ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Гнипа Михайла Володимировича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект підсистеми захисту периметру мережі на базі обладнання Cisco".

2. Актуальність роботи зумовлена потребою у розробці та впровадженні у практику діяльності організації захищених комп'ютерних мереж.

3. Основний зміст пояснювальної записки роботи викладено на 72 сторінках тексту, записка містить 6 таблиць, 56 ілюстрацій, 3 додатка. Список використаних літературних джерел налічує 37 найменувань. Невід'ємною складовою роботи є реалізований у середовищі моделювання GNS3 проект мережі на базі обладнання фірми Cisco.

4. Пояснювальна записка складається з реферату, вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений аналізу принципів, моделей, протоколів та технологій побудови підсистем периметрового захисту, зокрема, у розділі розглянуто: організація периметрового захисту для сучасних мереж, поняття топологій мереж, основні поняття технології Ethernet, принципи міжмережного екранування. У цьому ж розділі наведено огляд основних технологій захисту інформації в сучасних мережах.

Розділ 2 присвячений питанням проектування підсистеми периметрового захисту, зокрема, у ньому здійснено проектування топології мережі, розроблено схему адресації мережі, проведено вибір обладнання, розроблено політику інформаційної безпеки та сценарій тестування.

Розділ 3 присвячений питанням базового налагодження пристроїв мережі та питанням налагодження побудованої підсистеми периметрового захисту. Також у цьому розділі здійснено перевірку функціоналу підсистеми периметрового захисту та наведено аналіз результатів тестування.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять змодельовану схему мережі, результати моделюванням атаки на побудовану мережу, лістинги конфігураційних файлів налагоджених пристроїв.

8. Таблиці та ілюстрації оформлені якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту враховані.

11. Ставлення студента до виконання випускної кваліфікаційної роботи – дуже відповідальне.

12. У цілому при написанні випускної кваліфікаційної роботи студент Гнип М. В. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Теорія системі і системний аналіз». Також студент Гнип М. В. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити проект захищеної мережі, обрати відповідний інструментарій, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Гнипа М. В. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «відмінно».

Науковий керівник
к.т.н., завідувач кафедри КІ та КБ  А.А. Єфіменко
10 червня 2020 року

РЕЦЕНЗІЯ

на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Гнипа Михайла Володимировича
на тему: „Проект підсистеми захисту периметру мережі на базі обладнання Cisco"

Кваліфікаційна робота студента Гнипа М. В. „Проект підсистеми захисту периметру мережі на базі обладнання Cisco" присвячена актуальній тематиці – розробці та впровадженню у практику діяльності організації підсистем периметрового захисту.

Робота містить реалізований у середовищі моделювання GNS3 проект мережі на базі обладнання фірми Cisco та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, три додатки.

У першому розділі пояснювальної записки проведено аналіз принципів, моделей, протоколів та технологій побудови підсистем периметрового захисту, зокрема, у розділі розглянуто: організація периметрового захисту для сучасних мереж, поняття топологій мереж, основні поняття технології Ethernet, принципи міжмережного екранування. У цьому ж розділі наведено огляд основних технологій захисту інформації в сучасних мережах.

У другому розділі пояснювальної записки здійснено проектування підсистеми периметрового захисту, зокрема, у ньому здійснено проектування топології мережі, розроблено схему адресації мережі, проведено вибір обладнання, розроблено політику інформаційної безпеки та сценарій тестування.

У третьому розділі пояснювальної записки наведено процес базового налагодження та налагодження побудованої підсистеми периметрового захисту. Також у цьому розділі здійснено перевірку функціоналу підсистеми периметрового захисту та наведено аналіз результатів тестування.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані ґрунтовні теоретичні знання та практичні фахові навички, що отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено логічно, науково і технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що наведений у роботі, оформлений якісно і наведений у відповідних місцях. Оформлення роботи у цілому відповідає вимогам стандартів. Проект мережі реалізовано у середовищі моделювання GNS3 на базі обладнання фірми Cisco. Його функціонал відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – розроблений проект планується до впровадження в діяльності підприємства. Недоліками роботи є наступні: наявність деяких відхилень від вимог щодо оформлення пояснювальної записки (наприклад, відсутній перелік умовних скорочень, відсутні посилання на літературні джерела у розділі 1.1, неправильно підписані таблиці у розділі 2.2). Зазначені недоліки у цілому не впливають на високу якість і актуальність роботи.

У цілому кваліфікаційна робота студента Гнипа М. В. „Проект підсистеми захисту периметру мережі на базі обладнання Cisco" відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – «відмінно».

Рецензент,
декан факультету
інформаційно-комп'ютерних технологій,
канд.техн.наук, доцент Надія Лобанчикова
10 червня 2020 р.

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект підсистеми захисту периметру мережі на базі обладнання Cisco»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Гнип М. В.
Керівник, завідувач кафедри КІ та КБ, к.т.н.
_____ Єфіменко А. А.
Рецензент, декан ФІКТ, к.т.н., доцент
_____ Лобанчикова Н. М.

Житомир 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу

Студента **Гнипа Михайла Володимировича**
Тема роботи: **Проект підсистеми захисту периметру мережі на базі обладнання Cisco**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Міжмережний екран Cisco ASA серії 55xx
3. Маршрутизатори Cisco 7200
4. Комутатори Cisco 2960
5. Операційні системи Cisco IOS, Windows XP, Windows 7, Linux Debian
6. Графічний симулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	06.04.2020	06.04.2020
2	Єфіменко А. А.	20.04.2020	20.04.2020
3	Єфіменко А. А.	11.05.2020	11.05.2020

Керівник Єфіменко А. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 7 квітня 2020	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації периметрового захисту для сучасних мереж	8 квітня 2020 – 11 квітня 2020	Виконано
3	Аналіз технологій периметрового захисту на основі міжмережного екранування	12 квітня 2020 – 16 квітня 2020	Виконано
4	Аналіз можливостей мережного обладнання Cisco для організації периметрового захисту	17 квітня 2020 – 19 квітня 2020	Виконано
5	Розробка загального проекту мережі організації	20 квітня 2020 – 24 квітня 2020	Виконано
6	Проектування підсистеми периметрового захисту та вибір обладнання для її реалізації	25 квітня 2020 – 30 квітня 2020	Виконано
7	Розробка політики безпеки периметрового захисту	1 травня 2020 – 4 травня 2020	Виконано
8	Проектування та створення сценаріїв тестування функціоналу підсистеми	5 травня 2020 – 9 травня 2020	Виконано
9	Базове налагодження пристроїв мережі	10 травня 2020 – 13 травня 2020	Виконано
10	Налагодження підсистеми периметрового захисту	14 травня 2020 – 18 травня 2020	Виконано
11	Тестування роботи підсистеми периметрового захисту	19 травня 2020 – 22 травня 2020	Виконано
12	Аналіз результатів тестування	23 травня 2020 – 24 травня 2020	Виконано
13	Написання пояснювальної записки	25 травня 2020 – 29 травня 2020	Виконано
14	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 8 червня 2020	Виконано
16	Захист	13 червня 2020	Виконано

Студент _____ Гнип М. В.

Керівник _____ Єфіменко А. А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми периметрового захисту мережі та пояснювальної записки до нього. Пояснювальна записка до роботи містить 85 сторінок, 56 ілюстрацій та 6 таблиць.

Метою роботи є розробка проекту підсистеми захисту периметру мережі на базі обладнання Cisco.

В роботі визначено основні завдання на розробку підсистеми, яка забезпечить захист локальних мереж офісів від зловмисного впливу з глобальної мережі Internet. Також в роботі проаналізована організація захисного периметру мереж на базі апаратних міжмережних екранів, обґрунтовано актуальність даної системи захисту та описана сфера її використання, обґрунтований вибір виробника обладнання – Cisco. Розроблені, сформовані та налагоджені загальний проект мережі та проект підсистеми захисту. Наведено сценарій захисту від атак, загальна топологія мережі, опис конкретних серій обладнання, що будуть використані при побудові даного проекту захисту, опис політики інформаційної безпеки та тестування проекту. Також наводяться результати тестування підсистеми захисту.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, МЕРЕЖА, ПЕРИМЕТР МЕРЕЖІ, CISCO, ПІДСИСТЕМА ЗАХИСТУ ПЕРИМЕТРУ МЕРЕЖІ.

Зм.	Арк.	№ докум.	Підпис	Дата	КІК.КР.Б – 123 – 20 – ПЗ		
Розроб.		Гнип М.В.		1.10.20	Проект підсистеми захисту периметру мережі на базі обладнання Cisco	Літ.	Арк. 4 / Аркушів 105
Керівник		Єфіменко А. А.		1.10.20			
Н. Контр.		Єфіменко А. А.		10.06.20			
Рецензент.		Лобанчикова Н. М.		12.08.20	Пояснювальна записка	Державний університет «Житомирська політехніка», група КІ-2	
Зав. каф.		Єфіменко А. А.		1.10.20			

ABSTRACT

The qualification work consists of the project of the perimeter network protection subsystem and an explanatory note to it. The explanatory note to the work contains 85 pages, 56 illustrations and 6 tables.

The purpose of this work is to develop a project for a network perimeter protection subsystem based on Cisco equipment.

In work defines the main tasks for the development of a subsystem that will protect local office networks from malicious influence from the global Internet. The paper also analyzes the organization of the protective perimeter of networks based on hardware firewalls, substantiates the relevance of this protection system and describes the scope of its use, the reasonable choice of the equipment manufacturer – Cisco. A common network project and a security subsystem project were developed, formed, and set up. The scenario of protection against attacks, the general network topology, a description of specific hardware series that will be used in the construction of this protection project, a description of the information security policy and testing of the project. The results of testing the security subsystem are also provided.

KEYWORD: SECURITY, NETWORK, NETWORK PERIMETER, CISCO, NETWORK PERIMETER PROTECTION SUBSYSTEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1. ОРГАНІЗАЦІЯ ЗАХИСТУ ПЕРИМЕТРУ МЕРЕЖІ 10
1.1. Організація периметрового захисту для сучасних мереж 10
1.2. Міжмережне екранування як основа периметрового захисту 14
1.3. Можливості мережного обладнання Cisco для організації периметрового захисту 25
РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ 32
2.1. Проект мережі організації 32
2.2. Проект підсистеми периметрового захисту 40
2.3. Розробка політики безпеки периметрового захисту 44
2.4. Проект сценаріїв тестування функціоналу підсистеми 51
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ 60
3.1. Базове налагодження пристроїв мережі 60
3.2. Налагодження підсистеми периметрового захисту 65
3.3. Тестування підсистеми периметрового захисту 73
3.4. Аналіз результатів тестування 79
ВИСНОВКИ 83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 85
ДОДАТКИ 89

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List

ОС – операційна система

МЕ – міжмережний екран

OSI – Open Systems Interconnection

TCP – Transmission Control Protocol

WAN – Wide Area Network

IP – Internet Protocol

LAN – Local Area Network

MAC – Media Access Control

ДМЗ – демілітаризована зона

NAT – Network Address Translation

ASA – Adaptive Security Appliances

ВСТУП

Актуальність теми. Комунікабельність являється важливою складовою нашого життя. Залишатись завжди на зв’язку з оточуючими нам дозволяють комунікаційні технології, а зокрема Інтернет. Розвиток глобальної мережі йде стрімкими темпами і в недалекому майбутньому саме вона стане основою, якщо не монополістом усіх комунікаційних мереж. У міру втілення в життя все нових і нових ідей та проектів, які здавалися раніше недосяжними, можливості об'єднаних мереж, що утворюють Інтернет, будуть грати все більш зростаючу роль в реалізації цих проектів.

Одна з найважливіших і основних потреб людини – взаємодія з іншими людьми. На сьогоднішній день спілкування стає для нас так само важливим, як повітря, вода, їжа і дах.

У теперішньому світі, як ніколи, нас зв’язує один з одним використання мереж. Щоб втілити свої ідеї в життя, ми просто і легко можемо миттєво зв’язуватися з іншими людьми та ділитися ними. Новини та відкриття стають відомими у всьому світі в лічені секунди. Вихід в мережу і гра з іншими людьми, що знаходяться на інших континентах – лише забавка, що стала доступною завдяки комунікаціям.

Але з приходом новітніх технологій в комунікаціях почали з’являтись зловмисники. Їх метою є перехоплення чи пошкодження конфіденційної інформації, яка, в свою чергу, може бути як особистою, так і корпоративною. Тобто це можуть бути особисті фото, відео, файли документообігу чи таємні листування керівних структур. Звісно, це все робиться з метою матеріальної вигоди.

