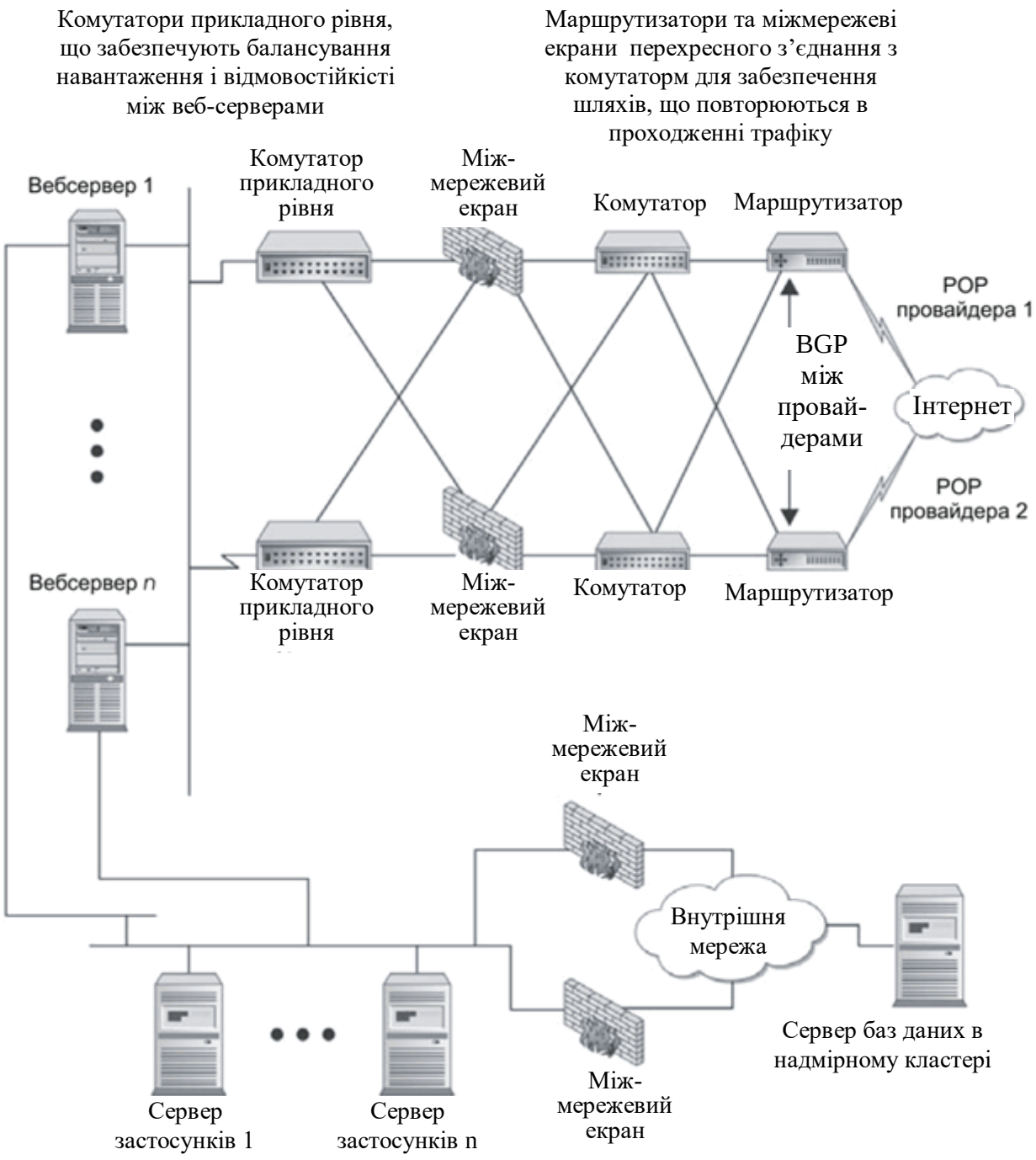

Рисунок 12.6 – Архітектура системи електронної комерції для сайту з високим ступенем доступності

Розташування серверу й з'єднання

Розглядається сайт із високим ступенем доступності й більшим обсягом оброблюваного трафіку. Організація має зв'язок із двома різними провайдерами Інтернет-послуг, і з ними досягнуто згоди про використання BGP для забезпечення відказостійкої маршрутизації. У цьому випадку мається на увазі, що організація зволіла розмістити свої сервери електронної комерції в одному приміщенні. Дана архітектура могла б бути розширена для включення інших будинків.

