ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ТЕХНОЛОГІЯ ПОБУДОВИ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА ВІД НЕСАНКЦІОНОВАНИХ ВТРУЧАНЬ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ CISCO»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Циганок Д.О.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2021

РЕФЕРАТ

Текстова частина магістерської роботи: 82 сторінок, 18 рисунків, 8 таблиць, 24 джерела.

Об'єкт дослідження – процес безпечного функціонування інфраструктури підприємства;

Предмет дослідження – методи захисту інфраструктури підприємства від несанкціонованих втручань шляхом використання обладнання Cisco.

Мета роботи – розробка підходів щодо побудови захищеної інфраструктури підприємства від несанкціонованих втручань шляхом використання обладнання Cisco.

Методи дослідження – теорія інформації, стандарти у сфері кібербезпеки, алгоритми оцінки загроз інформаційної безпеки підприємства, практичне тестування програмного забезпечення.

В роботі проаналізовано широкий спектр рішень від Cisco, що здатні захистити інфраструктуру підприємства на будь-якому ієрархічному рівні незалежно від топології мережі. Розроблено топологію, що ілюструє мережу середньостатистичної компанії та проведено тестування програмного забезпечення. Зазначено, що час тестування склав 10 сек, при цьому результат позитивний. Програма коректно реагує на всі зміни у файлах налаштувань та конфігурацій, та може бути запропонована для тестування на реальному обладнанні Cisco. Зроблено висновок, що в основу запропонованого методу захисту мереж від несанкціонованих втручань, шляхом коректного налаштування Cisco обладнання покладено найкращі тенденції, та рекомендації, що були сформовані та перевірені власне самою компанією Cisco.

Галузь використання – кібербезпека

ІНФРАСТРУКТУРА, ПІДПРИЄМСТВО, CISCO, ACL, ASA, СИСТЕМА, НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ, МЕРЕЖА, СИСТЕМА, КІБЕРАТАКА, ВІРУС, АТАКА, ПЕРЕДАЧА ДАНИХ.

ABSTRACT

Master’s thesis: 82 pages, 18 figures, 7 tables, 24 sources

Object of research - the process of safe functioning of the enterprise infrastructure

Subject of research – the method of protecting enterprise infrastructure from unauthorized intrusion through the use of Cisco equipment.

The aim of research is to develop approaches to building a protective enterprise infrastructure from unauthorized intrusion through the use of Cisco equipment.

Research methods - information theory, cybersecurity standards, algorithms for assessing threats to information security of the enterprise, practical software testing.

The paper analyzes a wide range of solutions from Cisco, capable of protecting enterprise infrastructure at any hierarchical level, regardless of network topology. A typical network topology was developed, and a software testing was conducted. It is noted that the testing time was 10 seconds, with a positive result. The program responds correctly to all changes in file settings and configurations, and can be recommended for testing on a real Cisco.

The method proposed of protecting networks from unauthorized interference is based on correctly configuring Cisco equipment and is based on the best trends and recommendations, which were formed and tested by Cisco

Field of use – cybersecurity.

INFRASTRUCTURE, ENTERPRISE, CISCO, ACL, ASA, SYSTEM, UNAUTHORIZED INTRUSION, NETWORK, SYSTEM, CYBERATTACK, VIRUS, ATTACK, DATA TRANSMISSION.

ЗМІСТ

ВСТУП

Актуальність дослідження. Здається логічним, що в будь-якій організації, такій як комерційне підприємство чи державна структура, повино бути створене та налагоджене безпечне функціонування всіх процесів. Організація, яка може продемонструвати захищену інфраструктуру може потенційно знизити страхові внески та може використовувати свою програму безпеки як маркетинговий інструмент, демонструючи клієнтам, що їх дані, продукт чи послуги захищені. Але найголовніше – безпечній організації не доведеться витрачати час і гроші на ідентифікацію порушення безпеки та реагування на результати порушення.

У минулому термін «інформаційна безпека» використовувався для опису заходів фізичної безпеки, що використовуються для запобігання доступу громадськості до важливої урядової чи комерційної інформації та для захисту її від зміни чи знищення. За рахунок поступового впровадження інформаційних технологій з’являлися все нові технології, методи та системи для збирання, опрацювання, зміни та передавання інформації. Методи захисту даних різко змінилися, тому і гостріше почало лунати питання безпеки не лише самої інформації, але й каналів, вузлів, обладнання, яке приймає участь в процесі передачі.

Звідси і випливає, що правильне та коректне налаштування мережевого обладнання, такого як брандмауер або маршрутизатор, може дати можливість уникнути більшості несанкціонованих втручань, які проникають від зловмисників із мережі, при передачі інформації.

Об’єкт дослідження – процес безпечного функціонування інфраструктури підприємства;

Предмет дослідження – методи захисту інфраструктури підприємства від несанкціонованих втручань шляхом використання обладнання Cisco.

Мета роботи – розробка підходів щодо побудови захищеної інфраструктури підприємства від несанкціонованих втручань шляхом використання обладнання Cisco.

Наукові завдання:

– проаналізувати моделі безпеки для побудови інфраструктури підприємства з використанням обладнання Cisco;

– дослідити функції безпеки мережевих пристроїв Cisco;

– виокремити рекомендації щодо вибору ios для потреб безпеки інфраструктури підприємства;

– розглянути модель протидії наслідкам несанкціонованих втручань з використанням рішень безпеки Cisco;

– дослідити особливості впровадження безпечних ідентифікаторів Cisco для профілактики несанкціонованим втручанням .

Методи дослідження – теорія інформації, стандарти у сфері кібербезпеки, алгоритми оцінки загроз інформаційної безпеки підприємства, практичне тестування програмного забезпечення.

Практичне значення одержаних результатів полягає в розробці підходів щодо побудови захищеної інфраструктури підприємства від несанкціонованих втручань шляхом використання обладнання Cisco.

1 АНАЛІЗ МОДЕЛЕЙ БЕЗПЕКИ ДЛЯ ПОБУДОВИ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ОБЛАДНАННЯ CISCO

Необхідність створення захищеної корпоративної мережі або побудова захищеної інфраструктури підприємства за допомогою кількох маршрутизаторів, комутаторів, серверів, робочих станцій являється найбільш актуальним сьогодні завданням. Перш ніж приступити до питань безпеки в корпоративній мережі, необхідно розуміння роботи мережі на більш загальному рівні. Для цього виключно важливим є питання нормального функціонування не лише всіх протоколів маршрутизації, але й розуміння ролі та функцій усіх розгорнутих мережевих пристроїв.

Професійний, кваліфікований зловмисник розглядає мережу як єдине ціле. Він або вона не пропустить можливості проникнути в будь-який мережевий пристрій, де це можливо, використовувати його для подальшої експлуатації.

Це схоже на отримання облікових даних користувача в системі, оскільки після їх отримання набагато легше отримати локальний доступ.

Захист, який необхідно розгорнути для інфраструктури підприємства чи організації, має охоплювати всі сім рівнів моделі OSI, враховуючи і безпеку кожного окремо розгорнутого хоста. На щастя, доступні рішення безпеки мережі Cisco охоплюють кожен окремий аспект мережі, що варіюється від магістральної багатопротокольної комутації та організації віртуальних приватних мереж (MPLS VPN) до захисту програмного забезпечення кінцевих точок комп’ютерів та ноутбуків користувачів.

На жаль, лише деякі системні адміністратори, мережеві інтегратори та архітектори, і навіть консультанти з IT-безпеки знають про масштаби та потужність цих рішень. Окрім того, ефективно та дійсно вигідно використовувати обладнання та продукцію компанії Cisco, адже при умові належного регулювання та налаштування, воно здатне захищати корпоративні мережі та мережі організацій та підприємств від будь-яких несанкціонованих втручань.

Залежно від розміру та призначення мережі, Cisco рекомендує кілька практичних моделей. Кожна модель має свої плюси і мінуси безпеки і сильно відрізнятиметься від інших, коли мова йде про наявність гарантій безпеки, конфігурації та обслуговування обладнання.

1.1. Модель безпеки «flat earth»

Модель «flat earth» - це базовий дизайн мережі на основі рівня 2. Раніше в її основі було покладено широке використання хабів, ретрансляторів та мостів. Сьогодні ж переважна більшість інфраструктур підприємств використовують комутатори та маршрутизатори, що призвело до змін і в безпроводовому світі (рішення 802.11) та навіть 802.15 (наприклад, технологія Bluetooth).

В ідеалі, модель «flat earth» повинна застосовуватися лише до локальних мереж невеликого офісу/домашнього користування. Однак є рекомендації, що зазначають можливість використання цієї моделі для мереж із розгортанням більш ніж 50 вузлів.

На практиці зазвичай підключаються кілька десятків користувачів на один домен, проте наявність безпроводового зв'язку здатно значно погіршити безпеку підключення. Проблема виникає в 12-портовому комутаторі, який може організувати підключення кількох точок доступу (з 30 до 40 користувачами) на кожну точку доступу. Крім того, багато комутаторів Cisco Catalyst мають високу щільність портів.

Якщо TCP/IP дозволяє підключати до 500 користувачів на локальну мережу без значного погіршення продуктивності через трансляцію трафіку, то розгортання інсталяторів мережі буде організовано без урахування питань управління та безпеки. Через обмежену кількість можливих заходів щодо організації безпеки, які можна вжити для протидії втручанням, модель «flat earth» вважається дуже небезпечною. До традиційних гарантій моделі входять: доступ до медіа, фільтрація MAC, сегментація мережі за допомогою віртуальних локальних мереж (VLAN).

При цьому, автентифікацію пристрою на основі MAC-адреси елементарно обійти. Однак, попередньо визначена кількість MAC-адрес на порти комутатора та призначення вручну всіх дозволених MAC-адрес є корисним, хоча і трудомістким завданням, яке зупиняє роботу атаки переповнення таблиці CAM комутатора.

І IOS, і Set/Clear Command Line Interface (CLI) Catalyst комутаторів підтримують фільтрацію MAC-адрес з широкими можливостями.

Процес управління великими таблицями фільтрації MAC-адрес не настільки громіздкий процес, як прийнято вважати. Можна вилучити та зберегти файл конфігурації комутатора (або лише таблицю CAM) та відредагувати його в залежності від вимог. Наприклад, для створення нового файлу конфігурації для завантаження в комутатор. Для цього навіть не потрібно входити в систему; інформацію про порти та MAC –адреси з комутаторів Catalyst легко отримати за допомогою протоколу SNMP.

При цьому, одразу випливають переваги сегментації VLAN. В спільноті Cisco вони також являються підсиленням для приватних мереж VLAN (PVLAN) та списків доступу до VLAN (VACL).

Приватна VLAN підтримується на комутаторах Catalyst 6000 під керуванням CatOS 5.4 або пізнішої версії Моделі Catalyst 4000, 2980G, 2980G-A, 2948G та 4912G під управлінням CatOS 6.2 або пізнішої версії. VACL підтримується комутаторами Catalyst 6000 з CatOS 5.3 або пізнішої версії і можуть бути реалізовані на Catalyst 6500 на 2-му рівні без використання маршрутизатора, якщо функція політики встановлена. Оскільки виконується пошук та виконання записів VACL в апаратних засобах немає штрафу за продуктивність, а швидкість пересилання залишається незмінною.

802.1x забезпечує механізм автентифікації та авторизації для підключення пристроїв до комутаторів, маршрутизаторів або точок безпроводового доступу. Фактична автентифікація та авторизація здійснюється службою віддаленої аутентифікації абонента (RADIUS) або терміналом доступу до сервера контролера доступу (TACACS) від імені автентифікатора пристрою (комутатор,

маршрутизатор або точка доступу) і на основі даних запиту (автентифікаційний хост). На рис.1.1, зображено захищену модель «flat earth» [1].

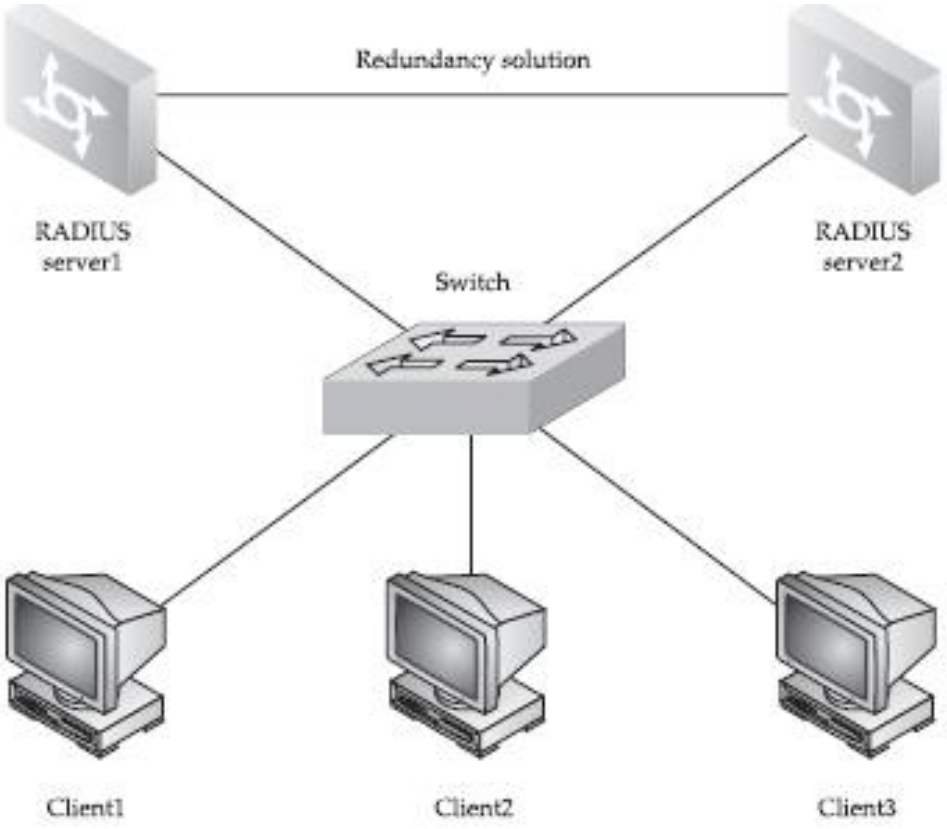

Рис.1.1. Модель «flat earth»

Два сервери RADIUS забезпечують автентифікацію та авторизацію для пристроїв кінцевого користувача, а комутатор служить пристроєм автентифікації. Додатковий зв'язок між серверами RADIUS забезпечує стійкість та протокол відмови (протокол HSRP) або протокол стійкості VRRP. При цьому важливо пам’ятати, що HSRP і, меншою мірою, VRRP мають відомі проблеми щодо безпеки, які необхідно враховувати при розгортанні цих протоколів.

Комутатори на рис.1.1., можуть бути із серії Catalyst, які підтримують технологію Cisco на основі ідентифікації мереж (802.1x, IBNS). Це комутатори Cisco Catalyst серії 4000, 4500 або 6500. Крім того, їх можна замінити на Cisco з можливістю точки безпроводового доступу Aironet з програмним забезпеченням, що підтримує захищений безпроводовий доступ (WPA).

1.2. Модель безпеки «зірка»

Модель «зірка» - це економічно ефективний дизайн мережі з одним маршрутизатором, який діє як фокус точка, що забезпечує з'єднання для всієї мережі. На рис.1.2 показаний концентратор VPN, що запропонований для використання замість звичайного маршрутизатора.

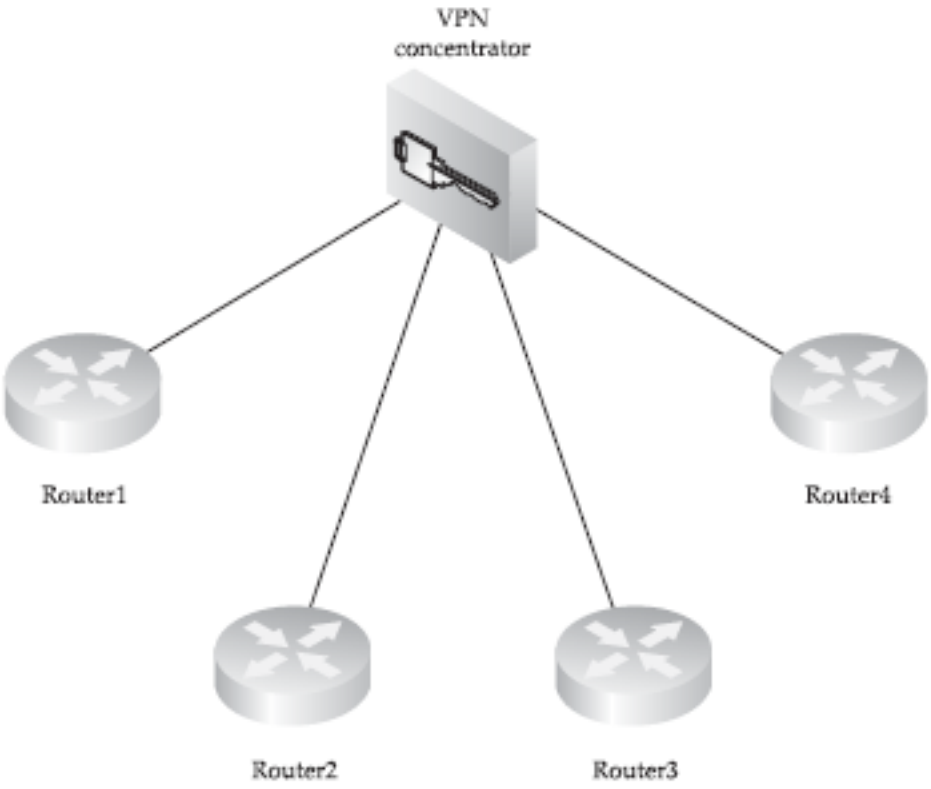

Рис.1.2. Модель дизайну зірки, що показує концентратор VPN

Дизайн мережі «зірка» найбільш поширений для розгортання реальних VPN, коли концентратор у центральному офісі забезпечує безпечні зв'язки з віддаленими офісами організації. Окрім концентратора VPN, маршрутизатор зі зоряним ядром ідеально розташований для виявлення вторгнень, фільтрації, збереження якості обслуговування (QoS) та підтримання політик безпеки та маршрутизації.

Однак, навіть з точки зору мінімалізму, маршрутизатор повинен бути модульним, а отже повинен: володіти достатнім обсягом пам’яті, потужним процесором для обробки всіх трафіків в мережі, включаючи безпеку (фільтрацію,

шифрування, аналіз IDS), мати подвійне резервування джерела живлення, і підтримувати контекстовий контроль доступу (CBAC).

Для таких цілей підходять маршрутизатори серії Cisco 7000 і вище, а також комутатори Catalyst 5000 і вище, та встановлені модулі комутатора маршрутизації (RSM). І при цьому, рекомендується розгортати пару однакових маршрутизаторів або комутаторів під керуванням Cisco HSRP або VRRP, з підтримкою версії IOS 12.0 (18).

Звичайно всі атаки на маршрутизатори/комутатори слід розглядати у контексті захисту ядра мережі «зірка», включаючи фізичний захист та гарантії соціальної інженерії.

Наступне, що потрібно зробити, це забезпечити наявність надійних обхідних, резервних маршрутів у разі виходу з ладу основних маршрутів або атаки на них (таких як атаки відмови в обслуговуванні/розподіленої відмови в обслуговуванні, DoS/DDoS). Найдешевше рішення це цифрова мережа інтегрованих служб на вимогу (ISDN) з попередньо налаштованою маршрутизацією [2].

1.3. Дворівнева модель

Ця модель мережі являє собою, по суті, дві зіркові мережі, з'єднані разом, як показано на рис.1.3. Ця модель розділяє контроль над усією мережею між двома вузлами таким чином, хто завгодно може отримати контроль над зв'язком між компонентами мережі в організації.

Однак, при запуску мережі, необхідно переконатися, що посилання захищене за допомогою IPSec. Потім необхідно розгорнути відмовостійкий позадіапазоний зв'язок між рівнями, наприклад резервне копіювання ISDN на вимогу посилання (запропоноване у моделі «зірка»).