Актуальність обраної теми полягає в тому, що захист мережі зменшить, а в ідеальному випадку нейтралізує даний злочинний вплив. Функціональні можливості підсистеми захисту інформації дозволять використовувати її у відповідності до поставлених задач.

Метою кваліфікаційної роботи є розробка проекту підсистеми захисту периметру мережі на базі обладнання Cisco.

Встановлена мета обумовлює наступні завдання:

– аналіз основних підходів периметрового захисту сучасних мереж;
– розробка політики інформаційної безпеки мережі;
– вибір засобів реалізації підсистеми;
– вибір сучасного технічного забезпечення системи;
– розробка системи комунікацій, придатної для розширення надалі;
– реалізація підсистеми захисту мережі.

Об’єктом дослідження є процес захисту локальних мереж від зловмисних дій з зовнішньої мережі Internet.

Предметом дослідження є методи і засоби використання міжмережного захисту для захисту локальних мереж.

В процесі виконання кваліфікаційної роботи був розроблений проект підсистеми периметрового захисту мережі. При цьому були використані екрануючі маршрутизатори та МЕ експертного рівня.

РОЗДІЛ 1. ОРГАНІЗАЦІЯ ЗАХИСТУ ПЕРИМЕТРУ МЕРЕЖІ

1.1. Організація периметрового захисту для сучасних мереж

Інформаційний обмін в сучасному світі є невід’ємною складовою нашого життя. Зараз неможливо уявити світ без електронної пошти, спілкування в режимі «онлайн» чи інтернет-магазинів. Будь-який карантинний стан супроводжується тим, що компанії відправляють своїх працівників працювати віддалено – за допомогою мережі Інтернет. Все це сприяє тому, що кількість інформації в глобальній мережі з кожним днем лише збільшується. Інформація оточує нас завжди та всюди, більшість її – конфіденційна. Як і в будь-якій сфері діяльності, якщо є щось особисте, то є і той, хто хоче це поцупити. Тому перед системними адміністраторами постійно важливим питанням є захист мережі від інформаційних крадіїв – хакерів. За даними провідних аналітичних агентств, число інцидентів, пов’язаних з інформаційною безпекою, постійно зростає. Відповідальні за захист інформації фахівці відзначають зріст активності зовнішніх зловмисників, що використовують останні розробки в області нападу. Цим вони прагнуть проникнути в корпоративні мережі.

В наш час значного розвитку здобули технології електронних платежів і «безпаперового» документообігу, тому будь-який збій мережі може спричинити порушення в роботі банків і цілих корпорацій, що призводить до великих матеріальних збитків. Вони ж, в свою чергу, є відчутними як для підприємства, так і для його клієнтів. Щоб запобігти цьому потрібно організувати захист інформації в мережі.

Обов'язковим елементом системи інформаційної безпеки організації є захист периметра мережі. В сучасних реаліях, коли працівник компанії може працювати в будь-який момент часу із будь-якої точки світу з будь-якого пристрою, а обчислення переходять в так звані «хмари» – досить важко встановити чіткий периметр корпоративної мережі. Однак ще досить довгий час будова локальних мереж буде подібна до фортеці: є внутрішня частина з своїми

правилами, та точки, що мають вихід до глобальної мережі, а отже – утворюють зовнішній периметр локальної мережі. Подібно до стін фортеці, ці точки мають бути захищеними і захищати внутрішню мережу від вторгнення. Мінімізація зовнішніх загроз досягається шляхом впровадження багаторівневої системи захисту інформації, і в першу чергу на зовнішньому кордоні мережі. Важливим завданням системи захисту периметра є розділення мережі на внутрішню і зовнішню області.

Розглядаючи проблему захисту інформації в мережі насамперед розглядають питання класифікації порушень роботи мережі та прав доступу, які можуть призвести до знищення чи небажаної модифікації даних. До потенційних загроз належать:

– порушення роботи обладнання;
– втрата інформації із-за некоректної роботи програмного забезпечення;
– втрата інформації, що пов’язана з несанкціонованим доступом;
– втрата інформації, що пов’язана з неправильним зберіганням архівних даних;
– помилки обслуговуючого персоналу і користувачів.

Розглядають два види несанкціонованого доступу до інформації, що знаходиться в мережі: з фізичним доступом до елементів мережі та без нього. При фізичному доступі зловмисник використовує пряме підключення до пристрою, що знаходиться в мережі. Далі, в залежності від його намірів, проводяться атаки, які спрямовані на непрацездатність мережі, парольні атаки, безпосередній доступ до пакетів, що передаються мережею, атаки на рівні додатків, збір інформації про мережу тощо. Коли ж фізичного доступу немає, вищевказані дії проводяться віддалено, через мережу Інтернет.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Вони, в свою чергу, мають відповідати основоположним принципам інформаційної безпеки. Цими трьома принципами є конфіденційність, цілісність і доступність. Вони забезпечують цілеспрямованість та дозволяють експертам з кібербезпеки визначити пріоритетність дій для захисту будь-якої мережевої системи.

Конфіденційність інформації запобігає її розкриттю неавторизованим людям, ресурсам або процесам. Цілісність – позначає їх точність, достовірність, узгодженість між відправником та отримувачем. Нарешті, доступність гарантує, що інформація буде доступна авторизованим користувачам у разі потреби.

Види захисту інформації, в залежності від можливих видів порушень роботи мережі чи несанкціонованого доступу, об’єднуються в два основні класи:

– технічні засоби;
– програмні засоби.

Технічні засоби захисту являють собою електричні, електромеханічні, електронні та інші типи пристроїв. Їх основні переваги – це надійність, незалежність від суб’єктивних факторів та висока стійкість до модифікації. Але є і недоліки. Перший з них – недостатня адаптивність до тієї чи іншої ситуації. Це зменшує зону їх використання до тих мереж, які є консервативними, а отже не будуть модернізуватись та збільшуватись. До фізичних недоліків можна віднести великий об’єм та масу. Наслідком цього є проблема транспортування даного обладнання. Вирішальним фактором не на користь технічних засобів у більшості невеликих фірм і підприємств – є висока ціна їх закупівлі.

Типовим прикладом технічних засобів є апаратні пристрої, що сполучаються чи вбудовуються безпосередньо в апаратуру локальних мереж. Також до технічних засобів захисту можна віднести охоронні сигналізації, замки на дверях, віконні ґрати тощо – те, що захищає від фізичного доступу до мережі.

Для захисту окремих комп’ютерів використовують програмні засоби захисту. Вони являють собою програми, що призначені для виконання функцій, пов’язаних з захистом інформації. На відміну від технічних засобів, програмні є більш універсальними та гнучкими у використанні. Також до переваг відносять поширеність, доступність, надійність, простоту встановлення, здатність до модифікації та розвитку. Але використання частини ресурсів об’єкта захисту, залежність від технічних характеристик та висока чутливість до змін є явними недоліками такого типу захисту.

Програмні засоби захисту поділяють на:

– засоби архівації даних;
– антивірусні програми;
– криптографічні програми;
– засоби ідентифікації і автентифікації користувачів;
– засоби керування доступом;
– протоколювання та аудит.

Зараз розробники операційних систем (ОС) приділяють значну увагу захисту своїх користувачів. Тому більшість з цих програмних засобів вже вбудовані в сучасні ОС. На практиці вони не завжди можуть вирішити виникаючі проблеми, тому, зазвичай, використовують спеціалізовані програмні засоби. Розробники останніх, на відміну від розробників ОС, спеціалізуються в питанні безпеки, а не функціонуванні комп'ютера в цілому.

Однак слід зазначити, що розподіл на програмні та технічні засоби захисту є досить умовним. Сучасні технології розвиваються в напрямку поєднання цих засобів з метою підвищення захисту. Такі програмно-апаратні засоби отримали найбільшого поширення в галузі контролю доступу, захисту від вірусів тощо. До їх переваг і недоліків одночасно можна віднести проміжні властивості цих засобів.

Також до засобів захисту відносять організаційні, які, в свою чергу, розділяють на організаційно-технічні (підготовка приміщень, прокладка кабельної системи з обмеженим доступом до неї тощо) та організаційно-правові (правила роботи підприємства та національні законодавства). Організаційно-технічні заходи зазвичай проводяться на етапі проектування мережі. До переваг даних засобів відносять необмежені можливості модифікації та розвитку, до недоліків – високу залежність від дотримання норм і правил, що є суб'єктивним чинником.

Фахівці даної галузі вже досить давно прийшли до висновку, що використання будь-якого з вищезазначених засобів захисту не забезпечує повністю надійного збереження інформації локальних мереж. Вони

рекомендують використовувати комплексний підхід до використання та розвитку всіх засобів і способів захисту інформації. Це підтверджується тим, що окремі сфери діяльності пов’язані з банківською справою чи системою державного управління вимагають більш спеціалізованих заходів безпеки даних і висувають підвищені вимоги до надійності функціонування та захисту мереж, відповідно до характеру і важливості вирішуваних ними задач.

Правильний і повноцінний захист периметра корпоративних мереж дозволяє домогтися захищеності доступу внутрішніх користувачів в зовнішні мережі, надає доступ з зовнішніх мереж до публічних корпоративних ресурсів, захищає від мережевих атак на корпоративні ресурси, організовує системи електронної комерції, створює єдину точку антивірусної і антиспам фільтрації, запобігає витоку конфіденційної інформації, проводить моніторинг та аналіз подій інформаційної безпеки.

1.2. Міжмережне екранування як основа периметрового захисту

Для захисту комп’ютерів в локальній мережі потрібна система аналізу трафіку з використанням системи правил і блокування доступу (за так званим «чорним списком»). Така система отримала назву «міжмережного екрану», хоча досі в різних публікаціях можна зустріти і більш ранні терміни – «брандмауер» або ж «фаєрвол». В сучасному світі це одним з найпоширеніших методів захисту локальних мереж.

В міжмережному екрані (МЕ), як правило, реалізуються механізми безпеки, які роблять даний пристрій безпечним і керованим. До цих механізмів відносять:

– аналіз даних, що проходять через нього;
– контроль комунікаційного середовища і партнерів з обміну даними;
– регламентування обміну даними відповідно до політики безпеки;
– реєстрація подій, що мають відношення до безпеки.

Класичним варіантом розміщення МЕ є його встановлення між внутрішньою та глобальною мережею, хоча іноді МЕ також можуть використовувати і для захисту від «нападів» із корпоративної мережі, до якої підключена локальна мережа підприємства. МЕ, у випадку його застосування, є єдиною загальною точкою обміну даними кожного вузла мережі із потенціально ворожою зовнішньою мережею і використовується між ними як захисний бар'єр. Сам МЕ відкритий для доступу ззовні, а мережа за ним – вже захищена. Таким чином, всі дані між мережами проходять безпосередньо через МЕ [1].

Для більшості організацій встановлення МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі.

Організаційно МЕ входить до складу мережі, що захищається, тому до його захисту також висуваються жорсткі вимоги:

– фізичний захист доступу до МЕ;

– наявність засобів захисту від завантаження ОС МЕ з несанкціонованого носія;

– наявність засобів захисту на рівні ОС, що розмежовують доступ до ресурсів системи;

– ОС МЕ повинна забороняти привілейований доступ до своїх ресурсів з внутрішньої мережі;

– ОС повинна містити засоби моніторингу/аудиту будь-яких адміністративних дій;

– на МЕ не дозволяється мати ніяких розділів користувачів.

До сьогодні не існує єдиної загальновизнаної класифікації МЕ. Так, за функціонуванням на рівнях моделі OSI (Open systems interconnection) МЕ можна поділити на 4 типи:

– МЕ з пакетною фільтрацією або екрануючі маршрутизатори;

– шлюзи сеансового рівня чи рівня з'єднання;

– шлюзи прикладного рівня;

– МЕ експертного рівня.

Пакетні фільтри сьогодні найчастіше реалізовані екрануючими маршрутизаторами, що з'єднують внутрішню і зовнішні мережі. У цьому

випадку, весь захист концентрується в найбільш вразливому місці – на кордоні інтранету, що знаходиться в технічному та адміністративному віданні компанії, і зовнішньої мережі, що належить організації, що надає транспортні послуги. Фільтрація інформаційних потоків полягає в їх вибірковому пропущенні через МЕ, можливо, з виконанням деяких перетворень. Фільтрація здійснюється на основі набору попередньо завантажених в МЕ правил, відповідно до прийнятої політики безпеки. Тому МЕ зручно представляти як послідовність фільтрів, що обробляють інформаційний потік.