Маршрутизатори, комутатори й міжмережеві екрани, підключені до Інтернету, з'єднані між собою таким чином, що збій у будь-якому компоненті ніяк не вплинув на трафік сайту. За міжмережевими екранами два комутатори прикладного рівня забезпечують розподіл навантаження між веб-серверами. Веб-сервери захищені міжмережевими екранами від атак по всіх портах, крім 80 і 443.

Веб-сервери мають другий мережевий інтерфейс, що забезпечує з'єднання з мережею, у якій розташовані сервери застосунків. Веб-сервери передають інформацію серверам застосунків, що запитують бази даних і передають дані клієнта на веб-сервери. Подвійні міжмережеві екрани з'єднують мережу серверу застосунків із внутрішньою мережею організації, у якій перебуває сервер бази даних. Вартість цих властивостей доступності більш ніж у два рази перевищує вартість базового Інтернет-сайту. Така структура вимагає наявності, принаймні, двох об'єктів із всіх мережевих компонентів і серверів, а також передбачає використання комутаторів прикладного рівня. Залежно від навантаження трафіком число веб-серверів і серверів застосунків велике (наприклад, більш ніж 20 одиниць кожного з об'єктів). Ця обставина також вимагає того, щоб сервер бази даних мав можливість обробки великої кількості транзакцій у секунду.

Якщо для сайту ключовим фактором є рівень затримок, можна забрати міжмережеві екрани. Хоча це й нерозумно з погляду безпеки,

даний крок необхідний для забезпечення вимог, пропонованих до рівня затримок. У цьому випадку маршрутизатори повинні бути настроєні на фільтрацію всього трафіку, а не тільки трафіку, що надходить через порти 80 і 443.

Сканування уразливостей

Для періодичного сканування всіх систем є стандартна програма. Сканування здійснюється із чотирьох місць розташування:

– Поза зоною, що охороняється міжмережевим екраном; показує, які порти є дозволеними міжмережевим екраном, і які уразливості видні з Інтернету.

– У мережі веб-серверу для виявлення служб і уразливостей на веб-серверах.

– У мережі серверу застосунків для виявлення служб і уразливостей на другому інтерфейсі веб-серверу й на серверах застосунків.

– У внутрішній мережі організації для виявлення служб і уразливостей у сервері бази даних.

Ці дії по скануванню виконуються щомісяця, і виправлення уразливостей відслідковується. Нові системи скануються перед уведенням в експлуатацію.

Дані аудита й виявлення проблем

Протоколи аудита на сервері бази даних перевіряються для виявлення внутрішніх співробітників, які здійснюють спроби внесення змін у базу даних. Ключові файли на веб-серверах і серверах застосунків перевіряються на зміни через кожні 10 хвилин для швидкого виявлення систем, у які можуть проникнути зловмисники.

Розробка архітектури сайту електронної комерції

Даний проект показує етапи розробки сайту, призначеного для реалізації електронної комерції. У рамках даного проекту будемо вважати, що банку потрібно надати своїм клієнтам домашню банківську систему. У банку вже є центр даних з відповідними мірами фізичної безпеки. Вся

інформація про облікові записи клієнтів зберігається на головному комп'ютері. У кожного клієнта є особистий ідентифікаційний номер PIN, використовуваний на автоматизованих банкоматах.

Керівництво банку вирішило надавати клієнтам доступ до їхніх облікових записів для виконання наступних дій.

– Передача засобів між обліковими записами в банку.

– Замовлення по чеку.

– Перевірка балансу облікових записів і перегляд недавніх транзакцій.

– Платежі по рахунку через партнера (клієнт для цього буде переспрямований до партнера через веб-сайт без необхідності повторного входу в систему).

Крок за кроком

1. Почніть із визначення вимог безпеки для системи щодо кожного із чотирьох аспектів: конфіденційність, цілісність, доступність і автентифікація.

2. Розробіть структуру високорівневої системи, що відповідає вимогам безпеки. Для даної частини системи припустіть, що система буде взаємодіяти з головним комп'ютером для одержання інформації про обліковий запис клієнта й для виконання передачі даних і чекових замовлень.