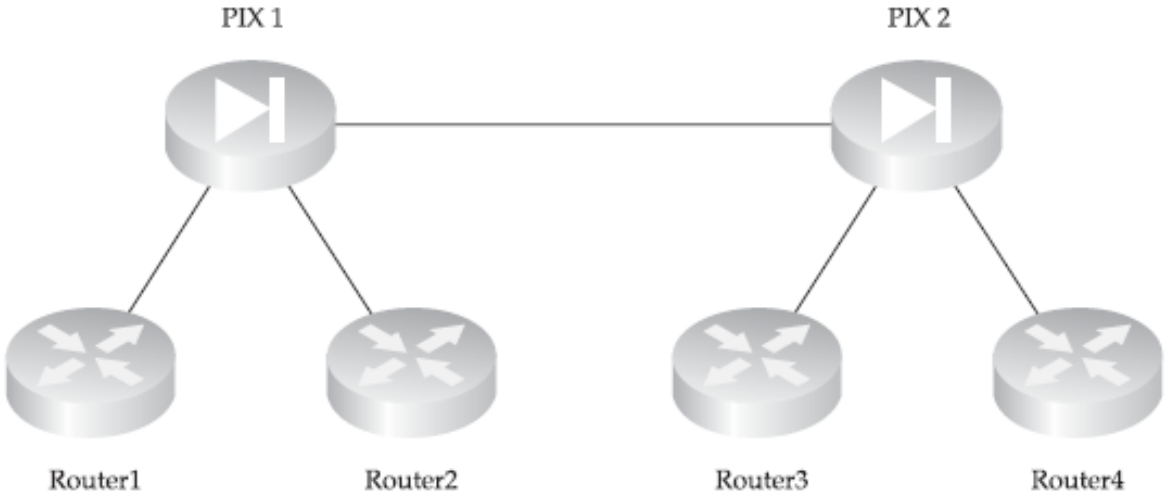

Рис.1.3. Дворівнева модель проектування

1.4. Модель «кільце»

Ця модель, показана на рис.1.4. гарантує, що кожен маршрутизатор має єдиний альтернативний маршрут.

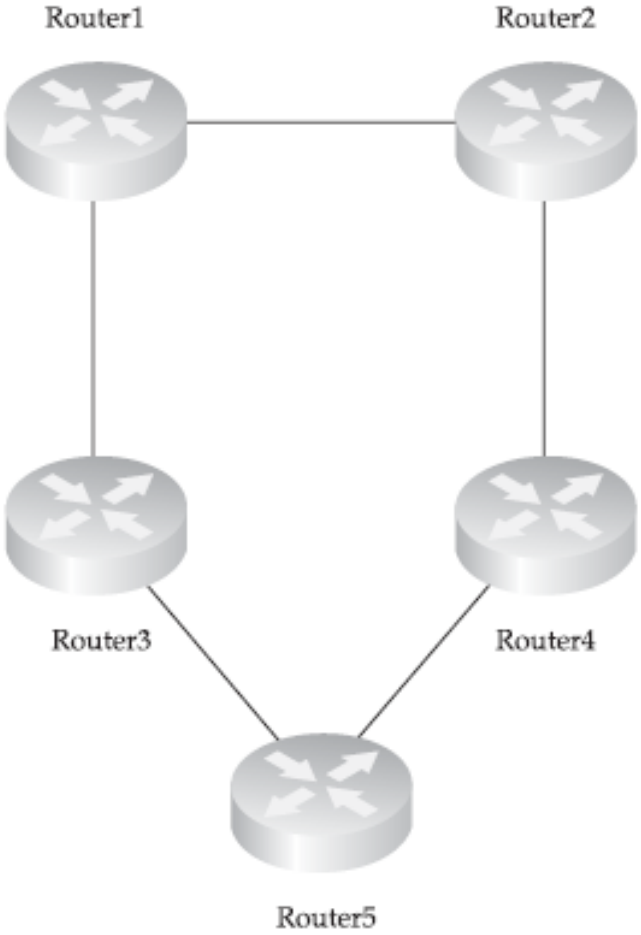

Рис.1.4. Модель «кільце»

Для ефективного використання моделі «кільце» необхідна динамічна маршрутизація. В середовищі Cisco, рекомендується використовувати розширений протокол маршрутизації внутрішніх шлюзів (EIGRP) з двох причин: цей протокол може використовувати метрики п'яти параметрів для визначення маршруту (гнучкість) та підтримує нерівні витрати на балансування навантаження (дисперсія) та обмін трафіку.

Необхідно переконатися, що протокол маршрутизації захищений від флеш-атак підроблених або шкідливих оновлень маршрутів, інакше модель «кільце» може розвалитися, як картковий будиночок.

Можна використовувати кільцеві маршрутизатори як розподілену систему виявлення вторгнень (IDS) з більш ніж одним центром управління IDS та централізованим центром, симетрично розташованим в моделі. При наявності коштів, можна розгорнути датчики серії Cisco IDS 4200 між кільцевими маршрутизаторами, але в більшості випадків можливостей IDS версій Cisco IOS з підтримкою фази II міжмережевого екрану має вистачити.

1.5. Модель «повна сітка» та «часткова сітка»

Модель «повна сітка» представлена на рис.1.5. З одного боку, велика кількість з'єднань ($N = (n\,(n-1)\,2)$, де n – число розгорнутих маршрутизаторів) забезпечує найвищу стійкість до DoS/DDoS атак у порівняння з іншими моделями в інфраструктурі організації. З іншого боку, нападник, якому вдається проникнути в мережу з мережевих маршрутизаторів із «повною сіткою» можуть легко вишукати всю мережу та мати декілька шляхів для вивчення вектору атаки. Таким чином, кожен окремий маршрутизатор у повномасштабній мережі є вразливим, з точки зору безпеки і повинні бути захищені так само добре, як і концентратор - маршрутизатор у моделі «зірка».

В свою чергу, це створює високі вимоги до обох мереж із процедурою управління безпекою та із використанням всіх загальних можливостей маршрутизаторів. Крім того, маршрутизація у великих мережах повинна бути

динамічною і досягати дуже високого, комплексного рівня. Те саме стосується і захисту від атак на різні протоколи маршрутизації.

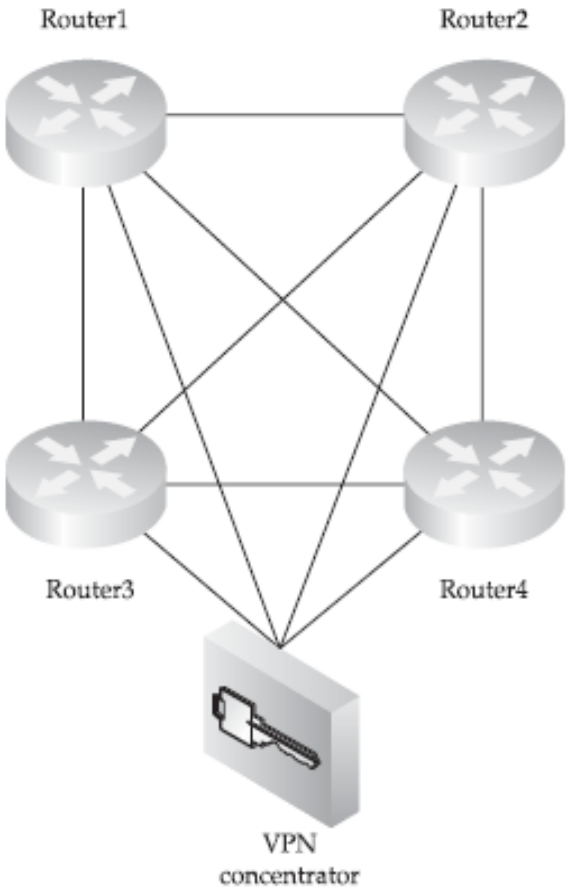

Рис.1.5. Модель «повна сітка»

Модель мережі з «частковою сіткою» (рис.1.6) – це спеціально розроблене рішення, яке поєднує в собі такі плюси, як надмірність, масштабованість та доступність, та мінуси - вартість посилань, складність загальної конфігурації та безпеки, управління та технічне обслуговування.

Універсальне правило маршрутизатора з найбільшою кількістю посилань, що вимагають найвищого рівня захисту та технічного обслуговування стосуються мереж із «частковою сіткою», а також будь-яких інших топологій проектування мережі. Мережі з «частковою сіткою» слідують нестандартним конструкціям щоб задовольнити конкретні корпоративні чи організаційні вимоги. Що стосується динамічної маршрутизації у великих мережах з «частковою сіткою», то є сенс використовувати її надійний протокол маршрутизації, що підтримує поділ мережі на різні області топології, значення та роль.

Безперечно, протокол Open Shortest Path First (OSPF) – це найкращий кандидат на таку роль, якщо не говориться про дуже великі багатодомні мережі з високими вимогами до політики маршрутизації, яка є типовим протоколом прикордонного шлюзу (BGP).

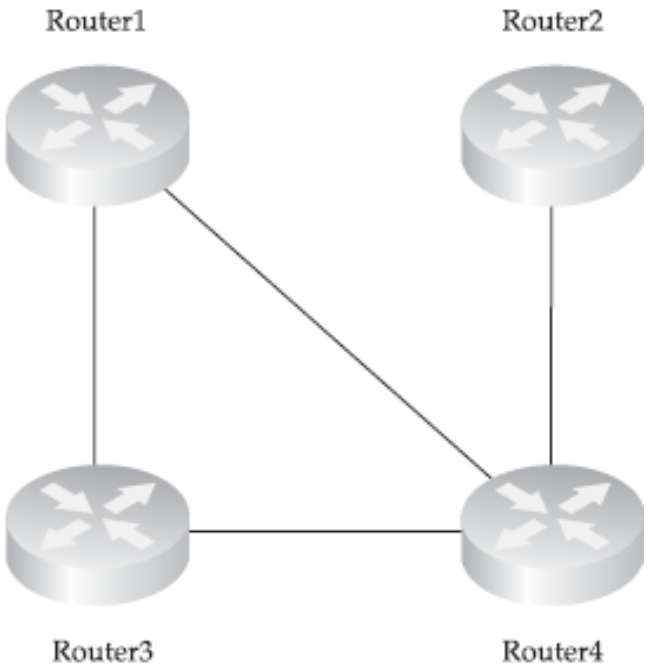

Рис.1.6. Модель «часткова сітка»

1.6. Аналіз особливостей побудови безпечних зон для інфраструктури підприємства

Якою б не була модель топології мережі, для забезпечення належної безпеки потрібно розділити мережу на зони з різним показником безпеки. Найчастіше мережа поділяється на три зони безпеки.

Найбезпечніша зона. Ця частина мережі зберігає найбільш конфіденційну інформацію, таку як Pretty Good Privacy (PGP) або ж приватні ключі. Доступ до цієї зони обмежений і жорстко контролюється. Окремо від використання спеціалізованого брандмауера, такого як Cisco PIX, для відділення цієї зони від решти мережі, рекомендується зашифрувати всі трафіки, що належать до найбільш безпечної зони використовуючи IPSec з надійними шифрами (наприклад, 256-розрядним розширеним стандартом шифрування [AES], або 128-розрядним кодом

автентифікації повідомлення з хешованим ключем [HMAC] SHA-1 або вище). Динамічні та часові списки доступу до маршрутизаторів можна використовувати для обмеження зовнішнього доступу до зони на основі користувачів у визначені проміжки часу.

Безпечна зона. У цій зоні розташовані внутрішні сервери та робочі станції. Повинен бути окремо підключений брандмауер, що зможе відокремити цю зону від інших. Таке розділення слід виконувати належним чином, включаючи блокування поширення пакетів протоколів маршрутизації (пасивні інтерфейси та списки розповсюдження, включені Cisco). Крім того, брандмауер має вимикати протокол розпізнавання адреси проксі (ARP) і не повинен поширювати інформацію рівня 2 (наприклад, протокол виявлення CDP та протокол STP) із захищеної зони.

Демілітаризована зона (DMZ). Сервери загального доступу розташовані на DMZ. Доступ до захищеної зони забезпечується через брандмауер і стежиться за векторами атак, що проходять до нього. Немає доступу до найбільш безпечної зони дозволено з DMZ.

DMZ – це зазвичай підмережа, розташована між загальнодоступною (Інтернет) та приватною мережами. DMZ створюються чотирма поширеними способами:

1) Триланковий брандмауер. Має мінімум три окремих інтерфейси, як PIX 515 і вище. На рис.1.7 представлено найпоширеніший із варіантів реалізації, при якому забезпечується гідний рівень контролю.

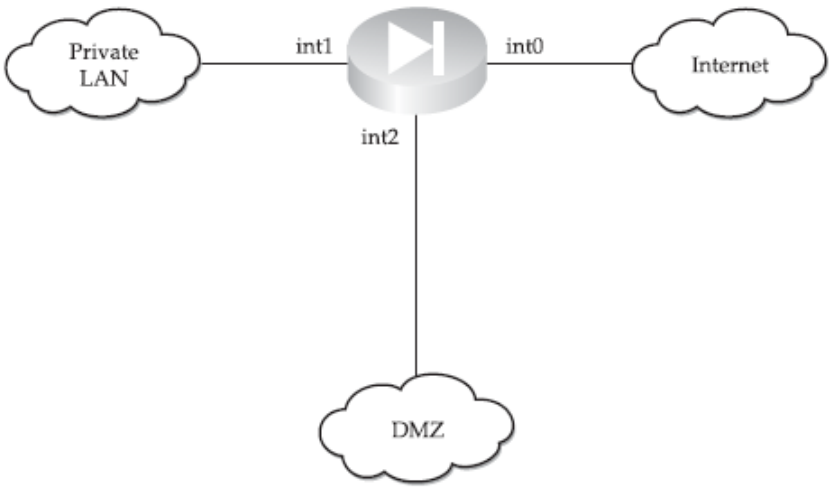

Рис.1.7. Триланковий брандмауер

2) Зовнішній брандмауер. Також можна розмістити за межами корпоративного брандмауера та підключити безпосередньо до загальнодоступної мережі, як показано на рис.1.8.. Така модель залежить повністю від безпеки серверів, розгорнутих у DMZ, і не рекомендується до широкого використання.

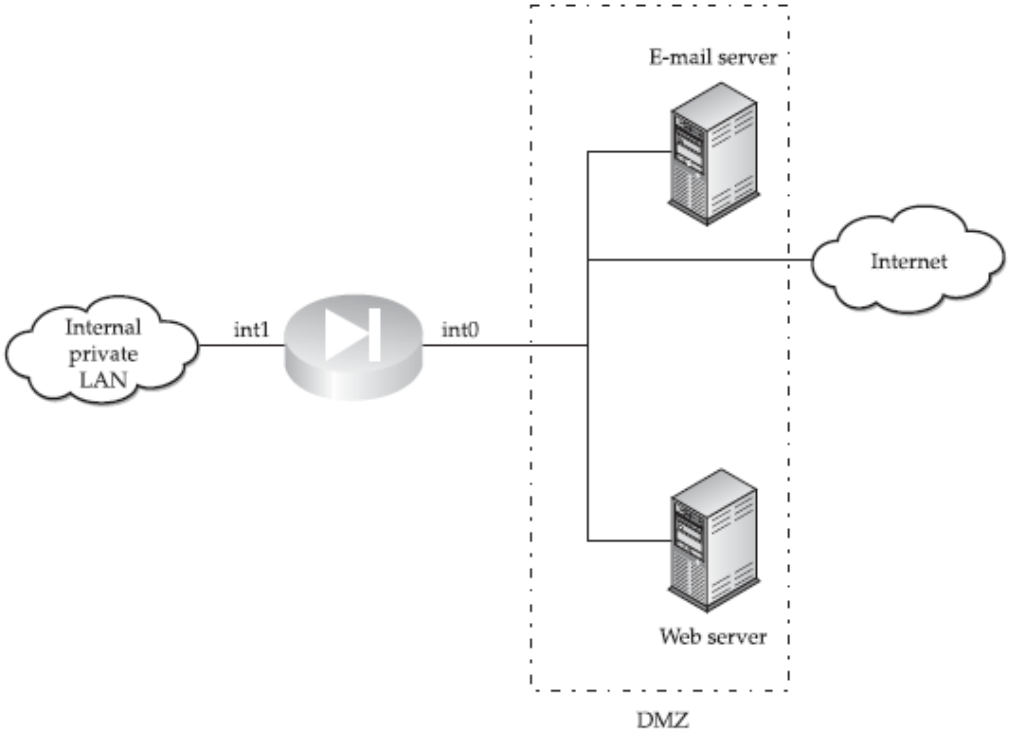

Рис.1.8. Зовнішній брандмауер

3) Dirty DMZ, або так звана «брудна» DMZ. Сервери загального доступу підключаються до одного з інтерфейсів корпоративного маршрутизатора, що позиціюється поза кордоном корпоративної мережі (рис.1.9).

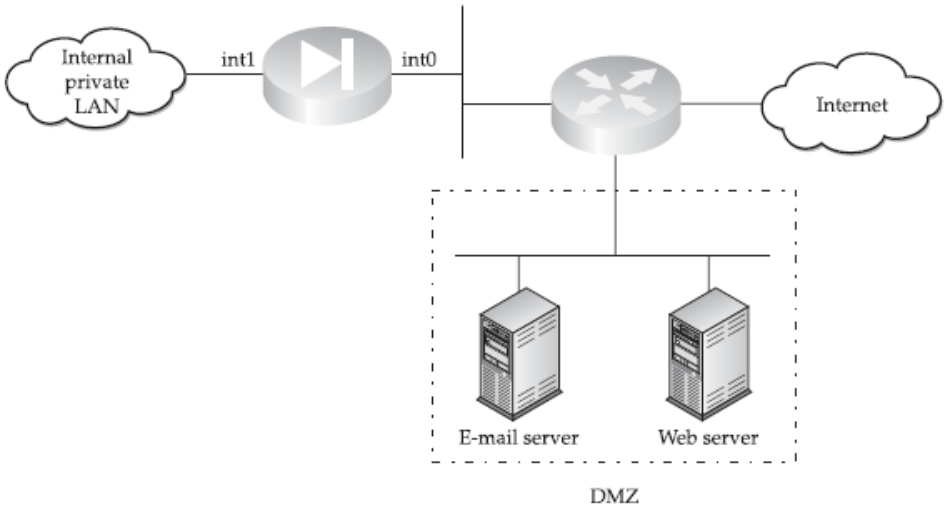

Рис.1.9. «Брудна» DMZ

«Брудна» DMZ часто встановлюється, коли брандмауеру бракує третього інтерфейсу або він не має можливості обробляти трафік навантаження між DMZ та загальнодоступною мережею. Це рішення більш безпечне, ніж зовнішнє DMZ. Проте насправді, багато що залежить від вибору маршрутизатора, який охоплює DMZ.

«Брудна» DMZ може стати достатньо безпечною, якщо маршрутизатор:

- Має достатню кількість оперативної пам’яті та процесора, щоб здійснювати безпечну обробку на основі програмного забезпечення;
- Має IOS з розширеними функціями безпеки;
- Має модулі, пов'язані з безпекою (наприклад, переобладнанням файлів або IDS) встановлені та належним чином налаштовані для роботи на апаратній основі, фільтрування або аналіз швидкісного підключення DMZ між збірними брандмауерами.

Нарешті, DMZ можна розташувати між двома брандмауерами, як показано на рис.1.10.

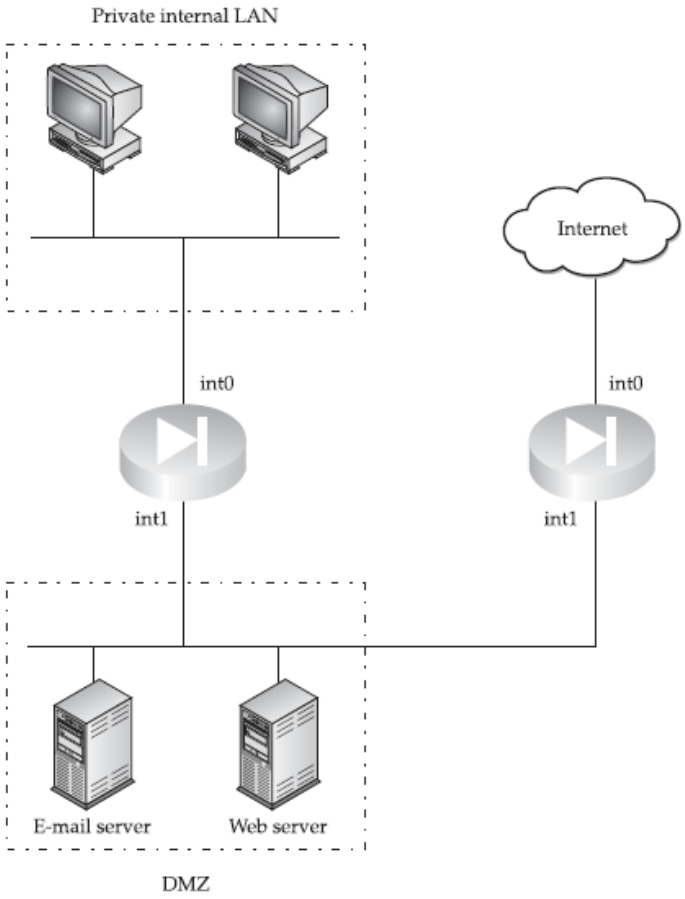

Рис.1.10. Двійний брандмауер DMZ

Ця реалізація є достатньо безпечною, але може коштувати дорого. Щоб зменшити витрати, можна розгорнути маршрутизатор з розширеними можливостями безпеки. Основною проблемою архітектури DMZ з двома брандмауерами є те, що трафік з захищеної приватної мережі повинен пройти менш безпечну DMZ, щоб досягти мережі. А скомпрометований хост може надати зловмисникам можливість змінити або викрасти сеанси, що проходять через DMZ. Щоб пом'якшити такі загрози, використовують приватні VLAN або навіть VPN.