Основу фільтрації пакетів виконують списки керування доступом (Access Control List – ACL). Це список прав доступу до об’єкта, що визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом [3]. Трафік, що надходить до фільтруючого маршрутизатора, порівнюється з записами ACL на основі порядку, в якому ці записи були утворені в маршрутизаторі. Нові складові додаються до кінця списку. Маршрутизатор продовжує шукати, поки не знайде збіг. Якщо збіги не будуть знайдені, коли фільтруючий маршрутизатор досягне кінця списку, трафік буде заборонений. В даному випадку мається на увазі заборона всього трафіку, який не дозволений. ACL з лише одним забороннім записом має ефект заборони всього трафіку, тому потрібно мати хоча б один запис дозволу. У випадку використання дозволу всього трафіку, що не заборонений процес обробки повністю аналогічний, але зі зворотнім ефектом [4].

Володіючи рядом позитивних якостей, пакетні фільтри не позбавлені серйозних недоліків. Вони не забезпечують високого ступеня безпеки, так як перевіряють тільки заголовки пакетів і не підтримують багато необхідних функцій захисту, наприклад автентифікацію кінцевих вузлів, криптографічне закриття пакетів повідомлень, а також перевірку їх цілісності та автентичності. Пакетні фільтри уразливі для таких поширених мережевих атак, як підміна вихідних адрес і несанкціонована зміна вмісту пакетів повідомлення. Однак такі переваги пакетних фільтрів, як простота реалізації, висока продуктивність, прозорість для програмних додатків і мала ціна, обумовлена тим, що будь-який

маршрутизатор в тій чи іншій мірі надає можливість фільтрації пакетів, переважують зазначені недоліки пакетних фільтрів і обумовлюють їх повсюдне поширення і використання як обов'язкового елемента системи мережевої безпеки. Крім того, вони є складовою частиною практично всіх МЕ, що використовують контроль стану.

Шлюз сеансового рівня або ж екрануючий транспорт – це технологія, яка використовується в МЕ, і полягає в тому, що шлюз виключає пряму взаємодію двох вузлів на сеансовому рівні моделі OSI. Його функціонування охоплює в процесі своєї роботи також транспортний і мережевий рівні еталонної моделі. Захисні функції шлюзу сеансового рівня відносяться до функцій посередництва (проксі-сервера). Він перехоплює всі запити одного вузла на доступ до іншого і, встановлює з'єднання після перевірки допустимості таких запитів. Потім шлюз сеансового рівня копіює пакети, що передаються в рамках однієї сесії між двома вузлами, не здійснюючи додаткової фільтрації. Як тільки авторизоване з'єднання встановлено, шлюз поміщає в спеціальну таблицю з'єднань адреси відправника і одержувача, стан з'єднання, інформацію про номер послідовності тощо. Як тільки сеанс зв'язку завершується, запис про нього видаляється з цієї таблиці. Всі наступні пакети, які можуть бути сформовані зловмисником відкидаються.

Такий контроль ґрунтується на інформації, що міститься в заголовках пакетів сеансового рівня протоколу TCP. Однак якщо пакетний фільтр при аналізі TCP-заголовків перевіряє тільки номери портів джерела і одержувача, то екрануючий транспорт аналізує інші поля, що відносяться до процесу підтвердження зв'язку.

Недоліки у шлюзу сеансового рівня ті самі, що й у екрануючих маршрутизаторів. На практиці більшість шлюзів сеансового рівня не є самостійними продуктами, а поставляються в комплекті зі шлюзами прикладного рівня.

Екрануючі шлюзи або ж шлюзи прикладного рівня функціонують на прикладному рівні моделі OSI, охоплюючи також рівень представлення, і забезпечує найбільш надійний захист міжмережних взаємодій. Захисні функції

прикладного шлюзу, як і шлюзу сеансового рівня, відносяться до функцій посередництва. Вони використовуються для аналізу пакетів, що приходять ззовні на його WAN-інтерфейс, у відповідності до встановлених політик безпеки. МЕ цього типу, що представляє собою, як правило, універсальний комп'ютер, на якому функціонують екрануючі агенти, інтерпретують протоколи прикладного рівня. Ці програми є резидентними і забороняють безпосередню передачу пакетів повідомлень між зовнішньою і внутрішньою мережею.

При необхідності доступу з внутрішньої мережі в зовнішню мережу або навпаки спочатку має бути встановлено логічне з'єднання з програмою-посередником, що функціонує на комп'ютері МЕ. Програма-посередник перевіряє допустимість запиту міжмережної взаємодії і при його вирішенні сама встановлює окреме з'єднання з необхідним комп'ютером. Таким чином, між клієнтом і сервером утворюються 2 з'єднання: від клієнта до МЕ і від МЕ до місця призначення. Далі обмін інформацією між комп'ютерами внутрішньої і зовнішньої мережі здійснюється через програмного посередника, який може виконувати фільтрацію потоку повідомлень, а також здійснювати інші захисні функції. Тим самим, МЕ «ховає» внутрішню мережу від зовнішнього світу і здійснює посередницьку функцію між двома вузлами, виключаючи їх безпосередню взаємодію, але дозволяючи проникати в контекст переданого трафіку, так як функціонує на прикладному рівні.

Слід мати на увазі, що МЕ може виконувати функції фільтрації без застосування програм-посередників, забезпечуючи прозору взаємодію між внутрішньою і зовнішньою мережею. Разом з тим програмні посередники можуть і не здійснювати фільтрацію потоку повідомлень.

Шлюз прикладного рівня володіє важливими перевагами. Зокрема, забезпеченням високого рівня захисту локальної мережі завдяки можливості виконання більшості функцій посередництва та захистом на рівні додатків, що дозволяє здійснювати велику кількість додаткових перевірок, зменшуючи тим самим ймовірність проведення успішних атак, можливих через недоліки програмного забезпечення. Також до переваг варто віднести і те, що при

порушенні його дієздатності блокується наскрізне проходження пакетів між мережами, що діляться, в результаті чого безпека мережі, що захищається, не знижується через виникнення відмов.

До недоліків прикладного шлюзу відносять високі вимоги до продуктивності і ресурсоємності комп'ютерної платформи, а також відсутність "прозорості" для користувачів і зниження пропускної здатності при реалізації міжмережних взаємодій.

МЕ експертного рівня (експертні МЕ) відстежують стан мережевих з'єднань при фільтрації пакетів. Їх також називають «інспекторами стану». Цей термін був введений, щоб підкреслити відмінність їх технологій від інших, що застосовуються в міжмережному екрануванні. Експертні МЕ оперують на сеансовому рівні, але "розуміють" і протоколи прикладного рівня.

Ці МЕ поєднують в собі елементи всіх трьох описаних вище категорій. Як і МЕ з фільтрацією пакетів, вони працюють на мережевому рівні моделі OSI, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес і номерів портів. Експертні МЕ також виконують функції шлюзу сеансового рівня, визначаючи, чи відносяться пакети до відповідного сеансу. І, нарешті, вони беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета відповідно до політики безпеки, виробленої в конкретній організації.

Крім статичної фільтрації пакетів експертні МЕ спостерігають за з'єднаннями в таблиці станів, яка відстежує інформацію до завершення з'єднання або після закінчення попередньо заданого тайм-ауту. Стан характеризує поточний статус даного сеансу з'єднання і залежить від програми, що обслуговує сеанс зв'язку і протоколу, використовуваного для обміну між сторонами. Це визначається тим, що багато виробників МЕ по-різному розуміють технологію експертного контролю.

Перевагою МЕ експертного рівня є прозорість для кінцевого користувача, що не вимагає додаткового налаштування або зміни конфігурації клієнтського програмного забезпечення. Крім прозорості для користувачів і більш високій швидкості обробки інформаційних потоків, до переваг МЕ експертного рівня

відноситься також те, що ці МЕ не змінюють IP-адрес пакетів, що проходять через них. Це означає, що будь-який протокол прикладного рівня, що використовує IP-адреси, буде коректно працювати з цими МЕ без будь-яких змін або спеціального програмування.

Оскільки дані МЕ допускають пряме з'єднання між авторизованим клієнтом і комп'ютером зовнішньої мережі, вони забезпечують менш високий рівень захисту. Тому на практиці технологія фільтрації експертного рівня використовується для підвищення ефективності функціонування комплексних МЕ.

Також варто згадати про персональні МЕ. Вони призначені для захисту комп'ютерів домашніх користувачів, робочих станцій співробітників або серверів, що знаходяться поза захищених сегментів внутрішньої мережі. Функції персональних МЕ аналогічні розглянутим раніше, проте деякі можливості у них не передбачені, наприклад централізоване управління або розсилка правил політики безпеки. Деякі захисні функції можуть бути додатково інтегровані в персональні МЕ, наприклад вбудована підтримка захищених віртуальних мереж, виявлення атак або антивірусний захист. Цей вид МЕ дозволяє далі розширювати захист, допускаючи управління по тому, які типи системних функцій або процесів мають доступ до ресурсів внутрішньої мережі.

Якщо ж розглядати захист всередині мережі, то деяку роль МЕ можуть також відігравати екрануючі концетратори (мости, комутатори). Вони є не стільки засобом розмежування доступу, скільки оптимізації роботи внутрішньої мережі за рахунок організації так званих віртуальних локальних мереж – Virtual LAN і використовуються для міжмережного екранування всередині внутрішньої мережі. Комутатори дозволяють здійснювати фільтрацію трафіку на основі MAC-адрес, що містяться у фреймах, які намагаються отримати доступ до певного порту комутатора. Однак практично всі сучасні мережеві карти дозволяють програмно змінювати їх MAC-адреси, що призводить до неефективності такого методу фільтрації. Тому в якості ознаки фільтрації можуть бути використані інші параметри. Наприклад, в комутаторах

розмежовується трафік. Більш досконалі комутатори можуть функціонувати на більш високих рівнях моделі TCP/IP.

Крім виконання фільтрації трафіку і функцій посередництва деякі МЕ дозволяють реалізовувати інші, не менш важливі функції, без яких забезпечення захисту периметра внутрішньої мережі було б неповним.

Легкість адміністрування є одним з ключових аспектів при створенні ефективної і надійної системи захисту. Помилки при визначенні правил доступу можуть утворити лазівку, через яку рано чи пізно буде зламана система. Тому в більшості МЕ реалізовані сервісні утиліти, що полегшують введення, видалення і перегляд набору правил. Наявність цих утиліт дозволяє також проводити перевірки на синтаксичні або логічні помилки при введенні або редагуванні правил. Зазвичай ці утиліти дозволяють переглядати інформацію, згруповану за якими-небудь критеріями, наприклад все, що відноситься до конкретного користувача або сервісу. При виконанні централізованого адміністрування слід подбати про захист інформації від пасивного і активного прослуховування мережі.

Найкращою практикою є адміністрування МЕ тільки з локального термінала. Але в повсякденному житті часто потрібна деяка форма віддаленого доступу для виконання деяких операцій з його адміністрування. Тоді віддалений доступ до МЕ по небезпечним мережам повинен здійснюватися з використанням посиленої автентифікації, такий як одноразові паролі і смарт-карти. Крім того, для запобігання перехоплення сеансів має використовуватися наскрізне шифрування всього трафіку віддаленого з'єднання з МЕ. Єдиними зареєстрованими користувачами на МЕ можуть бути тільки адміністратор МЕ і адміністратор архівних копій. Будь-яка модифікація системних програм на МЕ повинна здійснюватися ними з дозволу відповідального за мережні сервіси.

Для забезпечення можливості відновлення після збою або стихійного лиха МЕ, як і будь-який інший мережний хост, повинен мати політику створення архівних копій. Для МЕ (його системних програм, конфігураційних файлів, баз даних і т. д.) повинні створюватися щоденні, щотижневі і щомісячні архівні копії.

Архівні копії повинні зберігатися в безпечному місці на носії, з якого можна тільки зчитувати інформацію лише відповідним співробітникам, щоб їх випадково не загубили. Іншою альтернативою буде мати резервний МЕ, налаштований як основний, і підтримуваний в холодному резерві, щоб у разі збою основного, запасний міг бути включений і використаний замість нього, поки основний МЕ відновлюється.

Для адміністрування своєї доменної зони Domain Name System (DNS) багато організацій використовують послуги третьої організації, такої як провайдера Інтернету. У цьому випадку МЕ може використовуватися як кешуючий сервер DNS для поліпшення продуктивності. Якщо організація вирішила мати свою базу даних DNS, МЕ може функціонувати і як DNS-сервер (основний, вторинний, кеширующий). Тоді він може бути налаштований так, що буде приховувати інформацію про внутрішні хостах мережі. При цьому внутрішні хости отримують повну інформацію про внутрішні і зовнішні дані DNS, а зовнішні хости не мають доступу до інформації про внутрішні машини. Для зовнішнього світу всі з'єднання з будь-яким хостом внутрішньої мережі здаються вихідними від МЕ.