3. Визначте конкретні вимоги безпеки для кожного компонента системи: система-клієнт, веб-сервер, застосунок і база даних.

4. Визначте загальну архітектуру системи, включаючи компоненти для захисту кожної системи.

6. Додайте до наявної структури додаткові системи для відповідності вимогам доступності.

Отже, даний проект є серйозним проектом розробки й вимагає зусиль великої кількості людей. Не забувайте сфокусувати увагу на аспектах безпеки структур. Це дозволить одержати більш детальне

подання про те, що таке процес розробки. Для коректного виконання даної роботи необхідно оцінити ризик, що представляється для банку, і визначити відповідні контрзаходи для керування цим ризиком.

Список використаних джерел

1.Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. / Под ред. Ю.С. Ковтанюка. – К.: Юниор, 2003. – 504 с.

2. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.

3. Макс Ронге. Разведка и контрразведка / М. Ронге /. – К.: СИНТО, 1993. - 239 с.

4. Мухачев В.А. Методы практической криптографии / Мухачев В.А., Хорошко В.А./ . – К.: ПолиграфКонсалтинг, 2005. – 214 с.

5. Мицан И.Б. Стеганографические методы сокрытия информации / Мицан И.Б. // Специальная техника и вооружение. Научно-методическое издание. – К., № 1 – 5, 2001. – С. 28 – 32.

6. Хорошко В.О. Основи комп'ютерної стеганографії. Навчальний посібник / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчик /. – Вінниця: ВДТУ, 2003. – 143 с.

7. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. /. – К.: «МК-Пресс», 2006. – 288 с.

8. Безопасность информационных технологий. Методология создания систем защиты/ В.В. Домарев. - К.: ООО "ТИД "ДС", 2001. - 688 с.

9. Энциклопедия промышленного шпионажа/ Под общ. ред. Е.В. Куренкова - С.Петербург: ООО "Изд-во Полигон", 1999. - 512 с.

10. Хорев А;А. Способы и средства защиты информации. - М.: МО РФ, 2000. -316 с.

11. А.Ю.Щербаков. Введение в теорию и практику компьютерной безопасности. -М.: издатель Молгачева С.В., 2001.

12. Бармен, Скотт. Разработка правил информационной безопасности.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002.

13. С.Л.Емельянов Основы информационной безопасности.– Одесса: Юридична література, 2003.-198с.

14. Про державну таємницю. Закон України №3855-XII від 21.01.1994 р. (в редакції Закону № 1079-14 від 21.09.99).

15. Про затвердження зводу відомостей, що становлять державну таємницю. Наказ Голови Служби безпеки України від 12.08.2005 р. № 440.

16. НД ТЗІ 1.1 – 002 – 99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Нормативний документ ДСТЗИ СБ Украйни. Киев, 1999.

17. Про інформацію. Закон України № 2657-ХП від 02.10.92 р.

18. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 8.10.97.

19. Положення про технічний захист інформації в Україні. Указ Президента України №1229/99 від 27.09.99.

20. Тимчасові рекомендації з технічного захисту інформації вид витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). Затверджені наказом ДСТЗІ від 09.06.95р. № 25.

21. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

22. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

23. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

24. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1, затвердженою наказом ДСТСЗІСБУ 18.06.02 № 37).

25. НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації \№ЕВ-сторінки від несанкціонованого доступу.

26. 13.ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

27. http://www.intuit.ru/department/security/secbasics/

28. Галатенко В.А. Основы информационной безопасности Интернет-университет информационных технологий – ИНТУИТ.ру, 2008

29. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия Интернет-университет информационных технологий – ИНТУИТ.ру, 2005

30. Галатенко В.А. Стандарты информационной безопасности Интернет-университет информационных технологий – ИНТУИТ.ру, 2005

31. Э. Мэйволд Безопасность сетей Эком, 2006

32. Хаулет Т. Защитные средства с открытыми исходными текстами БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий – ИНТУИТ.ру, 2007

33. Department of Defense Trusted Computer System Evaluation Criteria DoD 5200.28-STD, 1993.

34. Information Technology Security Evaluation Criteria (ITSEC). Harmonized Criteria of France – Germany – the Netherlands – the United Kingdom Department of Trade and Industry, London, 1991.

35. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800 CCITT, Geneva, 1991.

36. Site Security Handbook. Holbrook P., Reynolds J., Request for Comments: 1244, 1991.

37. James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback Report on the Development of the Advanced Encryption Standard (AES) Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Technology Administration U.S. Department of Commerce. 2000г. 116с.

38. Государственный Стандарт Российской Федерации Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма 1994г.

39. Государственный Стандарт Российской Федерации Информационная технология. Криптографическая защита информации. Функция хэширования 1994г.

40. RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 2002г. 129с.

41. RFC 3281 An Internet Attribute Certificate Profile for Authorization 2002г. 40с.

42. RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols 1999г. 72с.

43. RFC 2511 Internet X.509 Certificate Request Message Format 1999г. 25с.

44. RFC 3369 Cryptographic Message Syntax 2002г. 60с.

45. RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP 1999г. 23с.

46. RFC 2797 Certificate Management Messages over CMS 2000г. 47с.

47. RFC 3379 Delegated Path Validation and Delegated Path Discovery Protocol Requirements 2002г. 15с.

48. RFC 2633 S/MIME Version 3 Message Specification 1999г. 32с.

49. RFC 2632 S/MIME Version 3 Certificate Handling 1999г. 13с.

50. Security Architecture for the Internet Protocol RFC 2401 1998г. 66с.

51. Internet Security Association and Key Management Protocol (ISAKMP) RFC 2408 1998г. 86с.

52. The Internet Key Exchange (IKE) RFC 2409 1998г. 41с.

53. RFC 2412 The OAKLEY Key Determination Protocol 1998г. 55с.

54. Смірнов О.А., Віхрова Л.Г., Осадчій С.І., Ковтун В.Ю, Мелешко Є.В. Основи захисту інформаціїї. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки України від 16.12.2010 року. № 1/11-11486. – Кіровоград 2008 – 322 с.

55. Смірнов О.А., Євсеєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж.

Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 1.12.2011 року № 1/11-11258. – Кіровоград: КНТУ 2012. – 454 с.

56. Смірнов О.А., Мелешко Є.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 17.04.2012 року № 1/11-5249. – Кіровоград: КНТУ 2012. – 250 с.

57. Смірнов О.А., Кузнецов О.О., Євсеєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5762. – Кіровоград: КНТУ 2012. – 315 с.

58. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. С.В. Кавуна. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5760. – Кіровоград: КНТУ 2012. – 442 с.

59. Смірнов О.А., Інформаційна безпека в комп'ютерних мережах: методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання за спеціальностями «Комп'ютерна інженерія», «Комп'ютерні науки» / уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов – Кропивницький: ЦНТУ – 2017. – 69 с.

60. Смірнов О.А., Інформаційна безпека в комп'ютерних мережах: методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання за спеціальностями «Комп'ютерна інженерія», «Комп'ютерні науки» / уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов – Кропивницький: ЦНТУ – 2017. – 69 с.

61. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.

62. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.

63. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.

64. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2014. – № 4(17). – С. 90-95.

65. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 150-153.

66. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

67. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.

68. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

69. Смирнов С. А. Комплекс GERT-моделей технологии облачной антивирусной защиты телекоммуникационной системы /

А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. - практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

70. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. – № 2 (46). – С. 146-149.

71. Смирнов С. А. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2016. – Вип. 3 (140). – С. 36-39.

72. Смирнов С. А. Метод безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы / В. Л. Бурячок, С. А. Смирнов // Системи управління, навігації та зв'язку. – Полтава, 2016. – Вип. 4(40). – С. 57-62.

73. Смирнов С. А. Способ контроля линий связи телекоммуникационной системы облачного антивируса / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2016. – № 2 (47). – С. 148-152.