Іншою важливою частиною архітектури безпеки мережі є правильне розгортання датчиків виявлення вторгнень та консолей управління. Можна виокремити декілька загальних вказівок щодо розміщення компонентів IDS в захищеній мережі [4]:

• Датчики повинні бути розподілені по всіх мережевих рівнях для забезпечення повного охоплення всієї IT-інфраструктури організації.

• Пропускна здатність датчиків ніколи не повинна перевищувати певний, узгоджений показник, і питання її масштабованості слід завжди враховувати. Кілька датчиків можна вимкнути при наростальних вимогах до пропускної здатності.

• Консоль управління має бути встановлена на захищеній платформі та розміщена в найбезпечнішій зоні.

• Весь трафік між датчиками та консолями управління має бути зашифрований і автентифікований. Це включає як сигналізацію про події, так і управління датчиком трафіку.

• Допускається розгортання одного датчика для VLAN.

• Більше однієї консолі управління слід розгорнути для резервування. Один датчик може надсилати тривожні повідомлення більш ніж на одну консоль.

• Датчики Cisco Secure IDS можуть бути налаштовані для управління функціями блокування трафіку на брандмауерах PIX. У цьому випадку датчик повинен бути розташований близько до брандмауера PIX, з яким він комунікує.

1.7. Аналіз особливості побудови ієрархічного дизайну для інфраструктури підприємства

Ієрархічний дизайн для інфраструктури підприємства, який також називають підходом до багаторівневого проектування інфраструктури мережі, активно впроваджується компанією Cisco як правильний спосіб створення ефективної та економічної мережі.

Cisco визначає три рівні мережевої ієрархії за допомогою чого можна легко розділити функціонал між ними:

- Основний рівень - це магістраль мережі, що забезпечує високу відмовостійкість та обробляє великі обсяги трафіку з мінімальною можливою затримкою.
- Рівень розповсюдження знаходиться між магістральною та локальною мережами кінцевого користувача і вважається частиною мережі, де функціонує контроль, у т.ч відбувається фільтрація пакетів, чергування та перерозподіл маршрутів.
- Рівень доступу включає робочі станції користувача, сервери, комутатори та доступ точки, що їх з'єднують, а також сервери набору номера та концентратори VPN для віддаленого доступу користувачів.

Масштабованість, простота усунення несправностей, простота оновлення, керованість, надійність та продуктивність згадуються як переваги ієрархічного проектування інфраструктури підприємства.

Однак існує кілька популярних питань, що стосуються ієрархічного дизайну Cisco, що мають пряме відношення до безпеки мережі, та включають:

- Захист належить до рівня розповсюдження і визначається лише там.
- Фільтрація MAC та VLAN є основними (або єдиними) засобами захисту, на яких слід розгортати рівень доступу.
- Заходи безпеки Cisco стосуються маршрутизаторів, комутаторів, концентраторів VPN, та брандмауерів.

1. Основний рівень. Даний рівень дає можливість повного адміністративного контролю на високошвидкісних магістральних маршрутизаторах або комутаторах, тому і вимоги до нього жорсткі. Адже, як тільки доступ отримають зловмисники, то одразу з’явиться вразливість для несанкціонованих втручань – соціальна інженерія, маніпуляції, переспрямування пакетів на недостовірні джерела, атаки DoS/DDoS.

Таким чином, магістральна безпека аж ніяк не обмежується проблемами надмірності, а головним завданням безпеки на основному рівні є забезпечення всіх форм доступу до маршрутизаторів цього рівня, а комутатори настільки обмежені, наскільки це можливо.

Інше дуже важливе завдання - це нагляд за безпечним впровадженням протоколу BGP, що використовується на магістралі, і будь-яке втручання у нормальну роботу даного протоколу - навмисне чи ні – призводить до появи збоїв у взаємопов'язаних мережах тощо. Для запобігання атак на BGP, необхідно впровадити наступні засоби безпеки: датчики IDS, брандмауери, VPN модулі.

Кілька пристроїв і модулів безпеки мережі які зараз актуальні у компанії Cisco, здатні виконувати функції щодо збереження терабітних та гігабітних шкидкостей на маршрутах, на яких вони розгорнуті.

До таких пристроїв належать: детектори аномалій трафіку Cisco XT 5600 та 5700, Cisco Guard XT 5650, брандмауер Cisco PIX 535, модуль послуг брандмауера Cisco (FWSM) для маршрутизаторів Cisco 7600 та Catalyst 6500, модуль системних служб виявлення вторгнень Cisco Catalyst серії 6500 (IDSM-2), датчик Cisco IDS 4250-XL, модуль послуг Cisco 7600/Catalyst 6500 IPSec VPN (VPNSM).

Немає технічних причин, чому підприємства не повинні використовувати ці потужні запобіжні заходи для імплементації в свою інфраструктуру для забезпечення безпечного доступу до рівня провайдера, наприклад. Фактично, детектори аномалій Cisco Traffi c XT 5600 та 5700, а також Cisco Guard XT 5650 були спеціально розроблені для розгортання на магістралі мережі виявляти та обробляти масивні DDoS -атаки.

2. Рівень розподілу. Це частина мережі, де трафік розподіляється між локальними мережами (кінцеві користувачі) або окремими станціями та магістральною мережею. Всі філіали підприємства, малий та середній бізнес, а також організаційні підрозділи будуть із впровадженням принципів рівня розподілу.

Типове розгортання мережевих пристроїв Cisco на рівні розподілу включають комутатори Catalyst, маршрутизатори серій Cisco 3600 та 3700 або Catalyst 5000. Рівень розподілу - це місце розгортання ще і для концентраторів VPN Cisco 3000 та датчиків Cisco IDS 4200.

На рівні розподілу необхідно виконання таких функцій:

- Централізоване ведення та зберігання журналів реєстрацій з різних джерел, включаючи доступ багаторівневих локальних мереж, в деяких випадках і магістральних каналів;
- Фільтрація маршрутів через списки розсилки, пасивних інтерфейсів та політики безпеки маршрутизації;
- Централізована політика безпеки та управління пристроями.

Для забезпечення централізованої політики безпеки та управління пристроями компанія Cisco розробила різноманітні продукти, включаючи вдосконалення популярного управління CiscoWorks Центр, наприклад CiscoWorks VPN/рішення для управління безпекою, CiscoWorks Security.

3. Рівень доступу. Фактично це рівень, в якому кінцеві користувачі отримують підключення до мережі. Отже, основною складовою безпеки рівня доступу є автентифікація, авторизація та облік (AAA), представлені RADIUS/TACACS+ Cisco Secure Access.

Керування серверами та агентами Cisco Secure/Cisco Trust Authentication відбувається і на стороні користувачів. Технологія Cisco IBNS є відносно новою, але дуже важливий гравець у ній саме AAA, адже використовується стандарт контролю доступу до мережі 802.1x.

Звичайно, захист рівня доступу також включає захист настільних комп'ютерів та ноутбуків кінцевих користувачів, а також сервери локальних мереж.

Cisco Security Agent (CSA)-це система запобігання вторгненням на базі хоста, яка працює за допомогою застосування політики безпеки до поведінки системи за допомогою перехоплення та аналізу системних викликів.

Модель мережі CSA складається з трьох компонентів:

• Центр управління агентами безпеки Cisco (CSAMC). CSAMC дозволяє централізоване віддалене управління декількома CSA, що включає поділ захищених хостів на групи з різними вимогами політики безпеки, а також ведення журналів порушень безпеки та надсилання сповіщень через служби повідомлень або електронну пошту.

• Робоче місце адміністрації. Робоча станція підключається до CSAMC за допомогою рівня Secure Sockets Layer (SSL) – захищеного веб-інтерфейсу.

• Програмне забезпечення CSA, встановлене на захищених хостах. CSA доступний для Windows, Linux та Solaris та складається з чотирьох модулів перехоплювачів. Перехоплювач файлової системи перевіряє всі файли зчитування та записує запити проти визначеної політики безпеки, керує модулем мережевого перехоплювача, а також може обмежити кількість з'єднань фільтруючи їх на основі IP портів. Перехоплювач перевіряє запити на читання/запис до реєстру Windows або сценаріїв ініціалізації UNIX. Нарешті, перехоплювач підтримує цілісність динаміки кожної програми в середовищі виконання. Запити на запис у пам'ять, що не належать процесу запиту за замовчуванням виявляється та блокується. Переповнення буфера класичного стека також являється атакою та спробою введення спільних або динамічних бібліотек посилань (DLL), тому і блокується. Таким чином, цілісність пам'яті та адресація мережевого вводу -виводу захищена [5].

При виявленні підозрілого системного виклику CSA може виконати наступні дії:

• Заблокувати дзвінок;

• Передате програмі ініціювання виклику повідомлення про помилку;

• Сформувати повідомлення -попередження, яке буде надіслано до CSAMC.

За характером своєї роботи CSA-це система запобігання вторгненням на базі хоста і не залежить від бази даних підписів атаки та її оновлень.

Висновки до першого розділу

Проаналізовано широкий спектр рішень від Cisco, що здатні захистити інфраструктуру підприємства на будь-якому ієрархічному рівні незалежно від топології мережі.

Досліджено декілька моделей безпеки, а також виокремлено головні переваги та недоліки кожної. Зазначено, що безпеку мережі слід розглядати та розвивати з першого етапу – з етапу проектування, адже топології та моделі проектування мережі, запропоновані компанією Cisco, мають унікальну безпеку, відповідні особливості, які слід враховувати при розробці політики безпеки, розгортання та захисту мережі.

Підкреслено, що для зловмисників, які зосереджені на більш хаотично спроектованих мережах, побудовані з використанням обладнання Cisco мережі більш складні в керувані, однак відповідають всім необхідним вимогам щодо контролювання, оновлення та вирішування проблем.

2 ДОСЛІДЖЕННЯ ЗАГАЛЬНИХ ФУНКЦІЙ БЕЗПЕКИ МЕРЕЖЕВИХ ПРИСТРОЇВ CISCO ТА ВИОКРЕМЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ВИБОРУ IOS ДЛЯ ПОТРЕБ БЕЗПЕКИ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Коли йде мова про елементи безпеки інфраструктури підприємства з використанням обладнання Cisco, зазвичай розглядається питання впровадження брандмауерів PIX, концентраторів віртуальної приватної мережі (VPN) та систем виявлення вторгнень (IDS). Однак кожен окремо обраний маршрутизатор і комутатор Cisco має безліч корисних функцій безпеки, які здатні протидіяти несанкціонованим втручанням.

У багатьох випадках, коли ці функції належним чином налаштовані, можуть запропонувати достатній рівень захисту для мережі без необхідності купувати дорогі спеціалізовані засоби безпеки. Тому необхідно розглянути загальні функції безпеки мережевих пристроїв Cisco та описати рекомендації щодо вибору версій IOS та CatOS для мережі і з врахуванням потреб безпеки.

2.1. Загальні рекомендації щодо вибору версій IOS та CatOS для мереж

Очікується, що будь-який маршрутизатор Cisco підтримуватиме засоби безпеки,наприклад такі:

- Підтримка автентифікації, авторизації та обліку (AAA);
- Стандартні, розширені, динамічні списки доступу, що базуються на часі та відновлені;
- Пасивні порти та списки розсилки маршрутів;
- Автентифікація маршрутів;
- Шифрування паролей;
- Локальна реєстрація подій у буфері нестандартного розміру;

- Віддалена реєстрація подій через системний журнал та пастки протоколу SNMP;
- Зворотній зв'язок для користувачів, які віддалено підключаються до маршрутизатору;
- Функціонування протоколу ARP;
- Аутентифікація мережевого протоколу часу (NTP).

Усі комутатори Cisco Catalyst підтримують наступне:

- Фільтрування адреси контролю доступу до медіа (MAC) та статичні MAC;
- Правильна статична та динамічна сегментація віртуальної локальної мережі (VLAN);
- Безпечний доступ до протоколу STP (Cisco RootGuard і BPDUGuard);
- Локальна та віддалена реєстрація подій за допомогою системного журналу та пасток SNMP;
- Обмежений адміністративний доступ до комутатора на основі вихідної IP;
- Шифрування паролем;
- Аутентифікація NTP.

Все, що виходить за межі перерахованих функцій, можна реалізувати за допомогою функцій додаткової безпеки у специфічних версіях IOS, додавання модулів безпеки до модульних маршрутизаторів або комутаторів, або використанням засобів безпеки, таких як брандмауери PIX, замість звичайних маршрутизаторів.

Перше, на що необхідно звернути увагу при виборі коду для маршрутизатора, це правильний випуск IOS [6].

Два основні типи випусків коду - це основні випуски та випуски раннього розгортання (ED). Основні випуски IOS надійні та стабільні, але вони не приймаються додавання найновіших функцій та підтримуваних платформ. Функції, якими користувачі ніколи не користуються, можуть бути використанні

зловмисниками, щоб викорінити або завершити роботу в мережі, і чим більше розгалуджений код, тим більша ймовірність того, що помилки безпеки там наявні.

З іншого боку, випуски ED можуть запровадити нові функції безпеки, наприклад, підтримка 802.1x для автентифікації користувача. Це залежить від користувачів, яку лінію випуску IOS вони будуть використовувати, залежно від того, чи мають всі поточні випуски всі передбачені ними засоби безпеки та функції, а також підтримку необхідних протоколів.

Випуски ED поділяються на чотири категорії: випуски консолідованої технології раннього розгортання (CTED), випуски специфічних технологій раннього розгортання (STED), специфічні випуски для раннього розгортання на ринку (SMED) подібні до випусків STED, але вони націлені на певні сегменти ринку - наприклад, на Інтернет –послуги та постачальників послуг (ISP), короткочасні випуски раннього розгортання, також відомі як випуски X (XED).

Приклади SMED включають Cisco IOS 12.0S та 12.1E, а XED не надають версії технічного обслуговування програмного забезпечення або звичайного програмного забезпечення із проміжними правками. Якщо помилка виявлена в XED до її зближення з CTED, ініціюється відновлення програмного забезпечення, а номер додається до «назви IOS». Наприклад, Cisco IOS 12.0 (2) XB1 та 12.0 (2) XB2 є прикладами 12.0 (2).

2.2. Дослідження особливостей функціонування брандмауерів в інфраструктурі підприємства

Один з найпотужніших інструментів в арсеналі мережевого адміністратора, який допомагає захистими IT-інфраструктуру підприємства чи організації - це система брандмауерів. Технологія брандмауера була розроблена ще на перших етапах сучасного Інтернету, коли усвідомлювалася зростаюча потреба в безпеці.

Перші брандмауери аналізували передачу трафіку та приймали рішення на основі вихідних та цільових адрес, зазначених в пакетах даних. З того часу, брандмауери пройшли трансформацію, і сьогодні можна класифікувати їх як:

брандмауери для фільтрації пакетів, брандмауери для фільтрації пакетів із підтримкою стану, брандмауери на основі проксі-фільтрів.

1. Брандмауери для фільтрації пакетів – аналізують мережевий трафік на транспортному рівні, співставляючи заголовки пакетів із заздалегідь визначеним набором правил. Брандмауери фільтрації пакетів представлені простими та розширеними списками контролю доступу IOS (ACL). Хоча стандартні списки керування доступом Cisco базуються на вихідному або цільовому IP, розширені ACL перевіряють такі поля заголовків пакетів, як: IP-адреса джерела, IP-адреса призначення, використання мережевих протоколів, джерела протоколу TCP/UDP та/або протоколу ICMP та призначення TCP/UDP або тип повідомлення ICMP.

Крім того, базовий аналіз TCP можна проводити за допомогою «встановленого» ACL параметр, який обмежує трафік TCP в одному напрямку, пропускаючи пакети лише в тому випадку, якщо встановлено фланги ACK або RST. Таким чином, пакети SYN будуть скинуті та ініціювання зовнішніх зв'язків TCP стають неможливими. Встановлений варіант у розширених списках керування доступом Cisco не слід плутати з фільтрацією пакетів у стані; крім того, зловмисник може легко обійти захист, пропонований цією опцією, шляхом сполучення TCP - флангів.

Найпоширеніша дія, яку можуть виконувати ACL-адреси Cisco - це прийняти, відхилити або переслати пакет. При необхідності внесені дії можуть реєструватися локально або віддалено. Динамічні списки ACL дозволяють реєструвати додаткові записи ACL після автентифікації користувача в маршрутизаторі, таким чином дозволяючи фільтрувати користувачів, а не IP і порт.

Автентифікація може працювати проти локальної БД облікових даних користувача або пароля або за допомогою RADIUS або серверу системи контролю доступу до терміналу доступу (TACACS+). Хоча це може звучати як чудова та гнучка функція, необхідно подбати про те, щоб автентифікація користувача здійснювалася за допомогою захищеного протоколу, такого як SSHv2. Як правило, доступ до Telnet маршрутизатора з будь–якого зовнішнього джерела повинен бути суворо заборонений.

Ще одне вдосконалення, доступне для стандартних та розширених ACL Cisco, це часове ACL. Часові списки керування доступом підтримуються на всіх платформах Cisco IOS і дозволяють вносити зміни для доступу до мережі залежно від часу доби, дня тижня або того і іншого.

Негативні сторони використання простого переналаштування фільтрації пакетів на основі ACL: несанкціоновані пакети можуть проходити через ACL за певних умов; фрагментовані пакети також можуть проходити через брандмауер за певних умов; здійснювати управління великими наборами ACL на кількох маршрутизаторах досить складно; підтримка динамічних/багатопортових протоколів, таких як H.323 або FTP досить неконструктивна.

При цьому, всі версії IOS як для маршрутизаторів Cisco, так і для модулів комутатора (RSM) підтримують фільтрацію пакетів, і ця підтримка може бути дуже корисною в певних випадках. Прикладом такого випадку є обмеження адміністративного доступу до маршрутизатор або переключитися на визначений набір внутрішніх IP-адрес. Проте пропонується використання рефлексних списків доступу та оновлення IOS до версій, що підтримують CBAC де це можливо.

2. Брандмауери для фільтрації пакетів із підтримкою стану. Брандмауер із можливістю перевірки пакетів із станом створює таблицю з інформацією про стан кожного встановленого підключення. Зазвичай така таблиця містить інформацію про наступне:

- IP -адреса джерела та призначення,
- Мережевий протокол,
- Джерело TCP/UDP та порт призначення,
- Інформація про послідовність TCP,
- Додаткові флаги для з'єднань TCP/UDP.

Як тільки встановлене успішне з'єднання, ініціоване через брандмауер, з'являється відповідний об’єкт. Всі наступні пакети порівнюються із значенням цього об'єкту, що зберігається у таблиці станів, і якщо брандмауер бачить співпадіння цього пакету, то він розглядається як частина актуального з'єднання. З

іншого боку, якщо фіксується відміність, то брандмауер передає його для подальшої перевірки на ACL (поводиться як стандартний пакетний фільтр).

До мінусів фільтрування пакетів із станом можна віднести наступне: низька продуктивність у порівнянні з простими пакетними фільтрами; підвищені вимоги до обчислювальної потужності та пам'яті маршрутизатора; погана підтримка динамічних/багатопортових протоколів.

Усі брандмауери підтримують перевірку пакетів у стані, використовуючи проксі послуги для обробки динамічних протоколів. Послідовність коду, що підтримує CBAC, що мають ідентифікатори також знають про стан і здатні проходити аналіз вищого рівня динамічний протокол трафіку.

Переглядаючи наявні списки доступу, які підтримуються усіма версіями IOS переобладнання фіксації стану; проте механізми фільтрації динамічних протоколів повністю відсутні, і доведеться обійти цю проблему збоку (наприклад, за допомогою тільки пасивний FTP). Це може змусити користувачів використовувати просту фільтрацію пакетів замість зворотніх списків або оновлень IOS, включивши підтримку CBAC.

3. Брандмауери на основі проксі-фільтрів. Перевіряють пакети на рівні додатка. З'єднання спочатку встановлюється від клієнта до пристрою фільтрації файлів, а потім сам пристрій встановлює інше з'єднання з пунктом призначення.