Однією з функцій забезпечення захисту є проектування демілітаризованої зони. Демілітаризованою зоною (ДМЗ) називають частину мережі, яка не є повністю надійною, так як до неї є доступ із зовнішнього середовища. Зазвичай, до загальнодоступних сервісів, що розміщуються в ДМЗ, відносять сервери, що фізично розміщені у локальній мережі та при цьому мають відповідати на запити зовнішньої мережі [10]. Для додаткового захисту зв’язок між серверами у ДМЗ також обмежується. Окрім основних функцій МЕ, у випадку використання ДМЗ, має також контролювати доступ до неї з зовнішньої та внутрішньої мережі.

Існує два основних варіанта архітектури мережі з ДМЗ. Перша – з використанням одного МЕ. При цьому МЕ має підключення до локальної мережі, ДМЗ та Інтернету за допомогою трьох окремих інтерфейсів. Дана схема є вразливою при відмові МЕ, так як він є «єдиною точкою відмови», та при його зломі – пряме з’єднання з внутрішньою мережею.

Друга схема використовує два МЕ, де ДМЗ розміщується між ними. Цей підхід є більш безпечним за рахунок контролю доступу з різних мереж окремими пристроями. Для досягнення кращої системи захисту рекомендується використовувати МЕ різних виробників та архітектур – це зменшує вірогідність наявності однакової вразливості.

Перш ніж користувачеві буде надано право отримати дозвіл на користування тим чи іншим сервісом, необхідно переконатися, що він дійсно той, за кого себе видає (передбачається, що цей сервіс для даного користувача дозволений). Ідентифікацію та автентифікацію користувачів на МЕ забезпечує система виявлення вторгнень (Intrusion Detection System – IDS). Вона забезпечує додатковий рівень захисту комп'ютерних систем. При отриманні запиту на використання сервісу від імені будь-якого користувача МЕ перевіряє, який спосіб автентифікації визначений для даного користувача, і передає управління серверу автентифікації. Після отримання позитивної відповіді МЕ формує запитуване користувачем з'єднання. МЕ, до складу яких входять проксі-сервери, забезпечують автентифікацію по імені/паролю (це найгірший варіант, так як ця інформація може бути перехоплена або отримана шляхом підглядання за її введенням тощо), одноразовими паролями і електронними сертифікатами. Але найчастіше використовують шифрування з відкритими ключами. Ряд МЕ підтримують систему Kerberos – один з найбільш поширених методів автентифікації. Більш просунуті системи виявлення вторгнень здатні не тільки виявляти вторгнення, але й сповіщувати про це. Також є активні системи, що відомі як системи запобігання вторгнень (Intrusion Prevention System – IPS). Вони здатні реагувати на загрозу, скидаючи з'єднання чи переналаштовуючи МЕ для блокування трафіку від злодія.

Проводити захист периметру мережі шляхом заміни IP-адрес МЕ дозволяє механізм трансляції мережевих адрес (Network Address Translation – NAT). Цей механізм дозволяє заощадити IP-адреси, транслюючи кілька внутрішніх IP-адрес в одну зовнішню публічну IP-адресу (або в кілька, але меншою кількістю, ніж внутрішніх). За таким принципом побудовано більшість мереж в світі: на

невеликий район домашньої мережі місцевого провайдера або на офіс виділяється одна публічна (зовнішня) IP-адреса, за якою працюють і отримують доступ інтерфейси з приватними (внутрішніми) IP-адресами [12].

Також NAT дозволяє запобігти або обмежити звернення зовні до внутрішніх хостів, залишаючи можливість звернення зсередини назовні. При ініціації з'єднання зсередини мережі створюється трансляція. Відповідні пакети, що надходять зовні, відповідають створеній трансляції і тому пропускаються. Якщо для пакетів, що надходять зовні, відповідної трансляції не існує (а вона може бути створеною при ініціації з'єднання або статичної), вони не пропускаються.

Ще одною перевагою даного механізму є приховування певних внутрішніх сервісів внутрішніх хостів/серверів. Фактично, виконується та ж зазначена вище трансляція на певний порт, але з можливістю підмінити внутрішній порт офіційно зареєстрованої служби (наприклад, 80-й порт TCP (HTTP-сервер) на зовнішній 54055-й). Наслідком цього є підвищення безпеки і приховування «непублічних» ресурсів.

Останньою розповсюдженою функцією МЕ є створення журналів подій або ж журналювання. Воно є важливою функцією адміністрування, що дозволяє реєструвати інформацію про всі події: відмови, вхідні та вихідні з'єднання, число переданих байт, що використовувалися сервісами, час з'єднання тощо. Всі ці дані накопичуються в файлах статистики. Багато МЕ дозволяють гнучко визначати чи підлягають журналюванню події, описувати порядок локального і віддаленого оповіщення і дій при атаках або спробах несанкціонованого доступу. В залежності від ПЗ МЕ може по-різному сповіщувати про ті чи інші дії. Серед них, наприклад, повідомлення на консоль, поштове повідомлення або SMS на мобільний телефон адміністратору системи тощо. Негайне виведення повідомлення про спробу злому може допомогти адміністратору в разі, якщо спроба виявилася успішною і атакуючий вже проник в систему. До складу багатьох МЕ входять генератори звітів, що дозволяють не тільки зібрати статистику по використанню ресурсів конкретними користувачами, по

використанню сервісів, відмов, джерел, з яких проводилися спроби несанкціонованого доступу тощо, а й обробити їх.

1.3. Можливості мережного обладнання Cisco для організації периметрового захисту

В останні роки значно зріс інтерес до програмно-апаратних рішень, які поступово витісняють виключно програмні системи. Широке поширення стали отримувати спеціалізовані програмно-апаратні рішення, що звуться security appliance. До переваг таких рішень можна віднести такі:

– Простота впровадження в технологію обробки інформації. Такі засоби поставляються із заздалегідь встановленою і налаштованою ОС і захисними механізмами, тому необхідно тільки підключити їх до мережі, що виконується протягом декількох хвилин.

– Простота управління. Дані засоби можуть керуватись з будь-якої робочої станції. Взаємодія консолі управління з пристроєм здійснюється або за допомогою використання протоколів віддаленого керування, або за допомогою консольного кабелю.

– Відмовостійкість і висока доступність. Виконання МЕ у вигляді спеціалізованого програмно-апаратного комплексу дозволяє реалізувати механізми забезпечення не тільки програмної, але і апаратної відмовостійкості і високої доступності даних пристроїв.

– Висока продуктивність і надійність. За рахунок виключення з ОС всіх "непотрібних" сервісів і підсистем, програмно-апаратний комплекс працює більш ефективно з точки зору продуктивності і надійності.

– Спеціалізація на захисті. Рішення тільки завдань забезпечення мережної безпеки не призводить до витрат ресурсів на виконання інших функцій, наприклад маршрутизації і т. п.

Одним з провідних виробників подібного обладнання, яке і буде взяте за основу проекту, є Cisco Systems.

Cisco Systems, Inc. — американська транснаціональна корпорація, яка є найбільшим у світі виробником мережевого обладнання, призначеного для обслуговування мереж віддаленого доступу, сервісів безпеки, мереж зберігання даних, маршрутизації і комутації, а також для потреб комерційного ринку IP-комунікацій і корпоративного ринку.

Cisco випускає рішення безпеки, які забезпечують захист будь-якого пристрою та будь-якого середовища – від локальної мережі до хмари. Лінійка програмно-апаратного середовища безпеки являє собою набір передових рішень у даній галузі. Важливою перевагою даних пристроїв є їх повноцінне налаштування й інтеграція, що спрощує захист від кіберзлочинців.

До того ж, серед великого асортименту обладнання кожен зможе обрати пристрій за його економічними можливостями та потребами – представлені як бюджетні, так і професійні пристрої захисту. В залежності від цього різниться і апаратна складова даного обладнання – випускається велика кількість апаратних моделей з різною продуктивністю, модульними інтерфейсними картами, функціями стекування і кластеризації. Продуктивність моделей починається з молодших лінійок з пропускною здатністю в 50 Мбіт/сек, закінчуючи рішеннями класу великих центрів обробки даних (ЦОД), де даний параметр досягає поділки в 60 Гбіт/сек.

У компанії Cisco є рішення для захисту електронної пошти та доступ в Інтернет, що працюють в режимі реального часу – Cisco Email Security і Cisco Web Security. Вони здатні до захисту організації від загроз, що проникають через Інтернет і електронну пошту, а також забезпечити мережу від цілеспрямованих і адресних атак.

Також в режимі реального часу працює платформа Cisco Identity Services Engine (ISE), що надає функції контролю доступу, збираючи контекстну інформацію про мережі, користувачів та пристрої. В її можливостях приймання попереджувальних рішень щодо управління мережею для застосування інтелектуальних політик доступу з високим рівнем безпеки в будь-яких мережах.

Аналітика загроз безпеки, що вбудована в дану платформу, допоможе захистити від усіх відомих і навіть нових загроз.

Ефективні та потужні функції захисту і контролю надають рішення хмарної безпеки Cisco. Вони дозволяють користуватися всіма можливостями захисту хмари, а саме – контролювати та захищати користувачів, дані і програми у будь-якій точці мережі. Ці ж засоби здатні контролювати дотримання політик та збирати аналітичні дані про ті чи інші загрози за допомогою керованих з хмари засобів безпеки Cisco.

Але одною з найбільших та найвагоміших частин виробництва продукції, що стосується захисту, є виробництво МЕ. Вони дають змогу запобігти загрозам і користуватись перевагою колективної аналітики інформаційної безпеки. Лінійка МЕ Cisco повноцінно почала розвиватись в 2005 році і була названа Cisco ASA (Adaptive Security Appliances). Дані пристрої розвиваються і до сьогодні. На даний час, останнім витком розвитку МЕ корпорації Cisco є Cisco Firepower. Це рішення поєднує в собі систему запобігання загрозам і систему блокування відомих та невідомих загроз.

Розробники програмно-апаратних рішень корпорації Cisco передбачили ряд можливостей захисту периметра у рамках ядра власного ПЗ, що зветься Cisco IOS. Вона дозволяє клієнтам продукції Cisco використовувати маршрутизатори в якості засобу первинного контролю мережного доступу до локальних мереж. Серед можливостей захисту виділяють обмеження зв'язку з вузлами, що мають невідомі або небажані адреси, маскування внутрішніх IP-адрес для зовнішніх спостерігачів, автентифікацію користувачів, авторизацію доступу, контроль потоку даних, що проходять через маршрутизатор, а також застосування спеціальних засобів адміністрування, що реалізують вимоги політики захисту в системі периметра мережі.

Лінійка маршрутизаторів досить широка і включає в себе різні рішення – від бюджетних домашніх маршрутизаторів до корпоративних. Звісно, як і у більшості виробників, у Cisco в маршрутизаторах є підтримка безпровідних модулів, як вбудованих, так і тих, що можуть бути встановлені пізніше.

Можливості МЕ та маршрутизаторів на сучасному етапі розвитку мережного обладнання досить близькі. Наприклад, МЕ фірми Cisco мають змогу маршрутизувати трафік і навіть підтримувати протоколи динамічної маршрутизації. В свою чергу, у маршрутизаторів є підтримка функцій МЕ – технологій CBAC (Context-based access control) та ZFW (Zone-based firewall). Але все ж є і відмінності. Як і в будь-якій сфері, є «універсальні» пристрої, в даному випадку – маршрутизатори, та більш спеціалізовані – МЕ.

На перший погляд, для реалізації такого завдання, як забезпечення захищеного підключення офісу до мережі Інтернет, обидва пристрої надають все необхідне:

– є маршрутизація (статична та динамічна), а також функція трансляції адрес NAT;

– можна створити підключення до двох і більше провайдерів (підтримується IP SLA (Service Level Agreements), BGP (Border Gateway Protocol));

– присутні функції МЕ;

– є підтримка VPN (Virtual Private Network).