Зміст

Вступ……3
ЗАГАЛЬНІ ВІДОМОСТІ ПРО АТАКИ НА ПРОГРАМНЕ ЗАБЕЗПЕ-ЧЕННЯ ТА ДАНІ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ……5
Комп'ютерні атаки й технології їхнього виявлення……..…..5
Етапи реалізації атак……..…..8
Класифікація атак……..15
DDoS – комп'ютерні атаки. Технології їхнього виявлення. Захист…….17
Варіанти реакцій на виявлену атаку……18

МІЖМЕРЕЖЕВІ ЕКРАНИ (ФАЄРВОЛИ, БРАНДМАУЕРИ)…….20
Технології міжмережевих екранів……...24
Стани TCP-з'єднання…….....28
Класифікація міжмережевих екранів…….……..31
Фільтрування пакетів……32
Пакетні фільтри з аналізом стану……....39

ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ (VPN)…….……43
Визначення віртуальних приватних мереж……44
Розгортання користувальницьких віртуальних приватних мереж…….46
Розгортання вузлових мереж VPN……..….52
Поняття стандартних технологій функціонування VPN……...…56
Сервер VPN……57
Алгоритми шифрування……..…….60
Система автентифікації…….61
Протокол VPN……...……62
Типи систем VPN……..……..…….63

ТЕХНОЛОГІЇ ТУНЕЛЮВАННЯ……..…..67
Протокол GRE……..……67
Віртуальні приватні мережі……..…68

Протоколи канального рівня……..….70
Протокол автентифікації Challenge-Handshake (CHAP)……...76
Розширення Microsoft PPP CHAP версії 1……..…80
Розширення Microsoft PPP CHAP версії 2……..83
Конфігурація LCP……..84
Протокол шифрування MPPE Microsoft……..88
Протокол конфігурування IP – IPCP……..….90

АРХІТЕКТУРА БЕЗПЕКИ ДЛЯ IP (IPSEC)……..93
Призначення сімейства протоколів IPSec……..……93
Можливі способи реалізації IPSec…….…..95
Протоколи захисту трафіку й поняття безпечної асоціації……..……96
Поняття домену IPSec…….…..99
Можливі топології IPSec…….……101
Інші топології……...…106
Обробка трафіку, виконувана ESP…….111
Алгоритми……...….113

ПРОТОКОЛ SSL/TLS……...……118
Протокол Запису……..……121
Протокол укостискання……..……125
Додавання додаткових можливостей до протоколу…….133
Перемовини про максимальну довжину фрагмента……135
URL сертифікат клієнта……..…136

БЕЗПЕКА БЕЗДРОТОВИХ З'ЄДНАНЬ……...138
Сучасні бездротові технології……...….138
Стандартні архітектури…….……..139
Безпека передачі даних……..……139
WPA і WPA2……....140
Автентифікація в WLAN……143
Протокол 802.1X: контроль доступу в мережу по портах……..144

Питання безпеки бездротових з'єднань…….....145
Реалізація безпеки бездротових мереж……..…..148
Приклад реалізації бездротової локальної мережі……...…152

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS-СИСТЕМИ)……154
Визначення типів систем виявлення вторгнень……..….154
Вузлові IDS……..…155
Мережеві IDS…….……..160
Установка IDS……..…162
Вибір об'єкта моніторингу……..165
Автоматична й автоматизована відповідь……....174
Визначення порогів…….175
Застосування системи IDS…….….178
Дослідження підозрілих подій……...184
Розгортання мережної IDS…….....189

СИСТЕМИ ПРОТИДІЇ ВТОРГНЕННЯМ (IPS-СИСТЕМИ)……..192
Запобігання вторгнень……..……192
HIPS……..…195
Проблеми, пов'язані з виявленням вторгнень……..….200
Повнота бачення/структура IPS……..…..202
Ключові тенденції розвитку систем виявлення вторгнень…….…203

РЕАЛІЗАЦІЯ МЕРЕЖЕВОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ……..…205
Плани проектів безпеки…….….218
Мережеві з'єднання…….220
Захист від шкідливого коду……..…….222
Фізична безпека……...…229
Використання стандарту ISO 17799……..231

БЕЗПЕКА БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ ……...236
Безпека електронних платіжних систем……..…….236
Крадіжки грошей з пластикових карт із використанням банкоматів…….246
Електронна комерція: вимоги до безпеки……248
Служби електронної комерції……249
Реалізація безпеки клієнтської сторони……257
Реалізація безпеки серверної частини…….…..261
Реалізація безпеки застосувань…….……268
Реалізація безпеки серверу бази даних…….……273
Розробка архітектури електронної комерції……....277
Список використаних джерел……283