Часто від користувача вимагається пройти автентифікацію на брандмауері та застосовується набір ACL. Існує тип брандмауера на основі проксі–фільтра, який не вимагає від ініціюючого клієнта мати специфічну підтримку вимог проксі. Натомість брандмауер відкрито перехоплює сеанс і створює два унікальні сесії. Завдяки здатності приймати розумні рішення на основі корисного навантаження пакета, такі брандмауери можуть виконувати функцію перетворення. Наприклад, видалення шкідливого вмісту ActiveX або Java та фільтрувати заборонену інформацію порнографічного характеру або політичного характеру, як це можна зробити перезавантаженням Cisco PIX разом із програмним забезпеченням для фільтрації вмісту, наприклад WebSense.

До мінусів таких брандмауерів можна віднести наступне:

• Найнижча продуктивність у порівнянні з іншими типами брандмауерів;

• Найвищі вимоги до обладнання;

• Складність розробки та підтримки протоколу-проксі;

• Обмежена доступність підтримуваних протоколів;

• Висока вартість;

• Можливість самого проксі бути вразливим до атак прикладного рівня.

2.3. Типи обладнання брандмауера Cisco

Сімейство пристроїв Cisco PIX варіюється від компактних настільних мережевих перезавантажувачів для невеликих офісних/домашніх офісів (SOHO)-наприклад, PIX 501-до модульних гігабітних пристроїв класу оператора для великих корпорацій та середовища Інтернет-провайдера (табл.2.1).

Таблиця 2.1.

Брандмауери Cisco PIX

Модель Cisco PIX	501	506	506E	515	515E	520	525	535
Мак швидкість(Мбіт/с)	60	10	100	120	188	370	330	1024
Макс кіл-сть одночасних сесій				125000		250000	280000	500000
Макс інтерфейси				6		6	8	10
Відновлення після відмови	Ні	Ні	Ні	Так	Так	Так	Так	Так

Середовище використання	SOHO		Маленькі відділення		Середні відділення		Великі відділення	Головні/корпоративні відділення

Вибираючи маршрутизатори з набором функцій брандмауера IOS, необхідно дотримуватися загальних правил Cisco щодо розгортання для різних розмірів мережі.

Наприклад, маршрутизатори SOHO 90 рекомендуються для малого бізнесу, а Cisco Серії 1700 призначені для маленьких відділень. Cisco 2600-2800 – для середніх, а Cisco 3700 – для великих корпоративних мереж. Маршрутизатори Cisco 7000 можуть бути розгорнуті на території великого підприємства, або, наприклад, SOC/ЦОД. Продуктивність брандмауера IOS CBAC для маршрутизаторів сягає від 10-2000Мбіт/с [7].

Ще один пристрій Cisco, який слід розглянути для розгортання - Cisco Guard XT 5650. Cisco Guard XT 5650 - це пристрій, який здатен зменшити вплив DDoS, для великих підприємств або державних організацій, для яких доступ до мережі Інтернет є критично важливим.

XT 5650 має два інтерфейси Gigabit Ethernet для обробки гігабітного трафіку, а для підтримки багатогігабітних трафіків можна розгорнути кілька пристроїв XT 5650. Cisco Guard XT 5650 був розроблений для роботи разом з Cisco Traffic детектор аномалій XT 5600. Коли виявляється DDoS -атака, Cisco Guard XT 5650 перенаправляє трафік шкідливих програм для перевірки та відокремлює «зловмисні» потоки. Пакети ідентифіковані як шкідливі, видаляються, а нормальний, достовірний трафік пересилається до місця призначення. Таким чином, не відбувається порушення доступності послуг.

Cisco Guard XT 5650 створений на базі Linux та підтримує Juniper. Тому здатен не лише керувати перенаправленням трафіку, а також пересилати без спотворення та створення циклів маршрутизації, включати функціонування

протоколу BGP, не заважати виконанню політики маршрутизації, тунелюванню та переадресації маршрутів VPN.

Перелічене обладнання підтримує детальне локальне та централізоване ведення журналу подій, коли параметр журналу додано до списків керування доступом. Однак ACL не можуть відображають усі можливі атаки на мережу, оскільки їх робота, як правило, обмежена рівнями OSI. Брандмауери PIX також можна використовувати як датчики IDS інтегрований в інфраструктуру підприємства із використанням Cisco Secure IDS.

2.4. Дослідження особливостей впровадження безпечних ідентифікаторів Cisco для профілактики несанкціонованим втручанням

Cisco IDS призначені для захисту периметра мережі та внутрішньої IT – інфраструктури. Зі збільшенням витонченості атак, досягнення ефективного виявлення та блокування вторгнень у мережі має вирішальне значення. Поєднуючи складність методології, Cisco стверджує, що забезпечує безперервність функціонування бізнесу та мінімізує вплив шкідливих атак та несанкціонованих втручань, використовуючи багаторівневий підхід до виявлення та запобігання вторгненням для забезпечення наявності наступних елементів: точне виявлення атаки, інтелектуальне розслідування нападу, простота управління безпекою, гнучкі варіанти розгортання для всіх моделей та топологій проектування мережі.

Для досягнення цих елементів Cisco впровадив лінійку IDS, які можна інтегрувати в поточні мережеві маршрутизатори та комутатори, розгорнуті як окремі пристрої IDS, або запускати як програмні програми на робочих станціях управління.

Cisco IDS складається з двох основних компонентів: датчика IDS та консолі управління. Поки датчик слідкує та аналізує трафік, консоль управління надає інтерфейси для моніторингу сигналізації та конфігурації розподілених датчиків.

Датчики бувають двох видів: ті, що здійснюють пасивний моніторинг трафіку (автономні прилади) та ті, що аналізують трафік, що проходить через

пристрій (програмне забезпечення IOS IDS і PIX). Пристрої пасивного пошуку не нав'язують жодних штрафних санкцій продуктивності мережі. Навпаки, вбудована обробка обходу трафіку може перевантажити учасників маршрутизації або прошивки PIX. Якщо пропускна здатність вбудованого пристрою моніторингу нижче пропускної здатності мережі, маршрутизатор або PIX можуть зависати.

2.4.1. Автономні апаратні датчики IDS

Автономний датчик Cisco IDS 4215/4235/4250/4250-XL, що монтується в стійку, забезпечує повний захист від несанкціонованих, підозрілих або відверто зловмисних втручань в інфтраструктуру підприємства. Цей спеціально побудований, високопродуктивний засоб мережевої безпеки може аналізувати трафік у режимі реального часу до 1000 Мбіт/с (Cisco 4250 XL), повідомляючи керівництву консолі про аномалії.

Датчики Cisco IDS підтримують обидва процеси - виявлення аномалій та виявлення атак на основі підписів. База даних підписів Cisco постійно оновлюється.

Датчик Cisco IDS 4215 контролює пропускну здатність до 80 Мбіт/с і підходить для моніторингу кількох каналів WAN. Можливе розміщення до п’яти інтерфейсів датчика IDS 4215 для одночасного спостереження за декількома підмережами.

Це стосується всіх моделей датчиків більш високого класу, крім Cisco IDS 4250-XL. Cisco IDS 4235 може обробляти 250 Мбіт/с трафіку і є відповідним для моніторингу комутованих середовищ на додаток до захисту декількох WAN. Cisco IDS 4250 підтримує швидкість 500 Мбіт/с і може бути розгорнутий на основному рівні мережі підприємства. Його також можна налаштувати для масштабування до повної гігабітної лінії з високою продуктивністю при необхідності, проте, Cisco IDS 4250-XL рекомендується для розгортання на повністю завантаженій гігабітній лінії [8].

Що стосується ОС, серія Cisco IDS 4200 базується на Solaris. Функціонал IDS датчика такий реалізовано як сукупність службових процесів, що включає:

- fileXferd. Службовий процес, який отримує файли конфігурації від керівництва консолі;
- loggerd. Створення службового log файл;
- managed. Службовий процес здатний надсилати команду відхилення на інший пристрій Cisco, такий як брандмауер PIX, для автоматичного блокування атак;
- packetd. Фактичний інтерфейс збору та аналізу пакетів;
- postofficed. Службовий процес керування комунікаціями.

Ці службові процеси та їх конфігурації, бібліотеки, журнали та тимчасові файли, а також утиліти конфігурації знаходяться в каталозі /usr /nr, який має таку структуру:

/usr/nr/bin /usr/nr/etc

/usr/nr/bin/eventd /usr/nr/etc/.lt

/usr/nr/bin/eventd/skel /usr/nr/etc/backups

/usr/nr/bin/sap /usr/nr/etc/licenses

/usr/nr/bin/sap/skel /usr/nr/etc/nrConfigure

/usr/nr/bin/sap/sql /usr/nr/etc/oem

/usr/nr/bin/sap/sql/skel /usr/nr/etc/oem/templates

/usr/nr/etc/wgc

/usr/nr/etc/wgc/templates

/usr/nr/lib /usr/nr/var

/usr/nr/skel /usr/nr/var/dump

/usr/nr/tmp /usr/nr/var/iplog

/usr/nr/tmp/queues /usr/nr/var/new

/usr/nr/var/tmp

Коли датчик Cisco 4200 IDS виявляє атаку, можна виконати наступне:

• No action

• Shun

• Log

• Shun + log

• TCP connection reset

• TCP connection reset + shun

• TCP connection reset + log

• TCP connection reset + shun + log

Shun (shunning) – ухилення - відноситься до повного блокування будь-якого трафіку від порушника або підмережі. Журнал (журналювання) відноситься як до тривог подій атаки, так і до всього підозрілого журналу IP–сеансу. Усі типи журналів можна надсилати або на консоль управління Cisco IDS, або на традиційний системний журнал UNIX. Через можливе з'єднання функцій відкидання і ухилення, датчик Cisco IDS 4200 більше, ніж просто датчик IDS у традиційному значенні терміну. Це ціла система запобігання вторгненням (IPS).

2.4.2. Модульні датчики IDS

Модуль Cisco IDS доступний для маршрутизаторів серій 2600, 3600 та 3700 (NM-CIDS-K9, лише один модуль на маршрутизатор), а також для комутаторів серії Catalyst 6500 (IDSM-2, WSSVC-IDS2-BUN-K9, якщо придбано як частину системи Catalyst, WS-SVC-IDS2BUNK9, якщо купується окремо як запасний).

Для підтримки NM-CIDS-K9 потрібно мінімальне програмне забезпечення Cisco IOS випуск 12.2 (15) ZJ, тоді як CatOS 7.6 (1) є мінімальною вимогою для підтримка IDSM-2.

Цей функціонал є частиною вбудованого датчика сімейства Cisco IDS та системою захисту від вторгнень Cisco. Датчики Cisco IDS працюють узгоджено з іншими компонентами IDS, встановленими по всій корпоративній мережі, в тому числі консолі управління Cisco IDS, CiscoWorks VPN/Рішення для управління безпекою та Cisco IDS Device Manager для ефективного захисту даних та підтримки інформаційної інфраструктури.

Дуже важливо оцінити, яку пропускну здатність може здійснити IDS. Якщо пропускна спроможність мережі вища, ніж може обробляти модуль IDS, то значний відсоток трафіку пройде без аналізу виявлення вторгнень на ньому.

NM-CIDS-K9 підтримує швидкість до 10 Мбіт/с в Cisco 2600XM, а також до 45 Мбіт/с в серії Cisco 3700, а модуль Cisco Catalyst IDS (IDSM-2) підтримує пропускну здатність 600 Мбіт/с. Таким чином, функціонал Cisco 2600 та 3700 IDS підходять для захисту декількох посилань WAN, тоді як IDSM-2 можна розмістити в будь-якому місці мережі,навіть на основному рівні. Кілька IDSM можна розмістити в обладнані Catalyst 6500 з можливістю масштабувати пропускну здатність понад 600 Мбіт/с.

Оскільки зберігання виявлених подій здійснюється локально на модулі, важливо знати скільки місця для зберігання доступно і скільки вільно. Це необхідно також для моніторингу обсягу оперативної пам'яті та циклів процесора, споживаних модулем.

Нижче наведені основні характеристики для NM-CIDS-K9 та IDSM-2, які будуть використовуватися як посилання.

Для NM-CIDS-K9:

- Операційна система Cisco IDS 4.1 Sensor Software
- Підтримувані платформи: Cisco 2600XM, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745;
- Процесор 500 MHz Intel Mobile Pentium III;
- SDRAM: 256Мб, макс.SDRAM: 512Мб;
- Внутрішня пам'ять: 20Гб IDE;
- Флеш-пам’ять: внутрішня 16 Мб плюс додаткова зовнішня флеш-пам’ять.

Для IDSM-2 (Cisco IDSM-2 класифікується як продукт із «надійним шифруванням», а його експорт обмежено):

- Операційна система: Red Hat Linux 6.2;
- Підтримувані платформи: Cisco Catalyst 6500 (1U module);
- Процесор: Pentium P3 1,13 ГГц на головній платі з 232 МГц IXP 32-розрядний процесор StrongARM на прискорювачі;
- RAM: 2Гб

- Внутрішня пам'ять: 100Гб жорсткий диск (використовується 20 Гб), 4 Гб пам’яті для подій.

Коли розгортається IDSM-2, трафік можна подавати в модуль двома способами:

• Використовуючи аналізатор комутованих портів (SPAN). Це зробити просто. Наприклад, Catalyst6500> set span 2/8 6/1 rx create відображатиме трафік від порту 2/8 до порту зчитування IDSM-2 6/1, тоді як Catalyst6500> set span 69 6/1 rx створювати копії трафіку VLAN 117 до порту 6/1 зондування IDSM-2 для аналізу.

• Використовуючи списки доступу до VLAN (VACL), як згадувалося раніше. Для цього потрібно, щоб механізм контролера комутаторів мав опцію картки функцій політики (PFC) і був складнішим у налаштуванні. Однак цей метод забезпечує більшу гнучкість у виборі трафіку для перевірки IDS. Якщо використовується кілька модулів IDSM-2, VACL можна використовувати для розподілу трафіку між ними.

За замовчуванням порт 1 перевірки IDSM-2 є магістральним портом, який отримуватиме трафік з усіх VLAN на комутаторі, доки до цих VLAN застосовуються списки ACL захоплення. Можна використати команди *set trunk* і *clear trunk* для вибору мереж VLAN, які необхідно контролювати за допомогою IDSM-2. Коли IDSM-2 відповідає сигнатурі, він може виконувати як реєстрацію подій/надсилання тривоги, так і уникання діапазон IP зловмисників. Однак немає можливості скидати з'єднання TCP.

2.5. Програмне забезпечення Cisco IOS IDS

Cisco IOS IDS ідентифікує більше 100 найпоширеніших атак та використовує сигнатури для виявлення зловживань мережевим трафіком. На відміну від датчиків Cisco 4200 або Cisco XT 5600 Detector Anomaly Detectors, відсутнє виявлення атак на основі знань.

У брандмауері Cisco IOS було надано лише 59 жорстко кодованих сигнатур виявлення вторгнень у Cisco IOS 12.2 (11) YU. Додаткові 42 нових жорстко

кодованих сигнатур включені до поточних випусків, на додаток до всіх (після випуску програмного забезпечення Cisco IOS 12.2T). Ці сигнатури були обрані з широкого спектру IDS і представляють найбільш серйозні порушення безпеки.

Загалом сигнатури Cisco IDS класифікуються за ступенем серйозності та складності:

• Інформаційні сигнатури (40). Виявлення спроб пінгу портів;

• Сигнатури атаки (61). Виявлення спроб зламу, таких як незаконні SMTP або надіслані команди FTP або спам поштою;

• Атомні сигнатури (74). Виявляють прості шаблони атак (специфічну атаку). Аудит цих сигнатур не залежить від інстенсивності трафіку.

• Складені сигнатури (27). Виявляють складні шаблони (тобто атаки проти декількох хостів, протягом тривалих періодів часу з кількома пакетами, надісланими зловмисниками). Для перевірки цих сигнатур CBAC виділяє пам'ять для ведення стану, конфігурації баз даних та внутрішнього кешування.

Різні типи сигнатур, що підтримуються Cisco Secure IDS, позначаються серійним номером, як показано:

• Серія 1000. Це сигнатури IP (проблеми фрагментації та неправильно сформовані IP –пакети);

• Серія 2000. Це сигнатури ICMP (різні типи трафіку ICMP та потоки ICMP);

• Серія 3000. Це сигнатури TCP (записи сеансів TCP, різні типи сканування портів TCP, викрадення TCP, потік SYN, пошта, FTP, NetBIOS, застарілі веб-атаки та інші форми сигнатур зловмисних дій, пов’язаних із TCP);

• Серія 4000. Це сигнатури UDP (записи трафіку UDP, сканування портів, повені та інші форми атак, пов'язаних з UDP);

• Серія 5000. Це сканування сигнатур атак, пов’язаних із веб-сайтом, загального інтерфейсу шлюзу (CGI);

• Серія 6000. Це міжпротокольні сигнатури (сигнатури системи імен доменів (DNS), віддаленого виклику процедур (RPC) і різних атак DDoS, а також позначення помилок автентифікації);

• Серія 8000. Це сигнатури зі збігом рядків (користувацькі строкові збіги та сигнатури користувацьких програм TCP);

• Серія 10000. Це сигнатури порушень ACL. Попередження про визначені порушення списків доступу IOS.

Класифікація за замовчуванням тривог, що надсилаються, коли сигнатури збігаються, прив’язані до рівня серйозності сигнатури. Для отримання інформації генеруються тривоги низького ступеня тяжкості 1 та 2 наприклад, при виявленні невідомого параметра IP. Середнього ступеня тяжкості 3 тривоги спрацьовують під час розгортання ping та сканування портів. Сигнали тривоги 4 та 5 високої тяжкості надсилається при виявлені повних з'єднань портів TCP і чітких атак (таких як спроби переповнення буфера). Якщо є сигнал тривоги на рівні 4 або 5, визначається можливий результат атаки (наприклад, захоплений банер проти віддаленої оболонки).

Якщо обхід пакетів відповідає відомій сигнатурі, можна налаштувати IDS Cisco IOS наступним чином:

• Надіслати повідомлення тривоги на віддалений сервер системного журналу або на інтерфейс централізованого управління.

• Викинути пакет, що порушує правила.

• Скинути підозріле з'єднання TCP. Відсутність уникнення або повний IP – сеанс реєстрація відбувається, як це можна зробити на датчиках серії Cisco IDS 4200 або (у разі ухилення) IDSM-2.

Налаштування надсилання, відкидання та скидання здійснюється за допомогою низки команд аудиту ip.

2.6. Брандмауери Cisco PIX як датчики IDS

Брандмауер PIX також є пристроєм IDS, подібним до програмного забезпечення IOS IDS на маршрутизаторі, тому і має подібний набір команд аудиту IP. Основною відмінністю між маршрутизаторами PIX та IOS IDS є кількість підтримуваних сигнатур і на які PIX не може надсилати повідомлення тривоги

консолі керування Cisco Secure IDS. Таким чином, при здійсненні централізованого віддаленого журналювання з PIX власник обмежений системним журналом UNIX. Адже функціональність IDS в PIX надається, перш за все, для покращення можливостей ведення журналу цього брандмауера та припинення атак на місці входу, відкидання, скидання та уникання трафіку, визнаного зловмисним.

PIX, природно, добре виконує такі дії і може працювати в парі з датчиком Cisco Secure IDS. Якщо це так, IP має пріоритет перед списками ACL, раніше налаштованими на PIX.

Дивно, але список сигнатур IDS на PIX не такий великий, як список на IOS IDS маршрутизатор і обмежується сигнатурами, що містяться в Cisco Network Security База даних (NSDB). Добре б відключити кілька сигнатур, щоб уникнути переповнення журналів інформацією мало значною для безпеки. Зазвичай додаються до маршрутизатора наступні файли конфігурації:

ip audit signature 2000 disable

ip audit signature 2001 disable

ip audit signature 2005 disable

Signatures. Підписи 2000, 2001 та 2005 означають відповідь ICMP Echo Reply, ICMP Host Unreachable, і 2005 ICMP. Їх не враховують, як критично важливі для безпеки, якщо компанія не прагне стежити за пінгом та трасуванням користувачів з власної мережі.

Повідомлення системного журналу PIX від 400000 до 400051 є повідомленнями підпису Cisco IDS; однак, якщо подивитися на весь список системного журналу PIX повідомлень, можна побачити більше повідомлень, пов'язаних з атаками, ніж просто 51.

Ось приклад, який, ймовірно, буде сигналом про спробу атаки, навіть якщо він не належить до Діапазон 400000–400051:

Message 403109

Error Message %PIX-4-403109: Rec'd packet not an PPTP packet. (ip) dest_address=dest_address, src_addr= source_address, data: string.

Пояснення. Брандмауер отримав підроблений пакет PPTP. Це може бути несанкціоноване втручання.