Якщо ж перейти до більш детального аналізу, то стане зрозуміло, що у МЕ більшість функцій безпеки активовані за замовчуванням і працюють за правилом «заборонено все, що не дозволено», на відміну від маршрутизаторів, на яких функції безпеки необхідно активовувати примусово. МЕ є більш функціональним (наприклад, Identity Firewall дає можливість надавати доступ на підставі імен користувачів або груп в Microsoft Active Directory), при цьому його конфігурування більш інтуїтивно зрозуміло. Також на МЕ є можливість впливу на порядок застосування правил NAT, що відсутня в маршрутизаторах. Класичний МЕ має функції глибокого аналізу вмісту протоколів, а також функцію виявлення загроз (сканування та атак Denial of Service – DoS-атак). МЕ здатен працювати в двох режимах: маршрутизованому і прозорому (Transparent Firewall). Також МЕ може працювати в режимі множинних контекстів (віртуальні МЕ, multiple context) або в режимі єдиного контексту.

Маршрутизатори також можуть працювати в двох режимах (маршрутизованому та прозорому), а замість контекстів, підтримує функціонал Virtual Routing and Forwarding (VRF). Щоправда, налаштовуючи Zone-Based Policy Firewall (ZFW) на маршрутизаторі, можна легко заплутатися зі створенням політик під кожну пару інтерфейсів, налаштуванням класів, списків доступу і їх зв'язкою в конфігурації. Маршрутизатори також поступаються у функціональності роботи з VPN з'єднаннями.

Ще одною відмінністю є резервування, яке представлене у МЕ компанії Cisco за рахунок функцій відмовостійкості та кластеризації. У режимі відмовостійкості два пристрої об'єднуються в одне логічне. Доступні два режими роботи: active/standby (з єдиним контекстом) і active / active (в режимі множинних контекстів). В першому режимі роботи один пристрій працює в активному режимі, а інший – в пасивному, і готовий «підхопити» весь трафік у разі відмови першого. В другому режимі обидва пристрої працюють в активному режимі як один логічний пристрій. Режим відмовостійкості зручний тим, що після об'єднання двох пристроїв, необхідно налаштовувати тільки один пристрій — активний. Дані з одного пристрою реплікуються на другий для забезпечення збереження стану всіх сесій при відмові одного з них.

Що ж до кластеризації, то вона дозволяє об'єднати в один логічний пристрій до 16 МЕ. Необхідно обмовитися, що на даний момент в кластер з 16 пристроїв ми можемо об'єднати тільки Cisco ASA 5585-X. Для інших моделей в кластер об'єднуються тільки два пристрої. Кластеризація забезпечує резервування пристроїв, єдину точку управління (всі пристрої об'єднуються в один логічний) і підвищення продуктивності (мова йде про те, що ми отримуємо один віртуальний пристрій з більшою продуктивністю ніж один фізичний пристрій).

У маршрутизаторів подібні функції відсутні. Відмовостійкість забезпечується відповідним налаштуванням кожного протоколу і функції. Для маршрутизації трафіку налаштування будуть свої, для міжмережного

екранування свої, а для VPN – свої. Failover, а саме так зветься режим відмовостійкості на МЕ, в цьому плані більш зручний.

У маршрутизації нове покоління МЕ зробило великий крок вперед. Але вона дещо відмінна від аналогічної в маршрутизаторах. По-перше, по кожному протоколу маршрутизації присутні обмеження і нюанси. Наприклад, МЕ при роботі з BGP не розрахований на обробку повної таблиці маршрутизації (full view). По-друге, на МЕ немає логічних тунельних інтерфейсів GRE (Generic Routing Encapsulation) / VTI (Virtual Tunnel Interface). Це призводить до труднощів з реалізацією тунелів через публічні мережі. Безумовно, маршрутизатор в даному аспекті істотно перевершує МЕ по функціональності.

Ще варто відзначити, у МЕ присутній web-інтерфейс – Adaptive Security Device Manager (ASDM), що дозволяє налаштовувати МЕ не тільки через командний рядок. Даний інтерфейс повнофункціональний і ряд функцій рекомендується налаштовувати саме через нього, так як для цього є досить зручні помічники (wizard). Web-інтерфейс у маршрутизаторів є – Cisco Configuration Professional, але його функціональність не є зручною.

На МЕ не так давно з'явилася підтримка Embedded Event Manager, що дозволяє отримати часткову автоматизацію. На маршрутизаторах даний функціонал присутній вже досить давно [6].

У деяких мережах маршрутизатор може бути використаний як самостійне ефективне рішення захисту периметра. Так, наприклад, дане використання доцільно використовувати для домашнього або віддаленого офісу, для внутрішнього сегменту мережі або як рішення захисту мережі з низьким рівнем ризику. Так чи інакше, правильно налаштований маршрутизатор може забезпечити ефективний захист периметру мережі. Однак разом з маршрутизатором слід також застосовувати й інші, більш глибокі принципи захисту, адже в такому випадку злам лише одного пристрою, маршрутизатора, призведе до незахищеності мережі.

Захист периметра мережі є складним комплексом технологічних рішень по захисту межі мережі від вторгнень. Захист периметра мережі повинен грати роль

стіни навколо мережі і забезпечувати захист від вторгнення мережевих порушників. Відсутність або слабкість захисту периметра відкриває проломи в захисті, які можуть бути використані порушниками. Тому фахівці рекомендують використання цих пристроїв одночасно. Це дасть можливість відокремити маршрутизацію від захисту мережі та зменшить навантаження на апаратні ресурси пристроїв [7].

Висновки до розділу 1

В результаті аналізу організації периметрового захисту сучасних мереж визначено основні принципи захисту внутрішніх мереж та обрано периметровий захист на базі МЕ. Потрібно розробити підсистему захисту локальних мереж від зовнішніх зловмисних дій.

Було розглянуто 4 існуючих різновида МЕ та проаналізовані їх переваги та недоліки. Дослідження даних різновидів МЕ показали, що для даного проекту слід використовувати екрануючі маршрутизатори та МЕ експертного рівня.

Також розглянуті вироби провідного виробника мережного обладнання – корпорації Cisco. Проаналізований їх асортимент, можливості налаштувань та експлуатації для периметрового захисту локальних мереж.

РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ

2.1. Проект мережі організації

В даній роботі була розглянута мережа організації, що представлена шістьма офісами. Офіси подібні за будовою та складаються з робочих станцій, принтерів, офісних комутаторів, серверів та мережевих пристроїв периметру (див. рис. А.1). Також є можливість збільшувати кількість кінцевих пристроїв за рахунок підключення до вільних портів комутаторів.

Для підключення пристроїв мережі між собою використовуються високошвидкісні порти FastEthernet/GigabitEthernet. Дані порти відрізняються пропускною здатністю в 100 та 1000 Мбіт/с відповідно.

Детальну топологію з'єднань перших трьох офісів можна побачити в табл. 2.1-2.3. Топологія з'єднань четвертого офісу подібна до другого, п'ятого – до третього, а шостого – до першого.

Таблиця 2.1

Параметри інтерфейсів пристроїв першого офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Міжмережний екран Firewall1	Gi0/0	Комутатор Switch1-1	Fa1/2
	Gi0/1	Міжмережний екран Firewall1(2)	Gi0/1
	Gi0/2	Комутатор Switch1-2	Gi0/0
Міжмережний екран Firewall1(2)	Gi0/0	Комутатор Switch1-1	Fa1/3
	Gi0/1	Міжмережний екран Firewall1	Gi0/1
	Gi0/2	Комутатор Switch1-2	Gi0/1
Комутатор Switch1-1	Fa0/0	Робоча станція PC1-VM	Fa0
	Fa0/1	Робоча станція PC1-1	Fa0
	Fa0/2	Робоча станція PC1-2	Fa0
	Fa0/3	Робоча станція PC1-3	Fa0
	Fa1/0	Принтер Printer1-1	Fa0
	Fa1/1	Принтер Printer1-2	Fa0
	Fa1/2	Міжмережний екран Firewall1	Gi0/0

Продовження таблиці 2.1

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор Switch1-1	Fa1/3	Міжмережний екран Firewall1(2)	Gi0/0
	Fa2/0	Принтер Printer1-3	Fa0
	Fa2/1	Принтер Printer1-4	Fa0
	Fa2/2	Сервер Server1-1	Fa0
	Fa2/3	Сервер Server1-2	Fa0
	Fa3/0	Сервер Server1-3	Fa0
Комутатор Switch1-2	Gi0/0	Міжмережний екран Firewall1	Gi0/2
	Gi0/1	Міжмережний екран Firewall1(2)	Gi0/2
	Gi0/2	Internet	
Робоча станція PC1-VM	Fa0	Комутатор Switch1-1	Fa0/0
Робоча станція PC1-1	Fa0	Комутатор Switch1-1	Fa0/1
Робоча станція PC1-2	Fa0	Комутатор Switch1-1	Fa0/2
Робоча станція PC1-3	Fa0	Комутатор Switch1-1	Fa0/3
Принтер Printer1-1	Fa0	Комутатор Switch1-1	Fa1/0
Принтер Printer1-2	Fa0	Комутатор Switch1-1	Fa1/1
Принтер Printer1-3	Fa0	Комутатор Switch1-1	Fa2/0
Принтер Printer1-4	Fa0	Комутатор Switch1-1	Fa2/1
Сервер Server1-1	Fa0	Комутатор Switch1-1	Fa2/2
Сервер Server1-2	Fa0	Комутатор Switch1-1	Fa2/3
Сервер Server1-3	Fa0	Комутатор Switch1-1	Fa3/0

Таблиця 2.2

Параметри інтерфейсів пристроїв другого офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор Router2	Gi0/0	Internet	
	Gi1/0	Міжмережний екран Firewall2	Gi0/1
Міжмережний екран Firewall2	Gi0/0	Комутатор Switch2	Fa1/3
	Gi0/1	Маршрутизатор Router2	Gi1/0
Комутатор Switch2	Fa0/0	Робоча станція PC2-VM	Fa0
	Fa0/1	Робоча станція PC2-1	Fa0
	Fa0/2	Робоча станція PC2-2	Fa0

Продовження таблиці 2.2

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор Switch2	Fa0/3	Робоча станція PC2-3	Fa0
	Fa1/0	Принтер Printer2-1	Fa0
	Fa1/1	Принтер Printer2-2	Fa0
	Fa1/2	Принтер Printer2-3	Fa0
	Fa1/3	Міжмережний екран Firewall2	Gi0/0
	Fa2/0	Принтер Printer2-4	Fa0
	Fa2/1	Сервер Server2-1	Fa0
	Fa2/2	Сервер Server2-2	Fa0
	Fa2/3	Сервер Server2-3	Fa0
Робоча станція PC2-VM	Fa0	Комутатор Switch2	Fa0/0
Робоча станція PC2-1	Fa0	Комутатор Switch2	Fa0/1
Робоча станція PC2-2	Fa0	Комутатор Switch2	Fa0/2
Робоча станція PC2-3	Fa0	Комутатор Switch2	Fa0/3
Принтер Printer2-1	Fa0	Комутатор Switch2	Fa1/0
Принтер Printer2-2	Fa0	Комутатор Switch2	Fa1/0
Принтер Printer2-3	Fa0	Комутатор Switch2	Fa1/0
Принтер Printer2-4	Fa0	Комутатор Switch2	Fa1/0
Сервер Server2-1	Fa0	Комутатор Switch2	Fa2/1
Сервер Server2-2	Fa0	Комутатор Switch2	Fa2/2
Сервер Server2-3	Fa0	Комутатор Switch2	Fa2/3

Таблиця 2.3

Параметри інтерфейсів пристроїв третього офісу

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор Router3	Gi0/0	Комутатор Switch3	Fa1/3
	Gi1/0	Internet	
	Gi2/0	Сервер Server3-1	Fa0
	Gi3/0	Сервер Server3-2	Fa0
	Gi4/0	Сервер Server3-3	Fa0
Комутатор Switch3	Fa0/0	Робоча станція PC3-VM	Fa0
	Fa0/1	Робоча станція PC3-1	Fa0

Продовження таблиці 2.3

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор Switch3	Fa0/2	Робоча станція PC3-2	Fa0
	Fa0/3	Робоча станція PC3-3	Fa0
	Fa1/0	Принтер Printer3-1	Fa0
	Fa1/1	Принтер Printer3-2	Fa0
	Fa1/2	Принтер Printer3-3	Fa0
	Fa1/3	Маршрутизатор Router3	Gi0/0
	Fa2/0	Принтер Printer3-4	Fa0
Робоча станція PC3-VM	Fa0	Комутатор Switch3	Fa0/0
Робоча станція PC3-1	Fa0	Комутатор Switch3	Fa0/1
Робоча станція PC3-2	Fa0	Комутатор Switch3	Fa0/2
Робоча станція PC3-3	Fa0	Комутатор Switch3	F0/3
Принтер Printer3-1	Fa0	Комутатор Switch3	Fa1/0
Принтер Printer3-2	Fa0	Комутатор Switch3	Fa1/1
Принтер Printer3-3	Fa0	Комутатор Switch3	Fa1/2
Принтер Printer3-4	Fa0	Комутатор Switch3	Fa2/0
Сервер Server3-1	Fa0	Маршрутизатор Router3	Gi2/0
Сервер Server3-2	Fa0	Маршрутизатор Router3	Gi3/0
Сервер Server3-3	Fa0	Маршрутизатор Router3	Gi4/0

Для забезпечення функціонування даної мережі організації було обрано оптимальні маршрутизатори, МЕ і комутатори корпорації Cisco, котрі мають адаптованість під модернізацію модулями.