Рекомендована дія. Звернутися до адміністратора ристрою, щоб перевірити налаштування конфігурації PPTP.

2.7. Детектор аномалій Cisco Traffi c XT 5600

Cisco Traffic Anomaly Detector XT 5600 забезпечує багатогігабітну продуктивність для захисту мереж, швидко виявляючи потенційні DDoS, DoS та інші несанкціоновані втручання. Використовує методологію виявлення вторгнень на основі знань про виявлення шкідливої активності.

Детектор аномалій Cisco Traffic XT 5700 відрізняється від XT 5600, оскільки він пропонує багатомодові волоконно-оптичні порти 1000BASE-SX з LC-роз'ємами замість портів Ethernet 100/1000Base-T на XT 5600. Ці пристрої розроблені працювати в парі з Cisco Guard XT 5650, щоб запобігти DDoS -атакам, спрямованим на захищену мережу [9]. Виявлені та заблоковані атаки включають такі підроблені та несанкціоновані атаки:

- Потоки TCP (SYNS, SYN-ACKS, ACKS, FINS, фрагменти);
- Потоки UDP (випадкові порти, фрагменти);
- Потоки ICMP (недоступні, луна, фрагменти);
- Потоки DNS;
- Деякі атаки на стороніх клієнтів;
- Неактивне та повне перевантаження з'єднань;
- HTTP-запити на отримання даних;
- BGP-атаки.

Детектор аномалій Cisco Traffi c XT 5600 знаходиться поза критичним маршрутом до захищеної мережі і відображає всі трафіки, що надходять до мережі при пасивному слідкуванні для виявлення можливих аномалій. Після виявлення аномалії оповіщення надсилаються операторам мережі та Cisco Guard XT 5650

блокує шкідливе несанкціоноване втручання і видаляє пакети, що порушують безпеку.

2.8. Консолі керування Cisco Secure IDS

Крім PIX та Cisco Traffic Anomaly Detector XT 5600, усі прилади IDS описані раніше можуть бути налаштовані, керовані та контрольовані з Cisco Secure IDS консолі управління. Крім того, ці консолі надають послуги підкачки сторінок та доступ до бази даних мережевої безпеки, заповненої інформацією про підписи актуальних, діючих датчиків.

Cisco пропонує два різні пакети програмного забезпечення з функціональними можливостями IDS: UNIX та Cisco Secure Policy Manager на базі Windows NT (CSPM) з консолю IDS. Обидва продукти пропонують подібну функціональність з основними відмінностями між ними - локальне ведення журналу, відправка сигналу тривоги та розпізнавання рівня серйозності тривоги.

Важливою особливістю як UNIX Director, так і CSPM IDS Console є можливість створювати та розповсюджувати нові власні сигнатури для адаптації до нових вразливостей та загроз.

Подібно до архітектури датчиків серії Cisco IDS 4200, функціональність Cisco IDS UNIX реалізована як колекція службових процесів на Solaris (хоча і з додатково встановленим HP Open View). Насправді, багато службових процесів, використаних датчиком 4200 та UNIX однакові - наприклад, fileXferd, loggerd, postofficed та configd. Службові процеси, які також використовуються UNIX, включають smid (службові процеси, що заповнюють сигнатури тривог в інтерфейсі користувача HP Open View), sapd (дані та файли керування службових процесів), sapx (надає популяцію баз даних Oracle або Remedy) та eventd (службові процеси, які надсилають різні повідомлення на основі отриманих даних сигнатур) [10].

Зауважте, що ці службові процеси, за винятком sapx, також можна запускати на датчиках IDS 4200, навіть якщо вони не мають вирішального значення для роботи цих приладів.

Звичайно, архітектура консолі Windows CSPM IDS дещо відрізняється і включає наступне:

• nr.postofficed. Подібний до службового;

• датчик CA. Подібний до fileXferd;

• nr.smid. Службові процеси інтерфейсу управління безпекою;

• інтерфейс бази даних EDI - схожий на eventd;

• система перегляду подій EVS - виконує функцію, подібну до тієї, яку виконує HP Open View;

• Графічний інтерфейс конфігурації CIDS подібний до графічного інтерфейсу UNIX і до configd

• cvtnrlog.exe. Утиліта командного рядка Windows, подібна до UNIX Loggerd.

2.9. Рішення Cisco VPN

Ще одним важливим компонентом безпечних мереж, запропонованих Cisco, є можливість використання VPN для захисту даних під час передачі. Актуальними є три типи сценаріїв розгортання VPN: хост-мережа, мережа-мережа та хост-хост.

- Сценарій хост-мережа зазвичай використовується для підключення зовнішніх хостів до внутрішньої мережі. Класичний приклад - це забезпечення безпечного доступу мобільних користувачів до внутрішніх ресурсів підприємства.
- Сценарій «мережа до мережі» зазвичай використовується для забезпечення безпеки комунікації між двома або більше мережами одного підприємства, розташованих у географічно віддалених місцях.
- Сценарій хост-хост є найменш поширеним з усіх типів VPN. Типова ситуація розгортання - це створення безпечного каналу між двома хостами в Інтернеті.

VPN має задовольняти трьом критеріям - конфіденційність, цілісність та доступність. Фактор доступності залежить від багатьох зовнішніх умов, що не залежать від адміністратора мережі; тому необхідно зосередитися на перших двох факторах.

Таблиця 2.2.

Можливості сімейств пристроїв Cisco VPN Concentrator.

Cisco VPN Concentrator	3005	3015	3020	3030	3060	3080	5001	5002	5008
Пропускна спроможність щифрування, Мбіт/с	4	4	50	50	100	100	45	190	760
Користувачі	200	100	750	1500	5000	10000	1500	10000	40000
Шифрування	ПЗ	ПЗ	ПЗ	обладнання	обладнання	обладнання	обладнання	обладнання	обладнання
IOS маршрутизатор	830	900	1700	2600	2691	7400	3725	3745	7200
Пропускна спроможність, Мбіт/с	6	6	8	14	80	120	150	180	225
Тунелі	50	50	100	800	1000	5000	2000	2000	5000

Деякі джерела називають протоколи, такі як L2F, протокол тунелювання (L2TP), загальна інкапсуляція маршрутизації (GRE) і протокол «точка-точка» (PPP)

лише протоколами тунелювання, без здатності відслідковувати автентифікацію або шифрування трафіку.

Ідеальний приклад класичного галузевого стандартного VPN - це, звичайно, IPSec. Не дивно, він підтримується маршрутизаторами на основі Cisco IOS, починаючи з версії IOS 11.3 та брандмауерами PIX, починаючи з версії PIXOS 5.0. Крім того, визнаючи зростаючу потребу для безпечного зв'язку Cisco розробила нове сімейство пристроїв, призначених для термінації високошвидкісних з'єднань VPN, а саме серія Cisco VPN Concentrator (табл.2.2)

Незважаючи на обмежену обчислювальну здатність брандмауера PIX та маршрутизатора IOS щодо шифрування, Cisco не змушує кінцевого користувача істотно інвестувати в додаткові послуги.

Натомість існують два типи прискорення VPN (VAC) - за розумною ціною пропонується значне збільшення продуктивності обробки паралельних з'єднань і досягнення максимальної пропускної здатності.

Додаткова перевага досягається шляхом заміни математичних розрахунків інтенсивної частини криптографії до апаратного процесора VAC, тому звільняються цикли процесора у бік збільшення можливостей перемотування файлів. В табл.2.3. показані можливості сімейства брандмауерів Cisco PIX.

Таблиця 2.3.

Можливості брандмауера Cisco PIX

Модель PIX	501	506E	515E	525	535
Пропускна спроможність (3DES/128AES)	3/4.5	17 /30	140 /140	155 /165 (VAC+)	440 / 535 (VAC+)
Миттєві підключення	10	25	2000	2000	2000

VAC підтримує стандарти шифрування даних (DES) та шифрування 3DES і може бути встановлений на будь-які пристрої сімейства PIX від PIX 515 і т.д. Однак можна встановити лише одну карту, 168-розрядна пропускна здатність 3DES буде

збільшена до максимум 100 Мбіт/с, а кількість одночасних тунелів збільшено до 2000.

Друге видання VAC+ схоже за своєю функцією на попередника, але воно має більші можливості обробки та підтримує новіший 256-бітний розширений стандарт шифрування (AES). Максимальна пропускна здатність VPN збільшується до 440 Мбіт/с. Різні модулі апаратного шифрування також доступні для звичайних маршрутизаторів на базі IOS, як узагальнено у табл.2.4. Функціонально ці модулі подібні до PIX VAC.

Таблиця 2.4.

Маршрутизатори на базі IOS з модулем VPN

Модуль VPN	Пропускна спроможність(Мбіт/с)	Шифрування	Миттєві підключення
MOD1700-VPN	8	3DES	100
AIM-VPN/BP	10	3DES	
AIM-VPN/EP	15	3DES	800
AIM-VPN/HP	42	3DES	2000
AIM-VPN/BPII	22	3DES/AES128	800
AIM-VPN/BP	150	3DES/AES128	800
AIM-VPN/BP	180	3DES/AES128	2000
AIM-VPN/BP	18	3DES	800
AIM-VPN/BP	22	3DES/AES256	800
AIM-VPN/BP	150	3DES/AES256	800
AIM-VPN/BP	180	3DES/AES256	2000

2.10. Рішення Cisco IPSec

IPSec складається з трьох складових частин: заголовок автентифікації (AH), інкапсульоване корисне навантаження (ESP) та обмін ключами (IKE) [11].

Заголовок автентифікації. AH (протокол IP51) використовується для забезпечення автентифікації та цілісності потоку даних між користувачами. Дайджест повідомлення обчислюється і надсилається до кінцевого вузла; це повідомлення містить похідні від значень як у заголовку IP, так і корисного навантаження даних. Приймальний кінець обчислює інший дайджест повідомлень на основі прийнятого пакету і порівнює його з отриманим повідомлень. Якщо будь-яке поле пакетів було змінено під час транзиту, така зміна буде помітна. AH також обліковує послугу проти відтворення, реалізуючи розсувне вікно для кожного вузла IPSec. Cisco підтримує стандартні функції перегляду повідомлень MD5 та SHA1.

Інкапсульоване корисне навантаження (ESP). Для клієнтів, яким потрібна конфіденційність потоку даних, ESP (протокол IP 50) пропонує два варіанти можливих рішень. Корисне навантаження даних може бути зашифровано, із можливістю залишити інформацію заголовка цілі (транспортний рівень) або повністю всього пакету, який можна зашифрувати (тунельний режим) і додаючи нові заголовки. Тунельний режим забезпечує додатковий рівень безпеки, оскільки джерело та адреса призначення пакета приховані. Cisco підтримує DES, 3DES та AES як стандартні алгоритми шифрування.

Обмін ключами. IKE - це протокол обміну безпекою загального призначення, який використовується на 1 етапі – аутентифікуються користувачі IPSec та встановлюється безпечний канал для захисту каналу (до фази 2).

Фаза 1. Під час фази 1 IKE виконуються такі функції:

• Аутентифікація та захист ідентифікацій вузлів IPSec;

• Відповідність каналам зв’язку щодо політики IKE Security Association (SA) для захисту IKE;

• Автентифікований обмін Diffie-Hellman для встановлення відповідного спільного секретного ключа, який є ключем сеансу для симетричного шифру (зазвичай 3DES або AES) для фактичного шифрування трафіку;

• Встановлення тунелю для комунікації для етапу 2 IKE.

Фаза 2. Використовується для узгодження SA IPSec, що використовуються для встановлення тунелю IPSec для захисту IP трафіку. Під час фази 2 IKE виконуються такі функції:

• Обмін інформацією щодо параметрів IPSec SA;

• Утворення каналу IPSec SA;

• Періодичний обмін інформацією про IPSec SA;

• Додатковий обмін Diffie-Hellman для PFS.

Cisco використовує дві форми аутентифікації для авторизації користувачів, які беруть участь у з'єднанні IPSec: PSK та сертифікати x509. Перший ґрунтується на доказі володіння спільним ключем. Хоча це працює добре для обмеженої кількості хостів-учасників, залучених до VPN, таке рішення гірше масштабується.

Другий спосіб ґрунтується на криптографії відкритого ключа RSA використовується як частина стандарту x509, де кожен вузол має public/private частину сертифікату. Метод ґрунтується на тому, що вузол-відправник шифрує деякі псевдовипадкові дані з відкритим ключем іншого вузла; таке повідомлення можна розшифрувати тільки власником відповідного приватного ключа. Приймаючий хост розшифровує такі повідомлення і повторює процес навпаки.

2.11. Cisco AAA

Методологія AAA. Методика автентифікації, авторизації та обліку була розроблена для динамічного контролю за рівнями доступу до мережевих ресурсів, включаючи можливість моніторингу мережі, застосування політики, обліку використання мережі та надання інформації, необхідної для стягнення плати за користування мережею (білінг). Пропонується використовувати принципи AAA як основу для безпечного та надійного розгортання мережі. Cisco визначає такі переваги використання AAA: підвищена гнучкість та контроль конфігурації доступу, масштабованість, стандартизовані методи аутентифікації, такі як RADIUS, TACACS+ і Kerberos, кілька систем резервного копіювання.

Програмне забезпечення та обладнання Cisco є гарним прикладом застосування системи AAA в масштабах всієї корпорації на різних рівнях розгортання мережевої інфраструктури. Усе обладнання Cisco може бути сконфігуровано таким чином, щоб дозволити аутентифікацію, авторизацію та облік користувачів із централізованої бази даних за допомогою RADIUS, TACACS+або іншого методу, такого як Kerberos. Cisco Systems розробила продукти для підтримки інфраструктури AAA, починаючи від обладнання мережевого сервера автентифікації користувачів (NAS) до кінцевих мережевих маршрутизаторів та комутаторів:

• Реєстр доступу Cisco CNS;

• Мережевий реєстратор Cisco CNS;

• Програмне забезпечення Cisco Global Roaming Server;

• Сервер управління безпечним доступом Cisco;

• Cisco Secure Access Control Server Solution Engine;

• Інструмент безпечної реєстрації користувачів Cisco.

Підсистема клієнта AAA Cisco. Усі пристрої Cisco, починаючи від обладнання SOHO і закінчуючи промисловими брандмауерами, комутаторами та маршрутизаторами, підтримують послуги AAA. Налаштування AAA для клієнтської сторони є відносно простим і дуже схожим для різних типів обладнання. Щоб увімкнути безпеку на маршрутизаторі або брандмауері Cisco за допомогою AAA, необхідно виконати процедуру [12]:

1. Увімкнення AAA за допомогою команди глобальної конфігурації AAA для нової моделі.

2. Якщо заплановано використання окремого сервера AAA, необхідно налаштування параметрів протоколу безпеки, такі як RADIUS, TACACS+ або Kerberos відповідно до вимог.

3. Необхідно визначення списків методів для автентифікації за допомогою команди автентифікації AAA.

4. За потреби застосовуються списки методів до певного інтерфейсу або рядка.

5. Необхідно налаштувати авторизацію за допомогою команди авторизації AAA.

6. Необхідно налаштувати облік за допомогою команди обліку AAA.

7. Потрібно створити на пристрої локальну базу даних користувачів із рядком імені користувача <ім'я> пароль <пароль> і встановити її як другий вибір після RADIUS/TACACS+ у команді автентифікації AAA (параметр локальний). Це позбавить користувачів від багатьох проблем у разі виходу з ладу центрального сервера автентифікації.

Непогано мати б резервний центральний сервер автентифікації, який би виконував між собою та основним сервером автентифікації протокол резервування, такий як протокол стійкості віртуального маршрутизатора (VRRP).

Cisco CNS Access Registrar. Це RADIUS-сумісний сервер, розроблений для підтримки AAA для здійснення комунікацій по ISDN, кабелю, DSL, безпроводовим каналам та VoIP. Cisco CNS Access Registrar забезпечує продуктивність і масштабованість операторського класу, а також можливості розширення, необхідні для інтеграції з системами керування послугами, що розвиваються.

Реєстр доступу Cisco з версії 3.0 також має можливість надсилати запити AAA в режимі реального часу до білінгових систем для підтримки ринку додатків з передоплатою, таких як точки безпроводового доступу. Нижче наведено деякі функції реєстратора доступу CNS:

- Підтримка баз даних Oracle через Open Database Connectivity (ODBC);
- Білінг;
- Підтримка EAP-MD5;
- Розширений інтерфейс конфігурації з автоматичним завершенням команди;
- Відкликання значень для швидкого редагування;
- Швидше та просте налаштування атрибутів користувача;
- Швидше та просте налаштування контрольних пунктів;
- Детальні повідомлення про помилки конфігурації;
- Правило префіксів у механізмі політики;

• Повторна прив'язка каталогу полегшеного протоколу доступу до каталогу (LDAP);

• Збільшена підтримка постачальників (ISP);

• Перенесення файлів обліку на основі часу;

• Заміна пароля користувача;

• Оптимізована обробка запитів обліку, включаючи вдосконалені алгоритми обробки повторюваних запитів, що містять Acct-Delay-Time.

Програмне забезпечення реєстратора доступу Cisco працює на апаратному забезпеченні Sun Solaris/SPARC із встановленою Solaris 7/8.

Мережевий реєстратор Cisco CNS. Це повнофункціональна система DNS/DHCP, яка забезпечує масштабовані послуги іменування та адресації для корпоративних мереж і мереж постачальників послуг. Для кабельних провайдерів мережевий реєстратор Cisco CNS додатково надає послуги масштабованого DNS та протоколу динамічної конфігурації хосту (DHCP) і лежить в основі системи забезпечення кабельного модему Data Over Cable Service Interface Specification (DOCSIS).

Мережевий реєстратор Cisco CNS містить стандартний DNS-сервер, який пропонує розширений набір функцій, включаючи підтримку зон, динамічних оновлень та сповіщень. Сервер DHCP Network Registrar Cisco CNS підтримує DHCP Safe (резервні сервери DHCP), динамічні оновлення DNS, кабельні модеми DOCSIS та інтеграція зі службами каталогів за допомогою LDAPv3. CNS Network Registrar доступний для серверів Solaris 8/9, Windows 2000 і різних платформ Linux.

Програмне забезпечення CiscoSecure. CiscoSecure Global Roaming Server (GRS) — це спеціалізоване програмне забезпечення безпеки для AAA. CiscoSecure GRS перетворює існуючі інфраструктури комутованого зв’язку у віртуальні точки присутності (PoPs). Використовуючи GRS, постачальник доступу до мережі може запропонувати оптові послуги доступу з набору номера, такі як роумінг в Інтернеті, роумінг інтранет (роумінг віртуальна мережа приватного набору номера [VPDN]) і доступ VPDN.

Підсистема AAA на основі сервера Cisco Access. У цьому пункті висвітлюються різні моделі серверів доступу Cisco, які використовуються для аутентифікації та авторизації як для RADIUS, так і для TACACS+.

Моделі серверів доступу зазвичай починаються з AS, за яким йде чотиризначне число, залежно від можливостей необхідної платформи. Наприклад, шлюз серії AS5800 є продуктом з найвищою ємністю та високою доступністю серед типів серверів доступу Cisco. Ця платформа призначена для задоволення потреб великих, динамічних постачальників послуг, підтримуючи до 5 каналізованих T3 (CT3), 96 T1s, 86 E1s або 2 STM-1 (108 E1s) послуг передачі даних, голосу та факсу, на будь-який порт у будь-який час підтримує до 3360 одночасних користувачів. Тоді як шлюз Cisco AS5350 є економічно ефективною платформою, яка підтримує 2-, 4- або 8-портові конфігурації T1/7-порту E1 і забезпечує універсальні дані порту, голосові та факс-послуги на будь-якому порту в будь-який час. AS5350 має модульну конструкцію і ідеально підходить для невеликих провайдерів Інтернет та корпоративних компаній. Сервер доступу середнього рівня серії AS5400 є ідеальним рішенням для доступу в організації середнього розміру, яка не вимагає продуктивності такого масштабного рішення, як AS5800.

Сервер управління безпечним доступом Cisco. Розгортання Cisco серверної платформи AAA має два варіанти. Один із них реалізований у програмному забезпеченні, яке доступне як для платформ Windows, так і для UNIX є сервер безпечного контролю доступу Cisco (ACS). Інший тип ACS — це високомасштабована апаратна платформа під назвою Cisco Secure Access Control Server Solution Engine. Він подає дані автентифікації, авторизації та обліку з централізованого протоколу RADIUS або TACACS+. Апаратний механізм допомагає забезпечити виконання призначених політик, дозволяючи адміністраторам мережі контролювати наступне:

- Хто може увійти в мережу;
- Привілеї, які має кожен користувач у мережі;
- Записаний аудит безпеки або платіжна інформація по рахунку;

• Елементи керування доступом та командами, які ввімкнені для адміністратора кожної конфігурації.

Необхідні специфікації:

• Процесор: Intel Pentium 4 3,2 ГГц;

• Пам'ять: 1 Гб оперативної пам'яті;

• Жорсткий диск: 80 ГБ вільного місця на диску;

• Мережа: Два вбудованих контролера 10/100 Ethernet.

Інструмент безпечної реєстрації користувачів Cisco. Засіб реєстрації користувачів Cisco (URT) — це інструмент динамічної авторизації та контролю політик, який керує доступом до ресурсів локальної мережі шляхом розподілу трафіку користувачів через мережі VLAN. Він забезпечує підвищену безпеку локальної мережі шляхом ідентифікації та аутентифікації користувачів, коли вони починають доступ до мережі. Cisco URT пов'язує користувачів із мережевими ресурсами, якими вони мають право користуватися, динамічно призначаючи їх до відповідної VLAN. Cisco URT може контролювати ідентифікацію користувачів, розташування та час доступу, а також дозволяти користувачам бути мобільними у всій організації та безпечно отримувати доступ до своїх ресурсів та послуг з будь - якого доступного мережевого порту.

Починаючи з версії 2.5 і новіших, URT представляє веб-ресурс клієнта та інфраструктуру внутрішньої аутентифікації на основі RADIUS, що робить його придатним для розширеного діапазону мереж клієнтів та програм. Сервер адміністрування URT доступний для цілого ряду серверів Windows, тоді як програмне забезпечення клієнта інтерфейсу доступне для платформ Windows, Linux та MacOS.

Методологія AAA, що працює на практиці, представлена на рис.2.1. Клієнти підключаються до Інтернет-провайдера за допомогою дозвону або іншим способом. Сервер NAS запитує облікові дані для автентифікації від користувачів і передає їх на сервер RADIUS/ TACACS+ ACS. Після успішної авторизації обладнання NAS надає клієнтам доступ до ресурсів мережі. Якщо функціональність обліку була ввімкнена, обладнання NAS надсилало б усі

необхідні дані на сервер обліку ACS для моніторингу використання мережі клієнтами[12].

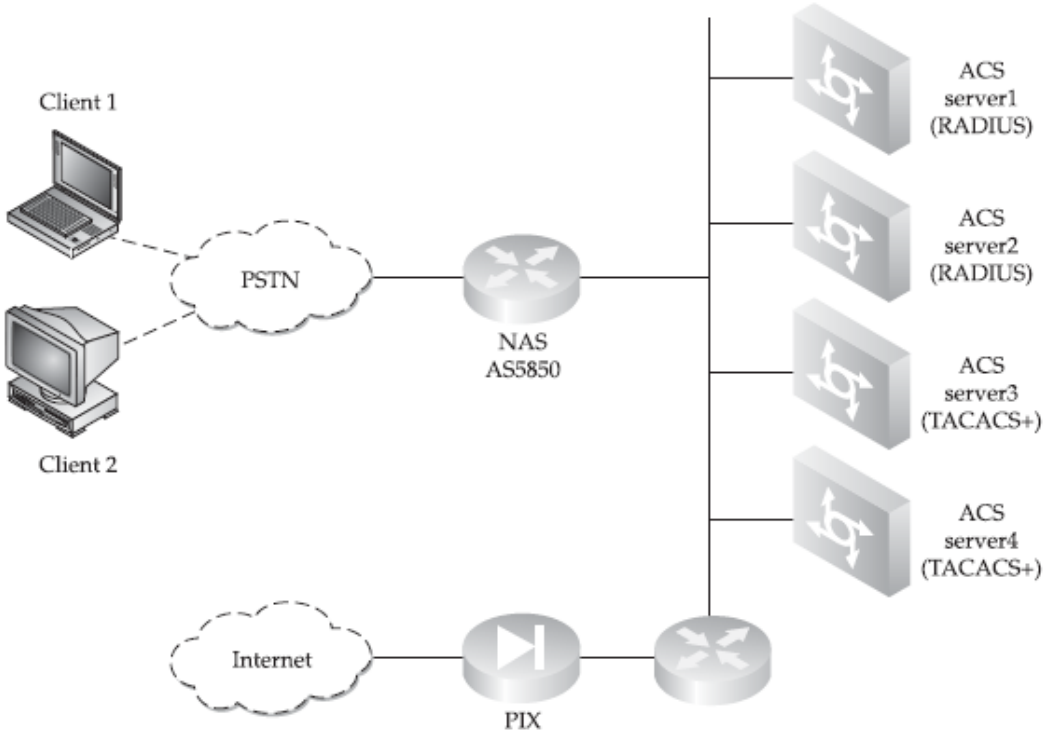

Рис.2.1. Типова конфігурація безпеки мережі AAA

2.12. Модель протидії наслідкам несанкціонованих втручань з використанням рішень безпеки Cisco

На рис.2.2 представлені різні пристрої безпеки Cisco, розповсюджені разом із трьома рівнями мережі підприємства. Звісно, рівнів може бути більше.

Одним із прикладів є декілька програм управління пристроями, розроблених компанією Cisco для спрощення складного завдання налаштування, оновлення та моніторингу пристроїв із дуже різним синтаксисом команд, включаючи, але не обмежуючись цим: IOS CLI, CatOS CLI, PIXOS CLI, Aironet CLI, Cisco 700 CLI, оболонка UNIX (пристрої Cisco на базі Linux та Solaris), CMD.EXE (серверні програми на базі Windows), snmpget, snmpset та інші утиліти Net-SNMP, різні графічні інтерфейси.

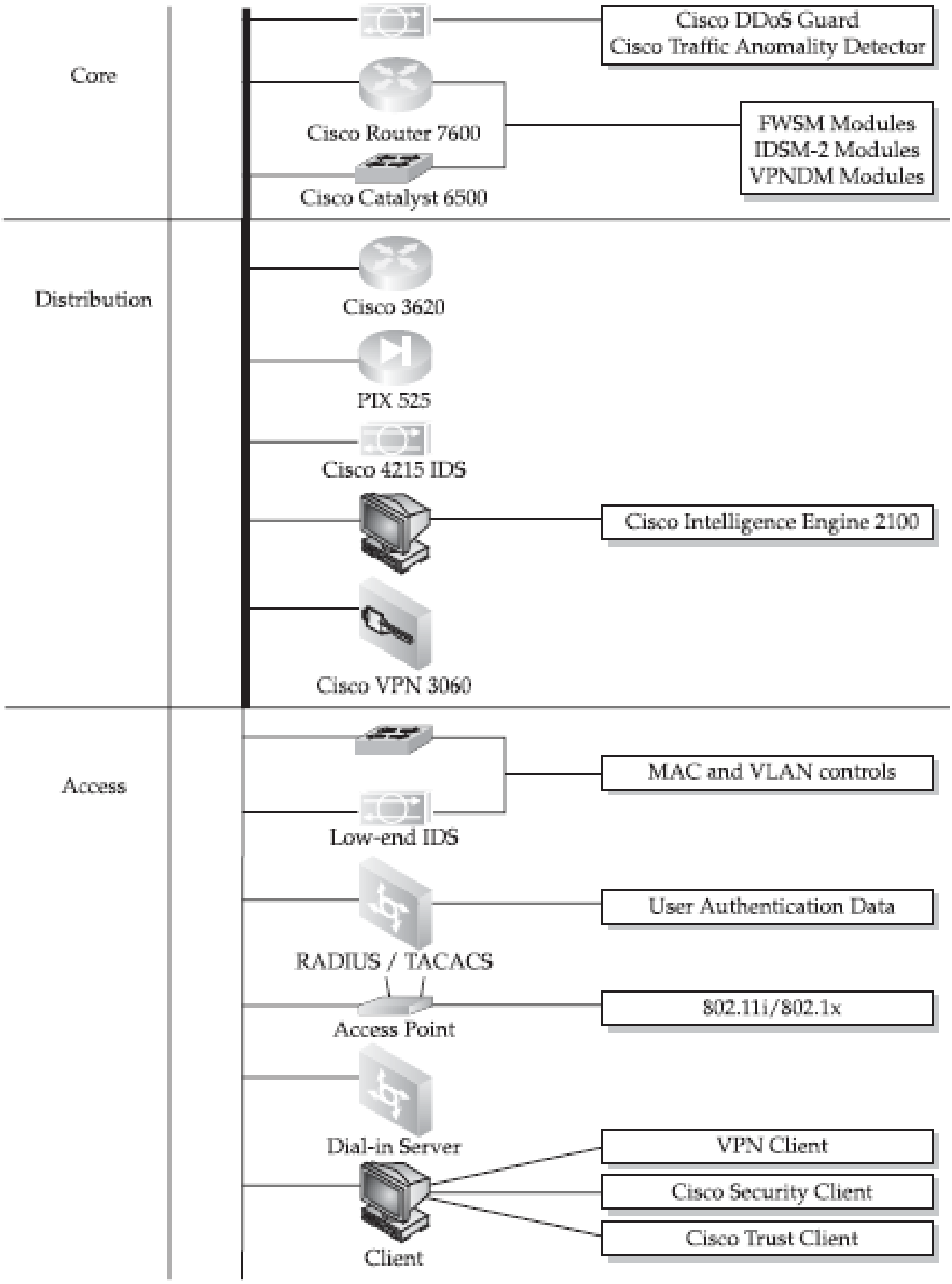

Рис.2.2. Модель безпеки мережі ієрархічного проектування Cisco

Програми управління Cisco охоплюють усі аспекти безпеки мережі та Cisco, і майже всі вони можуть бути інтегровані з набором CiscoWorks. CiscoWorks – це рішення для управління інформацією про безпеку (SIMS), яка охоплює збір, аналіз та співвідношення подій безпеки у всій корпоративній мережі. Налаштувати безпеки декількох маршрутизаторів Cisco одночасно, Cisco Router і Security Device Manager (SDM) підтримують маршрутизатори Cisco 830, 1700, 2600XM, 2691, 3600, 3700, 7204VXR, 7206XVR і 7301.

Для пристроїв Cisco, що стосуються безпеки, доступні Cisco PIX Device Manager, CiscoWorks VPN/Security Management Solution і Cisco IP Solution Center. Нарешті, для автоматизованого обслуговування та моніторингу мережі доступний набір продуктів Cisco CNS або так званих інтелектуальних агентів. До них відноситься Cisco CNS Access Registrar, який є сумісним із RADIUS сервером політики доступу для послуг ISP AAA, що підтримує всі типи доступу користувачів.

Інтелектуальні агенти Cisco CNS можна запускати на робочих станціях Solaris, Linux та HP-UX або на спеціалізованому пристрої-Cisco CNS 2100 Series Intelligence Engine, показаному на рис.2.2. Сервер політики VLAN Cisco 1102 також може бути розгорнутий на рівні доступу для управління мережами VLAN та запуску засобу реєстрації користувачів Cisco (URT), описаного раніше.

Усі ці рішення та прилади в комплексі складають те, що Cisco називає самозахисною мережевою стратегією. В ідеалі мережі, що самозахищаються, повинні мати можливість ідентифікувати атаки, належним чином реагувати на їх рівень серйозності, ізолювати зламані хости та переналаштовувати мережеві ресурси для блокування атак та несанкціонованих втручань.

Хоча постачальники можуть досягти майже автоматизованого керування мережею, включаючи управління безпекою, вони ніколи не можуть бути на 100% автоматизованими. Впровадження більшої кількості пристроїв і програм для забезпечення безпеки означає, що потрібно більше знань і навичок у сфері безпеки. Крім того, той факт, що CiscoWorks та компанія надають зручний для користувача

інтерфейс «клацання та натискання», не означає, що не слід знати особливості налаштування CLI.

Ці програми розробляються через необхідність управління масивними мережами, які неможливо обслуговувати інакше, з урахуванням кількості та навантаження системних адміністраторів. Графічні інтерфейси керування не охоплюють багатьох можливостей пристроїв, якими вони керують, вони також не мають помилок і комунікацій і завжди доступні[14].

Висновки до другого розділу

Досліджено величезну різноманітність рішень безпеки Cisco та їх елементів. Якщо їх правильно вибрати, розгорнути, налаштувати та підтримувати, ці пристрої та програми можуть зупинити більшість несанкціонованих втручань та мережевих атак. Виокремлено, що це мета поглибленої стратегії захисту самозахисних мереж Cisco.

Зазначено, що з іншого боку, засоби безпеки Cisco можуть самі стати цілю для хитрих зловмисників, які мають намір обійти контрзаходи мережевої безпеки та приховати свої сліди. Досвідчений нападник вивчить ці рішення безпеки з великою увагою, так само, як професійний зловмисник вивчає безпечні замки та системи сигналізації, перш ніж спробувати серйозного злому.

Підкреслено, що хоча постачальники послуг можуть досягти майже автоматизованого керування мережею, включаючи управління безпекою, вони ніколи не можуть бути на 100% автоматизованими. Впровадження більшої кількості пристроїв і програм для забезпечення безпеки означає, що потрібно більше знань і навичок у сфері безпеки, однак і визначає необхідність чуткого та правильного налаштування CLI.

3 МЕТОД ПОБУДОВИ СИСТЕМИ АВТОМАТИЗОВАНОГО ЗБОРУ ТА ПЕРЕВІРКИ НАЛАШТУВАНЬ БЕЗПЕКИ НА МЕРЕЖЕВОМУ ОБЛАДНАНІ CISCO З МЕТОЮ ПРОТИДІЇ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ

Управління контрольованим доступом до мережевих ресурсів з ненадійної мережі (нариклад, мережа Інтернет) є дуже важливою та критично необхідною функцією Cisco Security Appliance. Списки доступу, автентифікація та авторизація - це способи надання доступу через пристрій безпеки контрольованим способом. Крім того, версія програмного забезпечення PIX 6.2 і пізніших версій, а також програмне забезпечення ASA версії 7.0 мають нові функції, такі як об'єкт групування та TurboACL, які роблять управління та реалізацію складної політики безпеки набагато простіше та масштабніше[15].

Обмеження доступу до систем і служб у мережі підприємства є одним з основних обов’язків Cisco Security Appliance, які необхідно розгортат в мережі, якщо мова йде про підприємство з більш аніж одним офісом. Далі будуть надані рекомендації щодо того, як обмежити мережевий трафік за допомогою списків доступу, приховати внутрішні адреси за допомогою трансляції мережевих адрес (NAT) (як статичних, так і динамісних), а також налаштувати протоколи виправлення, які контролюють загальні протоколи доступу через Security Appliance.

3.1. Налаштування доступу через Cisco Security Appliance

В основі, двоетапний підхід, що дозволяє з'єднувати, ініціювати підключення до інтерфейсів із меншим рівнем безпеки, та отримувати доступ до інтерфейсів з більш високим рівнем безпеки.

Статичний NAT. Створює постійне, індивідуальне відображення між адресою на пристрої внутрішньої мережі (інтерфейс вищого рівня безпеки) та

зовнішньої мережі (нижчий рівень безпеки) інтерфей у всіх версіях Security Appliance. Щоб зовнішній хост ініціював трафік всередині хосту, для внутрішнього хоста має існувати правило статичного перекладу.

Таблиця 3.1

Статичні параметри команди

Команда	Опис параметра команди
prenat-interface	Зазвичай внутрішній інтерфейс, в цьому випадку застосовується переклад на внутрішню адресу.
postnat-interface	Зовнішній інтерфейс, коли prenat-interface-це внутрішній інтерфейс. Однак, якщо зовнішній інтерфейс використовується для інтерфейсу prenat, файл переклад застосовується до зовнішньої адреси та до поштового інтерфейсу є внутрішнім інтерфейсом.
mapped-address	Адреса, на яку перекладено реальну адресу.
interface	Вказує на перевантаження глобальної адреси з інтерфейсу.
dns	Вказує, що відповіді DNS, які відповідають xlate, перекладаються.
mask або network-mask	Відноситься як до глобального IP, так і до локального IP. Для адрес хостів завжди використовуйте 255.255.255.255. Для мережевих адрес використовуються відповідні маски класу або маска підмережі.
norandomseq	Не рандомізує порядковий номер пакета TCP/IP. Використовується цей параметр, тільки якщо інший вбудований брандмауер також має рандомізовану послідовність цифр, а результат - скремблювання даних. Використовуючи цю опцію відкриває діру безпеки в брандмауері PIX.
max-conns	Максимальна кількість з'єднань, дозволених через статику IP - адреса одночасно.
emb-limit	Ліміт початкового з'єднання. За замовчуванням 0, що означає необмежену кількість з'єднань.

Синтаксис статичної команди (детальніше в табл.3.1.) такий:

static [(prenat-interface, postnat-interface)] {mapped-address | interface}

real-address [dns] [netmask mask] [max-conns [emb-limit]] [norandomseq]

У наведеному нижче прикладі відображено сервер із внутрішньою IP -адресою 10.1.100.10 до IP адреса 192.168.100.10:

PIXFIREWALL(conf)#static (inside, outside) 192.168.100.10 10.1.100.10 netmask 255.255.255.255

Статичну команду також можна використовувати для перекладу підмережі IP:

PIXFIREWALL(conf)#static (inside, outside) 192.168.100.0 10.1.100.0 netmask 255.255.255.0

Наступний синтаксис показує сервер із внутрішньою IP -адресою 10.1.100.10, перекладеною на IP -адресу 192.168.100.10:

PIXFIREWALL(conf)#static (inside, outside) 192.168.100.10 10.1.100.10 255.255.255.255

Статичний PAT. Функція перенаправлення портів дозволяє зовнішнім користувачам підключатися до певної IP-адреси/порту та переспрямовувати трафік на відповідний внутрішній сервер. Спільна адреса може бути унікальною адресою або спільною вихідною PAT-адресою, або вона може бути спільною для зовнішнього інтерфейсу[17].

Наприклад, статична PAT дозволяє переспрямовувати послуги протоколу вхідної передачі (TCP) та протоколу користувацької дейтаграми (UDP). Використовуючи опцію інтерфейсу статичної команди, можна використовувати статичну PAT, щоб дозволити зовнішнім хостам отримувати доступ до служб TCP або UDP, що знаходяться на внутрішньому хості. (Однак, як завжди, список доступу також повинен бути встановлений для контролю доступу до внутрішнього хоста.)

Команда для налаштування статичного PAT виглядає наступним чином:

static [(internal-if-name, external-if-name)] {tcp | udp}{global-ip | interface}

global-port local-ip local-port [netmask mask][max-conns [emb-limit [norandomseq]]]

Статичний PAT підтримує всі програми, які підтримуються (звичайними) PAT, включаючи ті ж обмеження програми. Як і PAT, статичний PAT не підтримує H.323 або трафік мультимедійних програм. Наступний приклад включає статичний PAT для трафіку протоколу передачі файлів (FTP):

static (inside, outside) tcp 192.168.1.14 ftp 10.1.2.8 ftp

Наступний приклад показує наступне:

- Пристрій безпеки перенаправляє запити Telnet зовнішніх користувачів на 192.168.1.24 на IP -адресу 10.1.2.19.
- Security Appliance перенаправляє зовнішніх користувачів за протоколом передачі гіпертексту (HTTP)

port 8080 requests to 192.168.1.24 to PAT address 10.1.2.20 port 80:

static (inside,outside) tcp 192.168.1.24 telnet 10.1.2.19 telnet netmask 255.255.255.255

static (inside,outside) tcp 192.168.1.24 8080 10.1.2.20 www netmask 255.255.255.255

access-list 101 permit tcp any host 192.168.1.24 eq 8080

access-list 101 permit tcp any host 192.168.1.24 eq telnet

Зовнішня IP-адреса 192.168.1.24 однакова для обох відображень, але внутрішня IP-адреса відрізняється. Зовнішні користувачі, спрямовані на 192.168.1.24:8080, надсилаються як HTTP-запити на 10.1.2.20, який прослуховує порт 80.

Функція перехоплення TCP. До версії 5.2 Cisco PIX Firewall Security Appliance не пропонував жодного механізму захисту систем, до яких можна було б отримати доступ за допомогою статичного та TCP -каналу від атак TCP SYN.

Коли ліміт початкового підключення було налаштовано в статичній команді, попередні версії PIX просто припиняли нові спроби підключення, щойно було досягнуто початкового порогу.

Атака TCP SYN потенційно може спричинити порушення роботи сервісу для відповідного сервера. Для статичних командних команд без обмежень початкових з'єднання брандмауер PIX передає весь трафік. Якщо заражена система не має захисту від атак TCP SYN (більшість операційних систем не забезпечують достатнього захисту), таблиця початкових з'єднань ураженої системи перевантажується та припиняється весь трафік.