Так як доступу до реального обладнання немає, то мережа розробляється в графічному симуляторі. Із-за цього конкретні моделі пристроїв назвати важко. Тому нижче охарактеризовані серії пристроїв, які були використані для побудови мережі.

Маршрутизація мережі побудована на базі маршрутизатора Cisco з серії 7200 та МЕ Cisco ASA серії 5500.

Маршрутизатори Cisco 7200 Series є найбільш поширеними універсальними рішеннями для агрегації сервісів – величезна кількість компаній

довірили свій мережевий інтерфейс цим пристроям. Дана серія маршрутизаторів має велику кількість інтерфейсів, тому активно використовується не тільки великими компаніями, але і починаючими підприємствами, адже від цього в повній мірі буде залежати майбутній розвиток офісу підприємства.

Володіючи високою продуктивністю, маршрутизатори здатні відправляти дані в кілька потоків, тим самим, такий прийом передачі сприяє підвищенню швидкості обміну інформацією. Це досягається за рахунок чіпів Cisco 7200 NPE-G2. Цей процесор допомагає створити мережну платформу, здатну не тільки швидко передавати дані, але також і справлятися із завантаженістю на каналах передачі. У разі її виникнення вмикається магістральна передача інформації, яка допомагає відправити надлишок пакетів протягом короткого періоду часу. Також на вибір на користь даних пристроїв впливає широкий набір підтримуваних з'єднань, легкість в обслуговуванні і управлінні, та збільшена масштабованість і гнучкість завдяки новій карті адаптера портів.

Cisco 7200 Series має ряд переваг до яких відносять велику кількість віртуальних приватних мереж (VPN) – до 5000 на базі IPsec, інтеграцію передачі голосу, відео та даних – підтримка адаптерів голосових портів, та модульну архітектуру – форм-фактор 3RU дозволяє використовувати широкий набір гнучких модульних інтерфейсів (від DS0 до OC-3).

Що ж до Cisco ASA 5500, то це лінійка модульних багатофункціональних пристроїв захисту, що була створена корпорацією Cisco Systems як логічне продовження розвитку лінійки Cisco PIX – дуже популярного рішення для захисту периметра мережевої інфраструктури підприємства.

Основною ідеєю при створенні лінійки ASA 5500 була нова стратегія Cisco Systems по створенню SDN (Self Defending Networks), що забезпечує комплексний захист мережі та дозволяє активно реагувати на мережні атаки і запобігати їм на самому початку.

В інфраструктурі підприємства ASA 5500 займає місце класичного ME, що дозволяє захистити мережу підприємства або окремі сегменти, але функціонал даного рішення набагато ширше.

Зокрема ASA 5500 реалізує частину функцій сучасного маршрутизатора, такі як протоколи динамічної маршрутизації RIP і OSPF, резервування каналів доступу в мережу Інтернет, механізми забезпечення якості обслуговування (QoS).

Для комутації мережі доречно використовувати сімейство комутаторів Cisco Catalyst 2960. Це сімейство фіксованої конфігурації з великою різноманітністю моделей для організації рівня доступу локальної мережі (безпосереднє підключення комп'ютерів/робочих станцій/мережевих принтерів).

У лінійці представлені моделі на 8, 24 або 48 портів 10/100 Ethernet + 2-4 порти Gigabit Ethernet, а також моделі з усіма портами на 1 Gigabit. Порти комутаторів оснащені технологією PoE (Power over Ethernet) для живлення IP-телефонів або бездротових точок доступу. Також є підтримка надлишкового модуля живлення Cisco Redundant Power System 2300.

Серед можливостей комутаторів даної лінійки виділяють можливість регулювати швидкість передачі на кожному інтерфейсі з кроком в 64 Кбіт/с, підтримку об'єднання портів (Link Aggregation) для організації більш швидкісних з'єднань між комутаторами і серверами та можливість організації транкових з'єднань на кожному інтерфейсі за допомогою тегів 802.1q.

Майже всі серії Cisco Catalyst 2960 не підтримують маршрутизацію, але вміють фільтрувати трафік, ґрунтуючись на інформації 3-го рівня – IP. Починаючи від серії Cisco Catalyst 2960S комутатори володіють можливістю стекування.

Не так давно Cisco представила нову серію комутаторів Cisco Catalyst 2960-X/XR в даному сімействі. Оновлену серію розробники наділили відмінними технічними характеристиками, зробивши її більш продуктивною та інтелектуальною, а також приділили велику увагу «зеленим» технологіям [16].

Ця серія прийшла на зміну серії Catalyst 2960-S/SF, яка на сьогоднішній день є однією з найпоширеніших і широко використовуваної серій комутаторів в світі. Апаратна платформа 2960-S/SF дозволяє за допомогою технології FlexStack організувати стек комутаторів на швидкості 40 гбіт/с, достатню для

об'єднання чотирьох комутаторів. У серії 2960-X інженери Cisco домоглися майже дворазового поліпшення показників платформи 2960-S, і додали ряд опцій, що дозволяють поліпшити безпеку, забезпечити простоту впровадження та обслуговування. При цьому стекування серії 2960-X можливо з серією 2960-S. Таким чином, сумісність комутаторів 2960-X і 2960-S/SF при роботі в стеці дозволяє домогтися додаткового захисту інвестицій за рахунок зворотної сумісності і можливості міграції між серіями.

Комутатори Cisco Catalyst 2960-XR виділені в особливу групу і наділені наступними додатковими можливостями:

– можливість установки другого блоку живлення;
– підтримка Layer 3 і динамічної маршрутизації;
– 8 черг на порт, що налаштовуються;
– 48 груп EtherChannel.

У зв’язку з браком ресурсів комп’ютера була складена спрощена топологія мережі (див. рис. А.2). Як видно, в даній топології була спрощена кількість кінцевих пристроїв, більшість з них замінена на віртуальні симулятори персональних комп’ютерів. Кількість серверів зменшена до одного на офіс. Вони представлені у вигляді одного віртуального сервера, що виконує роль кластера серверів. Даної схеми буде цілком достатньо для того, щоб провести дослідження сформоване в завданні.

Для забезпечення функціонування спрощеної топології мережі, перш за все було виконано розрахунок параметрів IP-адресації. Під час розрахунку параметрів IP-адресації особлива увага була приділена економії IP-адрес, а також було приділено увагу можливості розширення внутрішньої мережі. Внутрішня адресація мережі буде налагоджена за рахунок протоколу динамічного налаштування вузла – Dynamic Host Configuration Protocol (DHCP). Внутрішні мережі для зручності налаштування та підвищення безпеки будуть поділені на віртуальні локальні мережі – Virtual Local Area Network (VLAN). Детальні параметри адресації мереж кожного з офісів представлені в табл. 2.4-2.6.

Таблиця 2.4

Параметри адресації мережі першого офісу

Підмережа/ Пристрій	Інтерфейс/Мереж-ний адаптер	IP-адреса	Маска підмережі	Префікс
Міжмережний екран Firewall1	Gi0/0.1	193.2.3.125	255.255.255.248	/29
	Gi0/0.10	193.2.3.1	255.255.255.240	/28
	Gi0/0.20	193.2.3.17	255.255.255.240	/28
	Gi0/0.30	193.2.3.33	255.255.255.240	/28
	Gi0/0.40	193.2.3.49	255.255.255.240	/28
	Gi0/0.50	193.2.3.65	255.255.255.240	/28
	Gi0/0.60	193.2.3.129	255.255.255.252	/30
	Gi0/1	1.1.2.1	255.255.255.252	/30
	Gi0/2	1.1.1.2	255.255.255.252	/30
Комутатор Switch1-1	Vlan1	193.2.3.126	255.255.255.248	/29
Робоча станція PC1-VM	Fa0	DHCP		
Робоча станція PC1-1	Fa0			
Робоча станція PC1-2	Fa0			
Робоча станція PC1-3	Fa0			
Принтер Printer1	Fa0			
Кластер серверів Servers1	Fa0	193.2.3.130	255.255.255.252	/30

Таблиця 2.5

Параметри адресації мережі другого офісу

Підмережа/ Пристрій	Інтерфейс/Мереж-ний адаптер	IP-адреса	Маска підмережі	Префікс
Маршрутизатор Router2	Gi0/0	2.2.2.2	255.255.255.252	/30
	Gi1/0	194.168.1.2	255.255.255.252	/30
Міжмережний екран Firewall2	Gi0/0.1	194.2.3.125	255.255.255.248	/29
	Gi0/0.10	194.2.3.1	255.255.255.240	/28
	Gi0/0.20	194.2.3.17	255.255.255.240	/28
	Gi0/0.30	194.2.3.33	255.255.255.240	/28
	Gi0/0.40	194.2.3.49	255.255.255.240	/28
	Gi0/0.50	194.2.3.65	255.255.255.240	/28
	Gi0/0.60	194.2.3.129	255.255.255.252	/30
	Gi0/1	194.168.1.1	255.255.255.252	/30
Комутатор Switch2	Vlan1	194.2.3.126	255.255.255.248	/29
Робоча станція PC2-VM	Fa0	DHCP		
Робоча станція PC2-1	Fa0			
Робоча станція PC2-2	Fa0			
Робоча станція PC2-3	Fa0			
Принтер Printer2	Fa0			
Кластер серверів Servers2	Fa0	194.2.3.130	255.255.255.252	/30

Таблиця 2.6

Параметри адресації мережі третього офісу

Підмережа/ Пристрій	Інтерфейс/Мереж-ний адаптер	IP-адреса	Маска підмережі	Префікс
Маршрутизатор Router3	Gi0/0.1	195.2.3.125	255.255.255.248	/29
	Gi0/0.10	195.2.3.1	255.255.255.240	/28
	Gi0/0.20	195.2.3.17	255.255.255.240	/28
	Gi0/0.30	195.2.3.33	255.255.255.240	/28
	Gi0/0.40	195.2.3.49	255.255.255.240	/28
	Gi0/0.50	195.2.3.65	255.255.255.240	/28
	Gi1/0	3.3.3.2	255.255.255.252	/30
	Gi2/0	195.2.3.129	255.255.255.252	/30
Комутатор Switch3	Vlan1	195.2.3.126	255.255.255.248	/29
Робоча станція PC3-VM	Fa0	DHCP		
Робоча станція PC3-1	Fa0			
Робоча станція PC3-2	Fa0			
Робоча станція PC3-3	Fa0			
Принтер Printer3	Fa0			
Кластер серверів Servers3	Fa0	195.2.3.130	255.255.255.252	/30

2.2. Проект підсистеми периметрового захисту

Кількість обраних офісів є невипадковою. Дана кількість дозволить детально проаналізувати різні підсистеми периметрового захисту.

В першому офісі для захисту периметра мережі застосована пара пристроїв Cisco ASA 5500.

ASA серії 5500 (див. рис. 2.1) об'єднує в собі безліч технологій і рішень щодо забезпечення інформаційної безпеки.

Контроль з'єднань між вузлами мережі забезпечує вбудований МЕ з механізмами інспекції пакетів з урахуванням стану протоколу (stateful inspection firewall) на рівнях 2-7, який дозволяє стежити за станом всіх мережевих комунікацій і допомагає запобігти несанкціонованому доступу до мережі. Механізми аналізу протоколів на прикладному рівні дозволяють забезпечити захист від нелегального використання дозволених портів, наприклад HTTP-TCP порт 80 для різноманітних додатків.

ASA 5500 дозволяє організувати захищений віддалений VPN доступ за допомогою технологій IPSec і SSL. Дані технології є найкращим способом

захисту критично важливої інформації при передачі її через публічні або недовірені мережі. Поєднання технологій VPN с механізмами адаптивного захисту від загроз забезпечує захист внутрішньої мережі організації від атак через VPN доступ [18].



Рис. 2.1. ME Cisco ASA 5500

ASA 5500 може функціонувати в «прозорому» режимі, при цьому вона не буде видимим вузлом мережі, буде прозоро для користувача пропускати трафік, забезпечуючи необхідний рівень захисту.