З функцією перехоплення TCP, як тільки буде досягнуто необов'язкове обмеження початкових з'єднань і доки кількість початкових з'єднань не впаде нижче цього порогу, кожен SYN, зв'язаний для ураженого сервера, перехоплюється. Для кожного SYN пристрій безпеки, такий як брандмауер PIX, відповідає від імені сервера порожнім сегментом SYN/ACK. Пристрій безпеки зберігає відповідну інформацію про стан, скидає пакет і чекає підтвердження клієнта.

Якщо отримано ACK, на сервер надсилається копія сегменту SYN клієнта, і між пристроєм безпеки та сервером виконується тристороннє рукостискання TCP. Якщо це тристороннє рукостискання завершиться, з'єднання відновиться в звичайному режимі. Якщо клієнт не відповідає протягом будь-якої частини фази з'єднання, Security Appliance повторно передає необхідний сегмент.

На додаток до функції перехоплення TCP, програмне забезпечення версії 6.3 та пізнішої впровадило файли cookie SYN як засіб зупинити заповнення SYN від заповнення черги SYN та спричинення розриву з'єднань. Файли cookie SYN використовують криптографічний метод для створення вихідних порядкових номерів TCP для потоку TCP. Цей новий метод допомагає Security Appliance керувати чергою TCP, відповідаючи на TCP -з'єднання за допомогою SYN+ACK, коли черга SYN заповнюється[18].

Security Appliance чекатиме ACK від віддаленого пристрою та перевірить ACK за допомогою призначеного 24-розрядного ключа. Пристрій безпеки потім відновить сеанс SYN на основі цієї інформації. Це дозволяє SYN збільшуватися, але ніколи не досягати такого розміру, який спричиняє відкидання, і усуває найбільший ефект атаки SYN flood, який полягає у відключенні великих вікон.

3.2. Команда nat 0

Як згадувалося раніше, можна налаштувати доступ до підмереж вищого рівня безпеки за допомогою команди nat 0. Наприклад, якщо є хост із загальнодоступною адресою у внутрішній мережі, а зовнішня мережа потребує доступу до цього хосту, можна використовувати nat 0, який вимикає переклад адреси, щоб внутрішні IP - адреси були видимими зовні. Наступний короткий приклад демонструє використання команди nat 0:

nat (inside) 0 192.168.1.10 255.255.255.255

Це також можна налаштувати наступним чином:

access-list 121 permit 192.168.1.10 255.255.255.255 any

nat (inside) 0 access-list 121

Політика NAT надає додаткові можливості у налаштуванні перекладу адрес. Функція політики NAT дозволяє ідентифікувати локальний трафік для трансляції адрес, вказуючи адреси джерела та призначення (або порти), тоді як звичайний NAT використовує лише порти/адреси джерела[19]. Іншими словами, один і той же локальний трафік для перекладу адреси може мати кілька «глобальних» перекладів залежно від IP -адреси або порту призначення (рис.3.1).

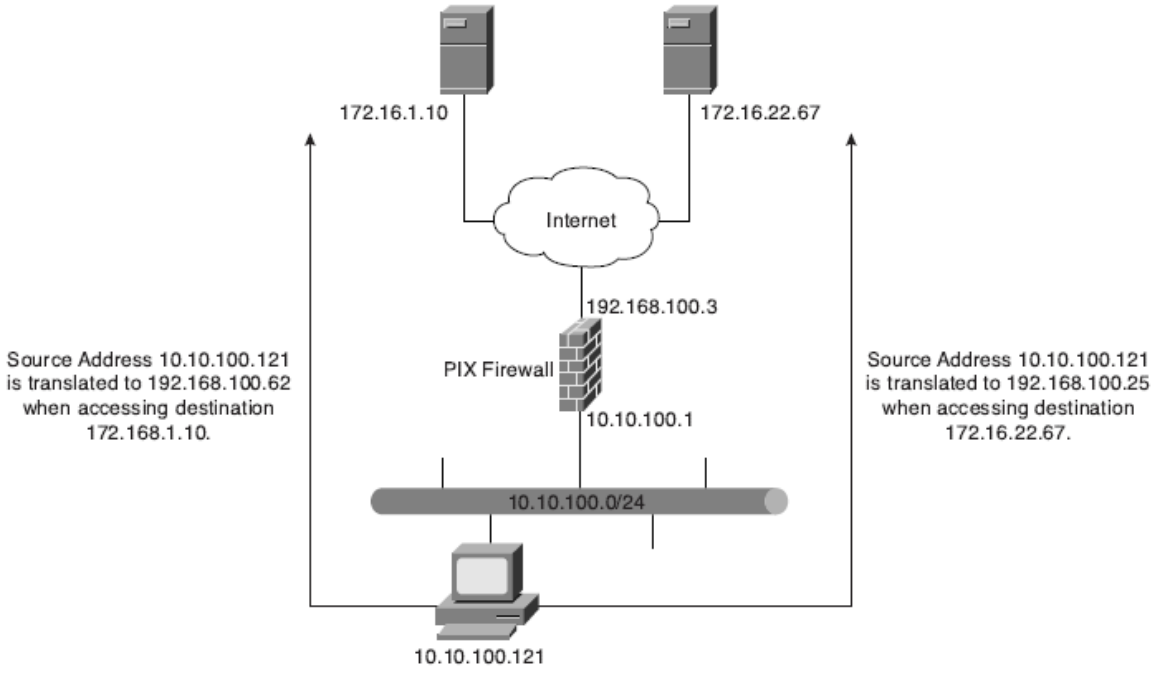

Рис.3.1. Визначення кількох зовнішніх адрес за допомогою NAT політики

Конфігурація для рис.3.1. така:

pixfw(config)#access-list 120 permit ip 10.10.100.0 255.255.255.0 172.16.1.10 255.255.255.255

pixfw(config)#access-list 130 permit ip 10.10.100.0 255.255.255.0 172.16.22.67 255.255.255.255

pixfw(config)#nat (inside) 1 access-list 120

pixfw(config)#global (outside) 1 192.168.100.62 255.255.255.255

pixfw(config)#nat (inside) 2 access-list 130

pixfw(config)#global (outside) 2 192.168.100.25 255.255.255.255

Існує ряд обмежень, про які варто знати, перед налаштуванням політики NAT:

1) Глобальна адреса не може використовуватися одночасно для NAT і PAT.

2) Списки доступу до політики NAT не можуть містити операторів заборони. Списки доступу повинні містити лише оператори дозволу.

3) Використовуються список доступу між командами nat і static, статичні команди узгоджуються та виконуються перед командами nat.

3.3. Списки доступу

Список доступу зазвичай складається з декількох записів контролю доступу (ACE), організованих внутрішнім Security Appliance. Коли пакет піддається контролю списку доступу, Cisco Security Appliance шукає цей зв’язаний список лінійно, щоб знайти відповідний елемент. Потім відповідний елемент перевіряється, щоб визначити, чи потрібно передавати або відкидати пакет.

За замовчуванням усі команди зі списком доступу мають неявну заборону, якщо чітко не вказується дозвіл. Іншими словами, за замовчуванням будь-який доступ до списку доступу заборонений, якщо явно не надається доступ за допомогою оператора дозволу[19].

Загальний синтаксис команди access-list виглядає наступним чином:

Таблиця 3.2

Параметри команд списку доступу

Команда	Опис
id	Назва списку доступу. Можна використовувати ім’я або номер.
line-num	Номер рядка, в якому потрібно вставити зауваження або ACE.
deny	Опція deny не дозволяє пакету перетинати брандмауер PIX
permit	Параметр дозволу вибирає пакет для переміщення між брандмауером PIX.
protocol	Назва або номер протоколу IP. Це може бути один з: icmp, ip, tcp або udp або ціле число в діапазоні від 1 до 254, що представляє номер протоколу IP. Щоб відповідати будь-якому Інтернет-протоколу, включаючи ICMP, TCP та UDP, використовуйється слово IP.
object-group	Вказує групу об'єктів.
source-addr	Адреса мережі або хосту, з якого надходить пакет.
source-mask	Біти маски мережі (маска), які будуть застосовані до source-addr, якщо джерело-адреса призначена для маски мережі.
port	Вказує послуги, до яких дозволяється або забороняється доступ, наприклад smtp для порту 25, www для порту 80 тощо. Можна вказати порти, а буквальне ім’я або число в діапазоні від 0 до 65 535.
interface if-name	Назва інтерфейсу брандмауера
obj-grp-id	Існуюча група об'єктів.
destination-addr	IP-адреса мережі або хосту, до якого передається пакет надісланий.
destination-mask	біти маски мережі (маска), які будуть застосовані до адреси призначення, якщо файл адреса призначення - маска мережі.

Продовження Таблиці 3.2

Log disable| default| level	Якщо вказано параметр журналу, він генерує повідомлення системного журналу 106100 для ACE, до якого він застосовується. Для згенерованого може бути вказаний необов'язковий рівень системного журналу (0–7) повідомлень syslog (106100). Якщо рівень не вказано, рівень за замовчуванням становить 6 (інформаційний) для нового ACE. Якщо вказано опцію вимкнення журналу, журналювання списку доступу є повністю відключена. Якщо немає повідомлень системного журналу, включаючи повідомлення 106023, воно буде створено.
interval secs	Часовий інтервал у секундах, від 1 до 600, протягом якого потрібно генерувати повідомлення системного журналу 106100. Інтервал за замовчуванням - 300 секунд для нового ACE.

access-list id [line line-num] deny|permit {protocol | object-group prot-obj-grp-id} {source-addr source-mask} | object-group netw-grp-grp-id [operator port [port] | interface if-name | object-group service-obj-grp-id] {destination-addr destination-mask} | object-group new-obj-grp-id | [operator port [port] | object-group service-obj-grp-id]} [log [disable | default] | [level]]

Команда access-list створює потрібне правило. Створене правило застосовується за допомогою команди access-group до потрібного інтерфейсу Security Appliance. Важливо також зауважити, що на відміну від списків доступу до програмного забезпечення Cisco IOS, які використовують символи підстановки (тобто 0,0.0.255 для адреси класу C) для ідентифікації своїх мережевих масок, програмне забезпечення PIX використовує звичайну маску підмережі (тобто 255.255.255.0 для адреси класу C) під час визначення маски мережі.

Синтаксис команди access-group виглядає наступним чином:

access-group id in interface interface-name

Ідентифікатор-це той самий ідентифікатор, який був вказаний у команді access-list. Параметр імені інтерфейсу - це ім'я інтерфейсу.

asafirewall(config)# static (iside, outside) 192.168.1.10 10.1.100.10

netmask 255.255.255.255

asafirewall(config)# access-list acl-out permit tcp any host 192.168.1.10 eq www

asafirewall(config)# access-group acl-out in interface outside

Приклад дозволу підключень від інтерфейсів із нижчим рівнем безпеки до інтерфейсів із підвищеним рівнем безпеки на пристрої безпеки. Ілюструє використання команд static і access-list, щоб дозволити з'єднання від інтерфейсів нижчого рівня безпеки до інтерфейсів вищого рівня безпеки на пристрої безпеки.

Статична команда переводить 10.1.100.10 на 192.168.1.10. Команда access-list дозволяє HTTP-доступ лише до хосту 10.1.100.10 (перекладено на 192.168.1.10).

Команда access-group застосовує список доступу acl-out до зовнішнього інтерфейсу. Щоб переглянути створений список доступу, необхідно скористатися командою show id списку доступу, де id-це ім'я або номер списку доступу.

Списки доступу також можна використовувати для контролю вихідного доступу до брандмауера PIX. Список вихідного доступу обмежує користувачів від початку з'єднання з надійної мережі до менш надійної мережі; наприклад, користувачі з внутрішнього інтерфейсу отримують доступ до хостів або мереж у зовнішньому інтерфейсі. За замовчуванням вихідний доступ дозволений, тому використовується дія заборони, щоб обмежити доступ під час використання списку вихідних доступів.

Наприклад, якщо необхідно обмежити доступ користувачів внутрішнього інтерфейсу до веб-сайту за адресою 172.16.68.20 у зовнішньому інтерфейсі, можна скористатися наступними командами (це приклад обмеження доступу внутрішніх користувачів до зовнішнього веб-сервера на порту 80):

pixfirewall(config)# access-list acl-in deny tcp any host 172.16.68.20 eq www

pixfirewall(config)# access-list acl-in ppermit ip any any

pixfirewall(config)# access-group acl-in in interface inside

Ця конфігурація списку доступу дозволяє будь-якому користувачу встановлювати підключення до Всесвітньої павутини (WWW) до будь-якого пункту призначення, за винятком 172.16.68.20. Списки доступу реалізуються за допомогою команд списку доступу та груп доступу.

Ці команди використовуються замість команд conduit і outbound, які використовувалися в попередніх версіях програмного забезпечення PIX Firewall. Програмне забезпечення Pix Firewall версії 6.3 підтримує команди каналу та вихідних команд. Для перетворення файлу конфігурації PIX, що містить команди передачі та вихідні команди, у підтримуваний файл конфігурації, що містить еквівалентні команди зі списком доступу, Cisco Systems створила інструмент.

Організація та управління ACE. Досить поширеним є наявність декількох списків доступу з кількома елементами списку доступу в них на Cisco Security Appliance. Боротися з цим іноді стає важко, особливо в таких ситуаціях:

- Під час спроби визначити причину кожного ACE в списку доступу, оскільки не включено описів або коментарів для випусків програмного забезпечення раніше версії 6.3.
- При видаленні окремого ACE зі списку доступу в командному рядку на програмному забезпеченні раніше версії 6.3, що стає багатоетапним процесом.

Налаштування зауваження або коментаря дозволяє користувачаам та адміністраторам зрозуміти та ідентифікувати записи списку доступу. Cisco Security Appliances дозволяє включати коментарі щодо записів у будь-який список контролю доступу (ACL). Зауваження може містити до 100 символів і може передувати або виконувати команду списку доступу. Нижче наведено синтаксис для налаштування зауваження до списку доступу:

access-list acl-id remark text

Примітка ACL може бути розміщена до або після оператора команди списку доступу, але вона повинна бути розміщена в узгодженому положенні, щоб було зрозуміло, яке зауваження описує яку команду списку доступу. Наприклад, було б незрозуміло мати деякі зауваження перед відповідними командами списку доступу та деякі зауваження після відповідних команд списку доступу[20].

Далі наведено зразок конфігурації щодо створення коментарів для ACE.

pixfirewall(config)# access-list 115 remark allow network engineering group to telnet

pixfirewall(config)# access-list 115 permit tcp 192.168.1.0 255.255.255.224 host 10.10.100.20 telnet

pixfirewall(config)# access-list 115 remark allowsales group to login

pixfirewall(config)# access-list 115 permit tcp 192.168.3.0 255.255.255.224 host 10.10.100.12 telnet

Окрім додавання зауважень до списків доступу, версія 6.3 та пізніші додають нумерацію до елементів списку доступу. Кожен ACE та зауваження мають відповідний номер рядка. Номери рядків потім можна використовувати для вставлення або видалення елементів у будь -якому місці списку доступу. Ці номери зберігаються всередині в порядку зростання, починаючи з 1. Номери рядків завжди зберігаються в порядку зростання, з індивідуальним номером рядка для кожного ACE.

Команда show access-list показує номери рядків. Номери рядків, однак, не відображаються у конфігурації. Далі приведено зразок результату команди show access-list.

pixfirewall(config)# show access-list 115

access-list 115: 4 elements

access-list 115 line 1 remark-allow network engineering group to telnet (hitcht=0)

access-list 115 line 2 permit tcp 192.168.1.0 255.255.255.224 host 10.10.100.20 telnet (hitcht=0)

access-list 115 line 3 remark-allow sales group to login (hitcht=0)

access-list 115 line 4 permit tcp 192.168.3.0 255.255.255.224 host 10.10.100.12 (hitcht=0)

Щоб видалити зауваження зі списку доступу, просто можна скористатися такою командою:

no access-list id line line-num remark text

or

no access-list id line line-num

Обидва видаляють зауваження за вказаним номером рядка.

Групування об'єктів. Групування об’єктів дозволяє групувати такі об’єкти, як хости (сервери та клієнти), послуги та мережі, а також застосовувати до групи політики безпеки. Групування об’єктів дозволяє застосовувати правила доступу до логічних груп об’єктів.

Коли застосовується список доступу до групи об’єктів, команда впливає на всі об’єкти, визначені в групі. Групування об’єктів надає спосіб зменшити кількість правил доступу, необхідних для опису складних політик безпеки. Це в свою чергу скорочує час, витрачений на налаштування та усунення несправностей правил доступу у великих або складних мережах.

Синтаксис створення груп об’єктів такий

[no] object-group object-type grp-id

Використовуйте перший параметр, object-type, щоб визначити тип групи об’єктів, яку потрібно налаштувати. Є чотири варіанти: мережа, протокол, обслуговування, icmp-тип. Можна замінити grp-id на описову назву групи.

Тип мережевого об’єкта. Використовується для групування хостів та підмереж. Сервери та клієнтські хости можна згрупувати за функціями. Наприклад, поштові сервери, веб-сервери або групу клієнтських хостів, які мають спеціальні привілеї в мережі, можна згрупувати відповідно. Далі приведено приклад налаштування групи об'єктів:

pixfirewall(config)# object-group network web-servers

pixfirewall(config-network)#description public web servers

pixfirewall(config-network)#network-object host 192.168.1.12

pixfirewall(config-network)# network-object host 192.168.1.14

pixfirewall(config-network)#exit

pixfirewall(config)#access-list 102 permit tcp any object-group web-servers eq www

pixfirewall(config)#access-group 102 in interface outside

Під час введення команди object-group система переходить у відповідний режим підкоманди для типу об’єкта, який налаштовується. У цьому випадку можна побачити підкомандний рядок config network. Підкоманда хосту мережевого об’єкта додає хост до групи мережевих об’єктів. Опис необов’язковий, але корисно включити його.

pixfirewall(config)# object-group network mis-ftp-servers

pixfirewall(config-network)#network-object host 10.10.100.154

pixfirewall(config-network)#network-object host 10.10.100.155

pixfirewall(config-network)#network-object host 10.10.100.156

pixfirewall(config-network)#exit

Щоб відобразити налаштовану групу об’єктів, можна скористатися командою show object-group, як показано далі:

pixfirewall(config)# show object-group

object-group network web-servers

description: public web-servers

network-object host 192.168.1.12

network-object host 192.168.1.14

Тип об'єкта протоколу. Ідентифікує групу протоколів IP за допомогою ключових слів, таких як icmp, tcp, udp або ціле число в діапазоні від 1 до 254, що представляє номер протоколу IP. Синтаксис команди – протокол групи об’єктів grp-id. Щоб додати єдиний протокол до поточної групи об'єктів протоколу, можна скористатися командою протокол-об'єкт протоколу. Приклад, представлений далі, показує, як використовувати режим підкоманди протоколу групи об’єктів для створення нової групи об’єктів протоколу.

pixfirewall(config)# object-group protocol grp-citrix

pixfirewall(config-protocol)# protocol-object tcp

pixfirewall(config-protocol)# protocol-object 1494

pixfirewall(config-protocol)#exit

Тип об’єкта служби. Визначає номери портів, які можна згрупувати. Це особливо корисно, коли адміністратор здійснює керування програмою. Синтаксис для сервісного типу об’єкта такий

[no] object-group service obj-grp-id tcp | udp | tcp-udp

Як тільки обирається підкоманда service, команда port-object eq service додає один номер порту TCP або UDP до групи об’єктів служби. Команда діапазону портів-об'єктів begin service end-service додає діапазон номерів портів TCP або UDP до групи об'єктів служби. Далі приведено приклад як використовувати режим підкоманд служби групи об’єктів для створення нової групи об’єктів порту (служби).

pixfirewall(config)# object-group service mis-service tcp

pixfirewall(config-service)# port-object eq ftp

pixfirewall(config-service)# port-object range 5200 6000

pixfirewall(config-service)#exit

Групування icmp-type – необхідний для групування певних типів повідомлень ICMP. Наприклад, повідомлення ICMP ECHO-REQUEST, ECHOREPLY і DESTINATION-UNREACHABLE зі значеннями числового типу 8, 0 і 3, відповідно, можна згрупувати, як показано далі:

pixfirewall(config)# object-group icmp-type icmp-test

pixfirewall(config-icmp-type)# icmp-object 0

pixfirewall(config-icmp-type)# icmp-object 3

pixfirewall(config-icmp-type)# icmp-object 8

Вкладені групи об’єктів. Команда object-group дозволяє логічно групувати однотипні об’єкти та будувати ієрархічні групи об’єктів для структурованої конфігурації. Щоб вкласти групу об’єктів в іншу групу об’єктів, можна скористатися командою group-object:

pixfirewall(config)# object-group network web-servers

pixfirewall(config-networks)# description web servers

pixfirewall(config-networks)# network-object host 192.168.1.12

pixfirewall(config-networks)# network-object host 192.168.1.14

pixfirewall(config-networks)#exit

pixfirewall(config)# object-group network public-servers

pixfirewall(config-networks)# network-object host 192.168.1.18

pixfirewall(config-networks)# group-object web-servers

pixfirewall(config-networks)#exit

Журнал ACL. Функція реєстрації ACL дозволяє реєструвати кількість дозволів або заборон потоку протягом певного періоду часу. Потік визначається протоколом, IP-адресою джерела, портом джерела, IP-адресою призначення та портом призначення. Коли трафік дозволено або відхилено, система перевіряє, чи трафік вже в системі. Якщо ні, то генерується початкове повідомлення системного журналу з числом звернень 1. Потім створюється запис трафіку, і кількість звернень збільшується щоразу, коли трафік дозволяється або відмовляється. Синтаксис команди, що дозволяє реєструвати кількість дозволів або заборон трафіку за допомогою запису ACL, виглядає наступним чином:

access-list acl-id [log [level] [interval seconds] | [disable|default]]

Для існуючого потоку повідомлення системного журналу генерується в кінці кожного налаштованого інтервалу, щоб повідомити ненульову кількість звернень для потоку в поточному інтервалі. Після створення повідомлення системного журналу кількість звернень для потоку скидається на 0 для наступного інтервалу.

Якщо протягом інтервалу не було зафіксовано жодного звернення, потік видаляється, і повідомлення системного журналу не генерується. Велика кількість потоків може одночасно існувати в будь-який момент часу. Щоб запобігти необмеженому споживанню пам’яті та ресурсів центрального процесора (ЦП), встановлено обмеження на кількість одночасних потоків заборони. Коли буде досягнуто обмеження, новий потік заборони не буде створено, доки не закінчиться термін дії існуючих потоків заборони. Щоб вказати максимальну кількість одночасних потоків заборони, які можна створити, необхідно ввести таку команду:

access-list deny-flow-max num-of-flows

Ключове слово deny-flow-max визначає максимальну кількість одночасних заборонених потоків, які можна створити. Нові значення для цієї опції набувають чинності негайно. За замовчуванням встановлено 4096 дозволених потоків.

Коли буде досягнуто максимальна кількість потоків, генерується повідомлення системного журналу (106101). За замовчуванням це повідомлення повторюється раз на 300 секунд. Повідомлення syslog, створене для запису ACL, має такий формат:

106101: access-list <acl-id> <grant> <prot> <intf/src-ip(src-port)> ->

<intf/dst-ip(dest-port)> hit-cnt <nnn> (first hit|n-second interval)

Розширена обробка протоколів. Деякі програми вимагають спеціальної обробки функцією перевірки додатків Cisco Security Appliance. Ці типи програм зазвичай вбудовують інформацію про IP-адресу в пакет даних користувача або відкривають вторинні канали на динамічно призначених портах. Функція перевірки додатків працює з NAT, щоб допомогти визначити розташування вбудованої адресної інформації [21].

На додаток до ідентифікації вбудованої інформації адресації, функція перевірки програми відстежує сеанси для визначення номерів портів для вторинних каналів. Багато протоколів відкривають вторинні порти TCP або UDP для підвищення продуктивності. Початковий сеанс відомого порту використовується для узгодження динамічно призначених номерів портів. Функція перевірки програми відстежує ці сеанси, визначає динамічні призначення портів і дозволяє обмін даними на цих портах протягом всього конкретного сеансу. Мультимедійні програми та FTP-програми демонструють таку поведінку.

Таблиця 3.3.

Опис формату системного журналу

Поле	Опис
<grant>	Відображає, чи потік дозволено чи заборонено.
<prot>	Відображає тип протоколу: tcp, udp, icmp або номер протоколу IP.
<intf>	Відображає назву інтерфейсу (як налаштовано командою nameif) для джерело або призначення потоку, що реєструється. Це може включати логічне (віртуальні локальні мережі) інтерфейси.
<src-ip>	Відображає IP-адресу джерела зареєстрованого потоку.
<dst-ip>	Відображає IP-адресу призначення потоку, що реєструється.
<src-port>	Відображає вихідний порт зареєстрованого потоку (TCP або UDP). Для ICMP це поле дорівнює 0.
<dst-port>	Відображає порт призначення зареєстрованого потоку (TCP або UDP). Для ICMP, це поле типу icmp.
<nnn>	Відображає кількість разів, коли цей потік був дозволений або відхилений Запис ACL у налаштованому часовому інтервалі. Значення 1, коли першеДля потоку генерується повідомлення syslog.
first hit	Відображає перше повідомлення, створене для цього потоку.
n-second interval	Відображає інтервал, протягом якого накопичується кількість звернень.

3.4. Метод побудови системи автоматизованого збору та перевірки налаштувань безпеки на мережевому обладнані Cisco з метою протидії несанкціонованим втручанням

В попередніх розділах було описано головні особливості мережевого обладнання, впровадження в інфраструктуру підприємства дає мжливість нейтралізувати несанкціоновані втручання зловмисників шляхом оперативного реагування та нівелювання.

Слід зазначити, що в основу запропонованого методу захисту мереж від несанкціонованих втручань, шляхом коректного налаштування Cisco обладнання покладено найкращі тенденції, та рекомендації, що були сформовані та перевірені власне самою компанією Cisco.

Перелік обладнання, політик безпеки, рекомендацій може бути змінений, відредагований, в залежності від цілей та вимог підприємства. Тим паче, що деякі налаштування можна зробити вручну, а людський фактор ніхто не відміняє.

Для тестування було обрано бібліотеку Paramiko, що дає змогу здійснювати управління вводом та виводом «IOS shell» first_shell(), refresh shell(). При цьому було надано опис 16 розробленим функцям. Ці функції дають змогу отриматиінформацію щодо конфігурації мережевого обладнання (машрутизатор, комутатор, і т д), здійснити перевірку їх працездатності, та отримати звіт перевірки.

1 Крок. Вводиться IP адреса/логін та пароль пристрою з яким потрібно встановити з' єднання.

Рис.3.2. Форма для підключення

2 крок. Встановлюється підключення SSH

3 крок. Програма отримує перелік необхідних для функціонування налаштувань, таких як: «running-config» та «running-config all»

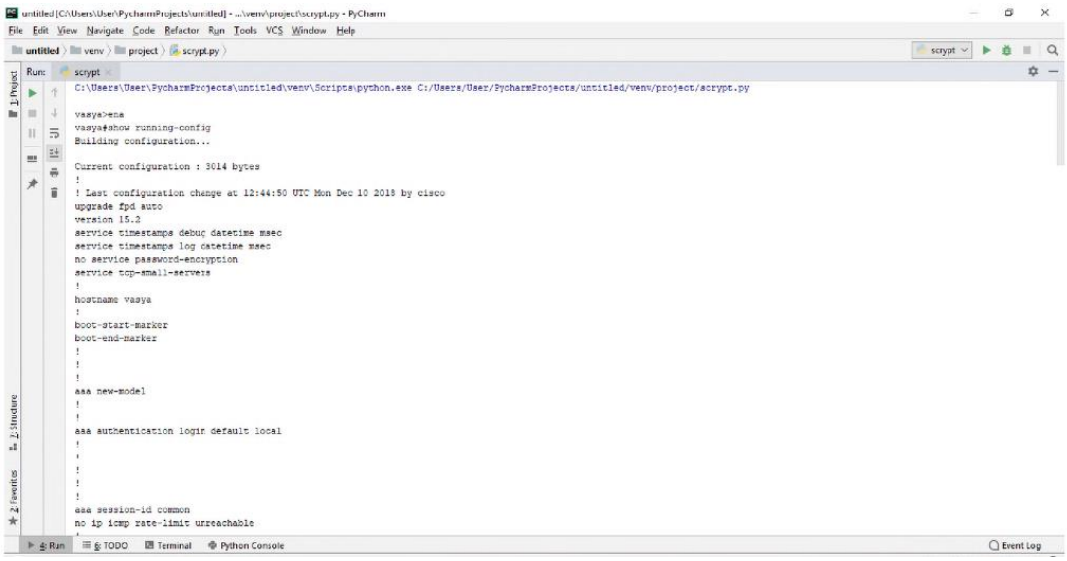

Рис.3.3. Виконання «running-config»

4 крок. Проводиться перевірка актуальних списків доступу.

5 крок. В отриманій інформації перевіряються налаштування, приведені раніше.

В ACL потрібно проаналізувати наявність «any» в двох рядках. Програма може видати після перевірки одного рядка ACL наступне:

«Informational» - може свідчити про наявну загрозу;

«Warning» - виявлено втручання, необхідно обов'язково реагувати;

«Ok» - все добре, втручань не виявлено.

Для реалізації даного алгоритму було розроблено наступні функції[23]:

1. Формується певний масив з номерами списків, які активні на одному з інтерфейсів;

2. Отримується на вході масив, та для кожного елемента ACL створюється масив рядків, та передається у наступну функцію;

3. Отримується рядок, а далі - проводиться аналіз (описаний раніше). Результат формується для адміністратора/клієнта;

4. Для виводу та перегляду результатів перевірки, конструктор формує зручний словник (базується на принципі «ключ->значення»).

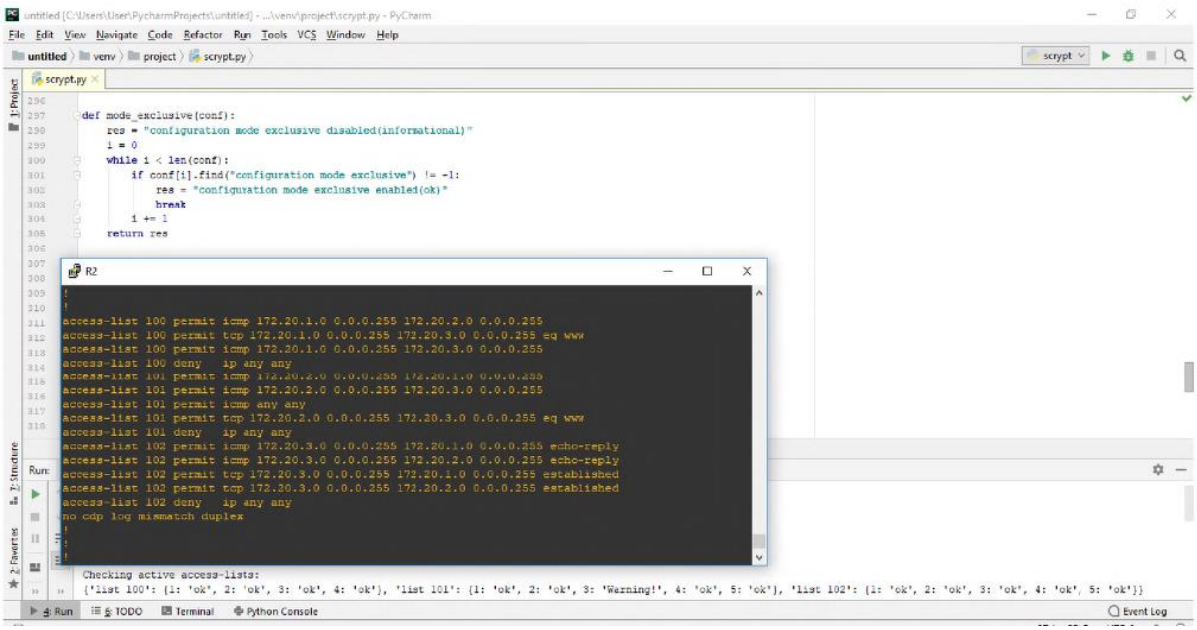

Рис.3.4. Результат аналізу ACL

Для тестування було обрано програмне забезпечення GNS3. Топологія містить один маршрутизатор R2, а також три комутатори до яких підключаються користувачі. Комп'ютер PC-l знаходиться у VLAN100, PC-2 у VLAN200, PC-3 у VLAN300. Усі комутатори працюють у режимі L2. Головним етапом тестування є перевірка налаштувань саме маршрутизатора, бо саме на ньому термінується внутрішня мережа, та саме він маршрутизує пакети між складовими мережі та VLAN. На комутаторах проводяться лише деякі перевірки за необхідністю.

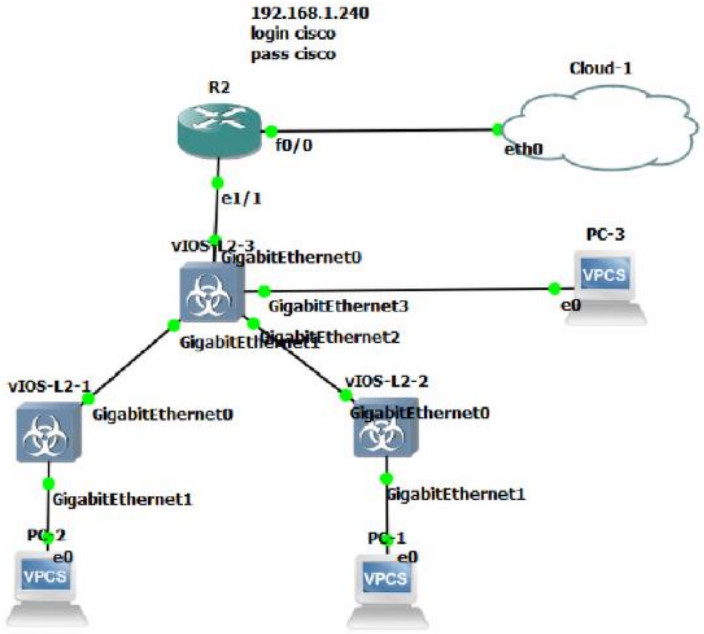

Рис.3.5. Топологія мережі для тестування

На рис.3.5 наведено результат роботи програми, щодо перевірки тестової мережі.

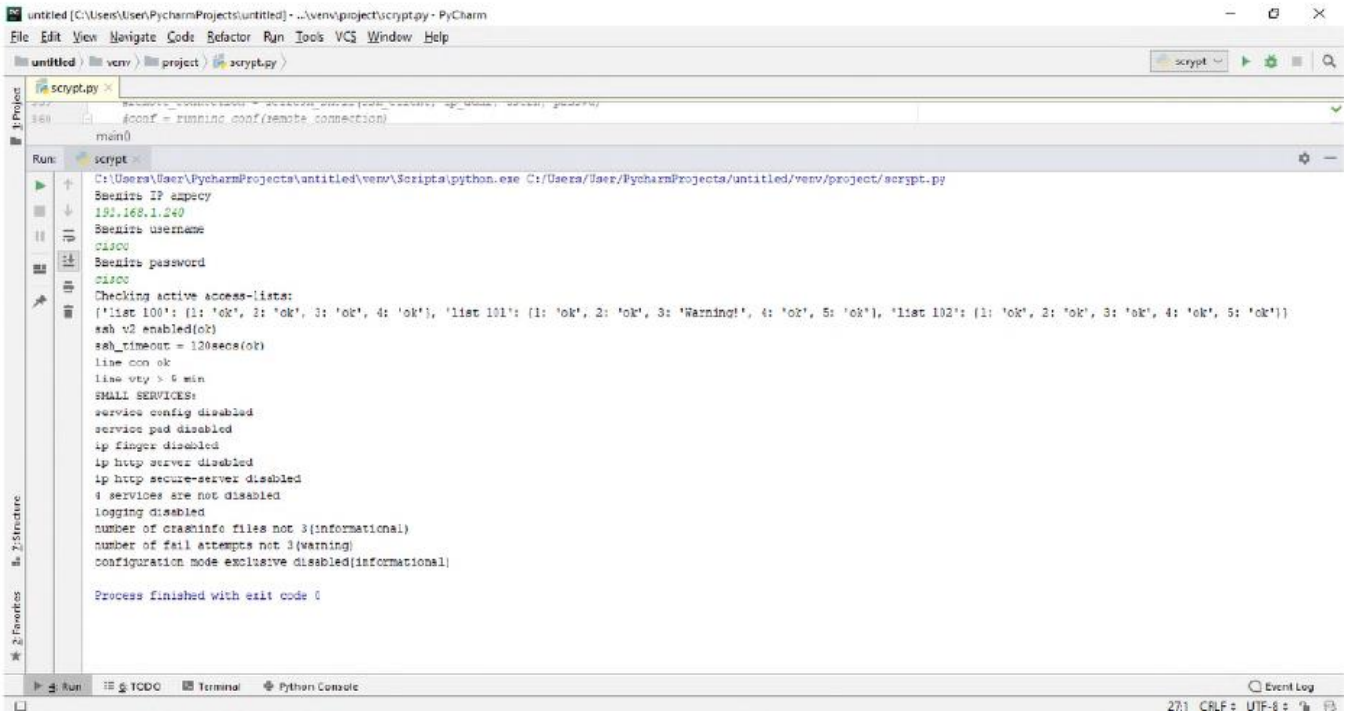

Рис.3.6. Результат тестування програми

Час тестування склав 10 сек, при цьому результат позитивний. Програма коректно реагує на всі зміни у файлах налаштувань та конфігурацій, та може бути запропонована для тестування на реальному обладнанні Cisco [24].

Висновки до третього розділу

Розроблено топологію, що ілюструє мережу середньостатистичної компанії Обрано, для проведення тестування, бібліотеку Paramiko, що дає змогу здійснювати управління вводом та виводом «IOS shell» first_shell(), refresh shell(). При цьому було надано опис 16 розробленим функцям.

Проведено тестування програмного забезпечення, при виконані якого замовник, що проводить аудит, може отримати перелік вразливих місць щодо конфігурації мережевого обладнання (машрутизатор, комутатор, і т д), здійснити перевірку їх працездатності, та отримати звіт перевірки.

Зазначено, що час тестування склав 10 сек, при цьому результат позитивний. Програма коректно реагує на всі зміни у файлах налаштувань та конфігурацій, та може бути запропонована для тестування на реальному обладнанні Cisco.

Зроблено висновок, що в основу запропонованого методу захисту мереж від несанкціонованих втручань, шляхом коректного налаштування Cisco обладнання покладено найкращі тенденції, та рекомендації, що були сформовані та перевірені власне самою компанією Cisco. Перелік обладнання, політик безпеки, рекомендацій може бути змінений, відредагований, в залежності від цілей та вимог підприємства. Тим паче, що деякі налаштування можна зробити вручну, а людський фактор ніхто не відміняє.

ВИСНОВКИ

В магістерській роботі отримано наступні теоретичні та практичні результати:

1) Проаналізовано широкий спектр рішень від Cisco, що здатні захистити інфраструктуру підприємства на будь-якому ієрархічному рівні незалежно від топології мережі. Досліджено декілька моделей безпеки, а також виокремлено головні переваги та недоліки кожної.

2) Підкреслено, що для зловмисників, які зосереджені на більш хаотично спроектованих мережах, побудовані з використанням обладнання Cisco мережі більш складні в керувані, однак відповідають всім необхідним вимогам щодо контролювання, оновлення та вирішування проблем.

3) Досліджено величезну різноманітність рішень безпеки Cisco та їх елементів. Якщо їх правильно вибрати, розгорнути, налаштувати та підтримувати, ці пристрої та програми можуть зупинити більшість несанкціонованих втручань та мережевих атак. Виокремлено, що це мета поглибленої стратегії захисту самозахисних мереж Cisco.

4) Підкреслено, що хоча постачальники послуг можуть досягти майже автоматизованого керування мережею, включаючи управління безпекою, вони ніколи не можуть бути на 100% автоматизованими. Впровадження більшої кількості пристроїв і програм для забезпечення безпеки означає, що потрібно більше знань і навичок у сфері безпеки, однак і визначає необхідність чуткого та правильного налаштування ACL.

5) Розроблено топологію, що ілюструє мережу середньостатистичної компанії Обрано, для проведення тестування, бібліотеку Paramiko, що дає змогу здійснювати управління вводом та виводом «IOS shell» first_shell(), refresh shell(). При цьому було надано опис 16 розробленим функцям.

6) Проведено тестування програмного забезпечення, при виконані якого замовник, що проводить аудит, може отримати перелік вразливих місць щодо

конфігурації мережевого обладнання (машрутизатор, комутатор, і т д), здійснити перевірку їх працездатності, та отримати звіт перевірки.

7) Зазначено, що час тестування склав 10 сек, при цьому результат позитивний. Програма коректно реагує на всі зміни у файлах налаштувань та конфігурацій, та може бути запропонована для тестування на реальному обладнанні Cisco.

8) Зроблено висновок, що в основу запропонованого методу захисту мереж від несанкціонованих втручань, шляхом коректного налаштування Cisco обладнання покладено найкращі тенденції, та рекомендації, що були сформовані та перевірені власне самою компанією Cisco.