Шляхом реалізації на одному пристрої декількох віртуальних пристроїв можна забезпечити гнучкість застосування ASA 5500 і зменшити фінансові вкладення в захист мережевої інфраструктури.

Розширити функціональність ASA 5500 можна за допомогою установки апаратних модулів захисту від вторгнень (AIP-SSM) і захисту контенту (CSC-SSM). Модуль AIP-SSM призначений для захисту мережі від типових атак, він працює під управлінням спеціалізованого програмного забезпечення Cisco IPS версії 5.0 і містить базу сигнатур мережевих атак. Модуль CSC-SSM розроблений спільно з компанією Trend Micro і призначений для захисту від широкого спектру атак і шкідливого програмного забезпечення, містить у своєму складі антивірус, антиспам, захист від шпигунських програм, фільтр URL-посилань, механізми захисту від фішингу. Його рекомендується

використовувати для захисту робочих станцій і серверів організації при доступі до мережі Інтернет.

Вбудовані механізми дублювання дозволяють забезпечити високонадійний доступ до необхідних ресурсів за допомогою двох пристроїв ASA 5500, в разі виходу з ладу однієї ASA 5500 другий пристрій візьме на себе все навантаження непомітно для користувачів. Це так званий режим Failover. Цей режим дозволяє двом фізичним пристроям діяти як один логічний. Його і буде застосовано в даному офісі організації в якості захисного обладнання локальної мережі.

Можливі два варіанта роботи даного режиму – Active/Standby та Active/Active.

При першому варіанті один пристрій працює в активному режимі, а інший – в режимі очікування. В разі збою другий пристрій стає активним і продовжує роботу мережі. Перевагою та недоліком водночас в цьому випадку є менше використання ресурсів МЕ в режимі очікування. Це призводить до неповномірного використання апаратних ресурсів, але меншого зносу обладнання в режимі очікування.

При другому варіанті обидва пристрої працюють в активному режимі, що дозволяє розподіляти навантаження. Водночас, в разі збою активним лишається один пристрій, який залишається основним до відновлення роботи другого фізичного МЕ.

В даному проекті для першого офісу буде використовуватись варіант Active/Standby, так як офіс достатньо невеликий і не потребує великих ресурсів для забезпечення нормальної роботи внутрішньої мережі.

В третьому офісі в якості захисту використовується лише граничний маршрутизатор.

Маршрутизатори серії 7200 корпорації Cisco (рис. 2.2) пропонують солідний набір сервісів, що забезпечують не лише захист самого маршрутизатора, а й допомагають захистити локальну мережу за ним.



Рис. 2.2. Маршрутизатор Cisco серії 7200

Перш за все це досягається за рахунок вбудованих служб безпеки, системою локальної автентифікації та розширеними можливостями AAA (Authentication, Authorization, Accounting).

Також маршрутизатори даної серії пропонують інтегрований пакет рішень IPsec/ME/IPS.

ME на базі маршрутизаторів Cisco 7200 дозволяють:

– контролювати пакети та виявляти невідповідність політиці безпеки;
– проводити розширену перевірку вмісту протоколів IPv4 та IPv6;
– проводити URL-фільтрацію (Websense & N2H2);
– налаштовувати користувацький ME;
– проводити аутентифікацію/авторизацію користувачів для протоколів HTTP/HTTPS, FTP і Telnet;
– фільтрувати трафік додатків;
– виявляти та запобігати відмові в обслуговуванні (DoS) тощо.

Основою для захисту внутрішньої мережі можна вважати NAT та ACL. Ці технології дозволяють отримати надійний захист на третьому рівні моделі OSI.

Для захисту ж самого маршрутизатора використовується технологія AutoSecure, розділений на ролі доступ до командного рядка та зовнішнє управління [15].

В другому офісі для забезпечення периметрового захисту внутрішньої мережі застосовано дворівневий захист з використанням граничного екрануючого маршрутизатора та МЕ експертного рівня. Дана схема допомагає відфільтровувати трафік ще до експертного МЕ, що дозволяє забезпечити захист не тільки внутрішньої мережі, але й самого пристрою експертного МЕ.

2.3. Розробка політики безпеки периметрового захисту

Захищена комп'ютерна мережа обов'язково повинна мати засоби розмежування доступу до її ресурсів, перевірки автентичності користувача і протидії виведенню комп'ютерної мережі з ладу.

Число атак на внутрішні мережі неухильно зростає, тому необхідно створити повністю захищене інформаційне середовище. Це дуже складне завдання – потрібні спеціалізовані засоби, призначені для здійснення постійного запобігання будь-яких несанкціонованих дій із зовнішнього і внутрішнього світу, контролю за використанням цього середовища і втілення в життя прийнятої організацією політики захисту її інформаційних і мережних ресурсів.

Оманливим є твердження, що МЕ захищає всі комп'ютери мережі і при його встановленні жодні додаткові заходи захисту вже не потрібні. МЕ – це лише одна складова ефективного захисту. Попередньо повинні бути переглянуті й інші додаткові компоненти, або рівні, що забезпечують ефективний захист мережі. Він складається з наступних компонентів:

1. політика інформаційної безпеки організації;
2. система захисту хостів внутрішньої мережі;
3. система захисту каналів зв'язку внутрішньої мережі;
4. мережний моніторинг і аудит з використанням систем аналізу захищеності і систем виявлення вторгнень;

5. план реагування на виявлені атаки.

Політика безпеки дуже важлива для функціонування захищеної мережі – потрібно знати, що захищати і в якій мірі. Всі інші рівні захисту логічно слідують після прийняття для мережі політики її безпеки. Логічне і методичне дотримання багаторівневого підходу при захисті має сприяти досягненню кращих результатів і гарантувати повну лояльність співробітників відділу безпеки організації. Секрет ефективного захисту інформації якраз і полягає в розробці політик безпеки для відкритої інформаційної системи, введенні їх в експлуатацію, моніторингу, аудиті та регулярному їх перегляді [8].

Перш за все політика необхідна для того, щоб донести до бізнесу цілі і завдання інформаційної безпеки компанії. Бізнес повинен розуміти, що політика безпеки це не тільки інструмент для розслідування фактів витоків даних, але і помічник у мінімізації ризиків компанії, а отже — у підвищенні прибутковості компанії.

Політика информаційної безпеки необхідна для обґрунтування введення захисних заходів в компанії. Вона повинна бути затверджена вищим адміністративним органом компанії (генеральний директор, Рада директорів тощо).

Також варто розуміти, що будь-яка захисна міра є компромісом між зниженням ризиків і зручністю роботи кінцевого користувача. При цьому будь-яке застосування захисних заходів, що стосуються взаємодії користувача з інформаційною системою компанії завжди викликає його негативну реакцію. Тому слід враховувати, що діяльність політики безпеки має бути непомітною або малопомітною для користувачів.

При налаштуванні політики МЕ розглядають два аспекти мережної безпеки: політику доступу до мережевих ресурсів і політику реалізації власне МЕ. Політика доступу до мережевих ресурсів відображає загальні вимоги з безпеки тієї чи іншої організації, і при її розробці повинні бути сформульовані правила доступу користувачів до різних сервісів, що використовуються в організації. Зазначені правила описують, який внутрішній (зовнішній)

користувач (група користувачів), коли, з якого внутрішнього (зовнішнього) вузла мережі і яким сервісом може скористатися з уточненням у разі необхідності способів аутентифікації користувачів і адрес цільових серверів.

Політика реалізації МЕ визначає, яким чином застосовується політика доступу до мережевих ресурсів, і в ряді випадків залежить від використовуваних сервісів і обраних засобів побудови екрану.

МЕ забезпечують підтримку та реалізацію політики мережної безпеки підприємства. Під політикою безпеки розуміють сукупність правил і практичних прийомів безпеки, що регулюють управління, захист і розподіл цінної інформації. Прийнятні та неприйнятні дії, що належать до безпеки, підпадають під високорівневі інструкції, що являють собою організаційну політику безпеки. На основі заданого набору правил, що є не чим іншим, як практичним втіленням політики інформаційної безпеки для МЕ, вони аналізують пакети на предмет дозволених/заборонених адрес і сервісів (точніше, відповідних їм TCP/UDP-портів). Зазвичай при конфігурації системи вказують, з яких адрес, за якими портами і з якими комп'ютерами можна працювати, а з якими ні.

Рішення про фільтрацію конкретних протоколів й адрес за допомогою МЕ, залежить від прийнятої політики безпеки в мережі, що захищається. Компоненти, що налаштовуються для реалізації обраної політики безпеки, а точніше їх набір і являють собою МЕ. Ефективність захисту локальної мережі за допомогою МЕ залежить від декількох факторів. Основною з них звичайно є обрана політика доступу до мережних сервісів і ресурсів внутрішньої мережі, але свій вплив також має раціональність вибору та використання основних компонентів МЕ.

Логічно, що до МЕ висувають підвищені функціональні вимоги, так як від цього залежить безпека мережі. У найзагальнішому випадку МЕ повинен:

– забезпечувати безпеку внутрішньої (тієї, що захищається) мережі і повний контроль над зовнішніми підключеннями і сеансами зв'язку;

– забезпечувати неможливість обходу політики безпеки;

– володіти потужними і гнучкими засобами управління для повного і простого введення в життя політики безпеки організації;

– забезпечувати просту реконфігурацію МЕ при зміні структури мережі;

– працювати непомітно для користувачів мережі і не ускладнювати виконання ними легальних дій;

– працювати досить ефективно і встигати обробляти весь вхідний та вихідний трафік в режимах найбільшого навантаження;

– володіти властивостями самозахисту від будь-яких несанкціонованих дій;

– мати можливість централізовано забезпечувати декілька зовнішніх підключень (наприклад, віддалених філій) для проведення єдиної політики безпеки;

– мати засоби авторизації доступу користувачів через зовнішні підключення.

Підсумовуючи, можна виділити наступні загальні вимоги до МЕ:

– фільтрація на мережному рівні;

– фільтрація на прикладному рівні;

– налаштування правил фільтрації й адміністрування;

– засоби мережевої аутентифікації;

– впровадження журналів і обліку.

Досить часто можна почути, що МЕ порівнюють з «пляшковим горлечком». Це порівняння є досить доречним, так як через МЕ має проходити весь вхідний та вихідний трафік мережі. За рахунок цього з’являється можливість відслідковувати та фільтрувати його. Фільтрація застосовується до тих пакетів, які не відповідають вимогам політики безпеки. Такі пакети МЕ може перенаправляти, переупаковувати чи знищувати – це залежить від конфігурації, яку налаштував адміністратор мережі [9].

Управління рівнем захищеності системи, яке виконує адміністратор, включає в себе підтримку цілісності загальної політики безпеки системи, забезпечення взаємозв'язку сервісів, механізмів і засобів управління захистом, системний журнал, управління механізмом відновлення системи та ін.

Управління сервісами захисту реалізує призначення чи зняття окремого сервісу, визначає правила вибору конкретних механізмів для реалізації необхідних сервісів, погоджує параметри механізмів захисту. Управління окремими механізмами захисту включає, зокрема, управління криптографічними ключами, управління контролем доступу, управління маршрутизації, управління арбітражем та ін.

Важливою ланкою є аудит безпеки кожної нової системи (як програмної, так і апаратної) при її інсталяції в внутрішню мережу, метою чого є перевірка її відповідності до політики і стандартів системної конфігурації:

– допомагає встановити правила роботи нової системи в контексті функцій, здійснюваних кожним хостом або всієї внутрішньої мережі;

– перевіряє відповідність роботи системи відносно політики безпеки хоста;

– перевіряє наявність в системі добре відомих лазівок в забезпеченні інформаційної безпеки.

Наступні два принципа зазвичай лежать в основі політики доступу до мережевих сервісів:

1. доступ з глобальної мережі у внутрішню заборонений, але доступ з внутрішньої мережі в глобальну – дозволений;
2. обмежений доступ у внутрішню мережу з глобальної дозволений і забезпечує роботу тільки окремих авторизованих систем.

Список сервісів в глобальній мережі, до яких користувачі повинні мати обмежений доступ визначається у відповідності до політики доступу до мережних сервісів. Також існує можливість задати обмеження на методи доступу до сервісів, наприклад, на використання протоколів SLIP (Serial Line Internet Protocol) чи PPP (Point-to-Point Protocol). Дане обмеження методів доступу забезпечить неможливість з’єднання користувачів з "забороненими" сервісами Internet обхідними шляхами. Так наприклад, адміністратор встановлює спеціальний шлюз, який не дає можливості користувачам працювати в системі «глобальної павутини», тим самим обмежує доступ в глобальну мережу, але при

цьому вони могли б встановити PPP-з'єднання з веб-серверами по комутованій лінії.

У відповідності до політики реалізації МЕ визначаються правила доступу до ресурсів внутрішньої мережі. У першу чергу, необхідно встановити, наскільки система захисту має довіряти чи підозрювати зовнішні чинники. Інакше кажучи, правила доступу до внутрішніх ресурсів повинні базуватися на одному з наступних принципів:

– дозволено все, що не заборонено;

– заборонено все, що не дозволено.

На перший погляд може здатися, що ці дві стратегії дуже прості і майже не відрізняються один від одного, насправді це не так.

При реалізації першого принципу внутрішня мережа виявляється менш захищеною від нападів хакерів, однак користуватися їй буде зручніше і буде потрібно менше витрат. Він будується на тому, що МЕ за замовчуванням дозволяє всі сервіси, які не вказані як заборонені. В цьому випадку для забезпечення безпеки мережі доведеться створювати правила, які враховували б всі можливі заборони. Ця стратегія є корисною, коли потрібно зробити виключення з правил. Наприклад, для користувача внутрішньої мережі заблокувати відеохостинг YouTube, щоб той не відволікався від роботи на перегляд відео. Цей принцип використовується в МЕ на основі фільтруючого маршрутизатора. Але для безпеки мережі ця стратегія є менш рентабельною, так як це призводить до необхідності опису великої кількості правил і змушує переглядати їх при появі кожного нового протоколу або сервісу, які існуючими правилами не охоплюються. Досить часто це може призвести до появи помилок в налаштуванні, так як при цьому можна заплутатись чи просто забути про них.

Друга стратегія суворіша і безпечніша. Реалізація МЕ на її основі забезпечує значну захищеність. Набагато простіше керувати МЕ, заборонивши весь трафік за замовчуванням і задавши правила, що дозволяють проходження через кордон мережі тільки необхідних протоколів і сервісів. Заборона всього трафіку за замовчуванням забезпечується введенням правила "заборонено все" в

останньому рядку таблиці фільтрації. Перевага для захисту мережі очевидна – всі вразливості «закриті» одразу і треба лише дозволити проходження легального трафіку. Однак правила доступу, сформульовані відповідно до цього принципу можуть доставляти великі незручності користувачам, а крім того, їх реалізація обходиться досить дорого. До того ж у ряді випадків, зокрема при використанні простого пакетного фільтра, опис правил допустимих сервісів також пов'язаний з трудомістким процесом, що вимагає досконального знання алгоритмів функціонування протоколів в рамках того чи іншого сервісу. Дана стратегія захисту за замовчуванням застосовується в експертних МЕ.

Перед початком конфігурування МЕ слід також продумати стратегію захисту. Так, наприклад, слід звернути увагу на те, чи будуть у підприємства працівники, які працюють віддалено. Робота з віддаленими користувачами вимагає налаштування більш жорстких обмежень доступу до інформаційних ресурсів мережі, при цьому залишивши можливість для роботи авторизованих користувачів. Тому досить часто може виникнути потреба в організації декількох секторів з різними рівнями безпеки у складі локальної мережі:

– вільно доступні сектори (наприклад, рекламний веб-сервер);

– сектори з обмеженим доступом (наприклад, для доступу співробітникам організації для віддаленої роботи);

– закриті сектори (наприклад, локальна фінансова мережа організації).

В даному проекті складена однорідна політика безпеки мережі для кожного з офісів. Вона включає в себе такі пункти:

1. внутрішня мережа офісу має бути розділена на декілька віртуальних підмереж (в залежності від потреби);
2. доступ з глобальної мережі до внутрішньої має бути заблокований, окрім кластера серверів;
3. кожен комп’ютер (робоча станція) повинен мати високошвидкісний доступ до глобальної мережі Інтернет, вийнятком є окремий комп’ютер системного адміністатора;

4. офіси мають вільно та безпечно контактувати між собою – між офісами мають бути створені приватні віртуальні мережі;
5. кожен комп’ютер (робоча станція) повинен мати доступ для друку на принтерах в межах офісу;
6. до внутрішньої та зовнішньої мереж, а також до кластеру серверів з підмережі принтерів не має бути доступу;
7. кластер серверів повинен бути доступний як у внутрішній, так і у глобальної мережі, тобто знаходитись в демілітаризованій зоні;
8. фізичний доступ до мережного обладнання повинен бути лише в системного адміністратора;
9. віддалений доступ до мережного обладнання повинен бути тільки з підмережі комп’ютера системного адміністратора;
10. фізичний та віддалений доступ повинні бути доступні лише авторизованим користувачам.

Дана політика буде реалізовуватись на різних мережних пристроях, але є єдиною для всіх офісів.

2.4. Проект сценаріїв тестування функціоналу підсистеми

Використання засобів захисту інформації, таких як МЕ, системи контролю доступу, антивіруси, не гарантує, що відкрита система стійка до несанкціонованих дій з боку зловмисників, що порушують встановлений порядок використання ресурсів. Будь-яке програмне чи апаратне забезпечення не є досконалим, і з великою часткою ймовірності можна припустити, що в ньому знайдуться вразливості, що дозволяють зробити такі дії. А, як відомо, рівень захищеності всієї мережі дорівнює рівню захищеності найслабшої її ланки. Тому при проектуванні і експлуатації відкритих інформаційних систем, наприклад інтранет, рано чи пізно виникає питання про їх захищеність від загроз інформаційної безпеки відповідно до політики безпеки організації. На сьогодні немає точного і єдиного визначення захищеності, але для прикладу візьмемо

тведження, що захищеність визначається як величина, що обернена до вразливості.

Виникає логічне питання: як оцінити рівень захищеності інтранету і як визначити, чи є він достатнім в даному середовищі функціонування? Аналіз захищеності різного ступеня деталізації входить як одна зі складових в аудит інформаційної безпеки відкритих інформаційних систем. Під аудитом інформаційної безпеки відкритої системи будемо розуміти незалежний і документований систематичний процес отримання та оцінки на відповідність політиці безпеки за певними критеріями об'єктивних даних про поточний стан забезпечення безпеки, включаючи події, що відбуваються в перевіряється системі. Його мета – ретельне обстеження процесів забезпечення безпеки при виконанні відкритих систем свого головного призначення – інформаційного забезпечення користувачів. До цих процесів відносять контроль за системою та її сервісами безпеки та подальше запобігання її злому.

Звідси можна вивести перелік професійних якостей, якими повинні володіти фахівці, які проводять роботи з аналізу захищеності і займаються повсякденним адмініструванням – вміння оцінювати ризики, знання типових загроз і вразливостей, критеріїв і підходів до аналізу захищеності, володіння методами аналізу і спеціалізованим інструментарієм і т. п.

Існує ще одне поняття, тісно пов'язане з поняттям аудиту, – моніторинг інформаційної безпеки, або моніторинг подій, пов'язаних з нею. Даний моніторинг реалізується на основі безперервного спостереження за подіями, що реєструються та пов'язані з інформаційною безпекою. Моніторинг фіксується в рамках технічного аудиту і контролює дотримання базових вимог безпеки і запропонованих регламентів. У процесі моніторингу ці події піддаються ретельному і регулярному аналізу, на основі якого робиться висновок про наявність або відсутність, а також можливості настання інцидента безпеки.

Спеціалізований інструментарій, який використовується при аудиті та моніторингу інформаційної безпеки, включає технічні засоби та інтеграційні рішення з регламентами їх експлуатації. При цьому важливо відзначити, що

значна увага приділяється комплексу організаційно-правових заходів в даній області, наприклад політиці і процедурам реагування на атаки і подальшого відновлення системи.

Для оцінки рівня реальної захищеності інформаційних ресурсів, а значить, правильності реалізації прийнятої в компанії політики безпеки і перевірки ефективності застосовуваних механізмів захисту, використовуються системи аналізу захищеності (САЗ), або сканери безпеки. Використання даних засобів дозволяє здійснити попереджувальний пошук наявних вразливостей в програмному та апаратному забезпеченнях, налаштуваннях або конфігураціях, протестувати захищеність і стійкість системи до злому, моделюючи дії зловмисника, а також сформувати рекомендації щодо усунення виявлених вразливостей і виправити їх. Причому варто відзначити, що завдання аналізу захищеності виникатиме з певною періодичністю – при оновленні компонентів відкритої системи, зміні конфігурацій обладнання та ОС тощо.

САЗ працюють на етапі попередження (з боку адміністратора внутрішньої мережі) або підготовки до вторгнення у внутрішню мережу (з боку зловмисника). Виявляючи і вчасно усуваючи вразливості, САЗ тим самим усувають саму можливість реалізації атаки, що дозволяє знизити витрати (фінансові, людські тощо) на експлуатацію засобів захисту. Технології аналізу захищеності є дієвим методом, що дозволяє проаналізувати і реалізувати політику безпеки перш, ніж здійсниться спроба її порушення зовні або зсередини організації.

Можна провести наступну аналогію охоронних заходів з аналізом захищеності – охоронець, періодично обходить всі поверхи будівлі в пошуках відкритих дверей, незакритих вікон та інших проблем. Також діє і САЗ. Тільки в якості будівлі виступає внутрішня мережа, а в якості незакритих вікон і дверей - її вразливості.

Сканування необхідно для підтвердження стану безпеки і реалізації у відкритій системі механізму превентивного (попереджувального) захисту, але недостатньо для якісного аудиту, оскільки сканери, як правило, шукають заздалегідь відомі вразливості, які внесені в їх бази знань (сигнатур

вразливостей). В результаті залишається невирішене питання: якщо при скануванні не виявлені вразливості, то їх немає насправді або їх не було на момент перевірки в базі сканера? Крім того, при скануванні завжди залишається ймовірність небажаного впливу на елементи системи. Наприклад, істотне збільшення трафіку в досліджуваному сегменті або навіть виведення з ладу сканованого вузла або окремої служби. Також важилим є і той факт, що сканером може скористатися не тільки адміністратор мережі, але і зловмисник, який намагається виявити вразливі ділянки системи для подальшого входу або злому її.

Отже, визначимо САЗ як систему пошуку вразливостей проектування, реалізації та експлуатації, що виконує попереджувальний пошук вразливих місць у внутрішніх мережах шляхом аналізу налаштувань її апаратного і програмного забезпечення (пасивний пошук) і імітацією мережевих атак (активний пошук), а також перевірку функціонування системи при запуску сканерів з різними обліковими записами, відповідними привілеями різних користувачів.

САЗ виконують серію перевірок з виявлення вразливостей, аналогічних тим, які застосовують зловмисники при підготовці та здійсненні атак. Пошук вразливостей ґрунтується на використанні бази даних, яка містить ознаки відомих вразливостей програмного та апаратного забезпечення і може оновлюватися шляхом додавання нових описів вразливостей. Сканування починається з отримання попередньої інформації про систему, наприклад про дозволені протоколи і відкриті порти, про версії ОС тощо, і може закінчуватися спробами імітації проникнення, використовуючи широко відомі атаки, наприклад спуффінг або підбір пароля. САЗ дозволяють швидко визначити всі вузли внутрішньої мережі, доступні в момент проведення сканування, виявити всі використовувані в ній сервіси і протоколи, їх налаштування і можливості для несанкціонованих впливів (як зсередини мережі, так і зовні). Функціонувати такі системи можуть на мережевому рівні, рівні ОС або на рівні додатків.

На сьогодні є велика кількість реалізованих САЗ. Серед них можна знайти не так багато, які б однозначно визначались за типом. Дуже часто вони є

інтегрованими реалізаціями декількох підходів до аналізу захищеності, наприклад, об'єднуючи активний аналіз на мережевому рівні з пасивними методами аналізу на системному рівні. Інтеграція часто відбувається за допомогою функції централізованого керування. Такий підхід важливий для мережного середовища, що не розпізнає чіткої межі між доступом на рівні ОС та доступом на мережному рівні. Правда при цьому експлуатація і супровід модулів комбінованого аналізу вимагає досить значних зусиль.

Мережні САЗ набули найбільшого поширення, в першу чергу тому, що вони універсальні. Вони функціонують на рівні мережі (network-based) і є засобами віддаленого пошуку вразливостей мережної взаємодії.

Вивченість і повсюдне використання таких мережевих протоколів, як IP, TCP, HTTP, FTP, SMTP та інших, значно впливають на захищеність внутрішніх мереж. Перевірка її реалізації в конкретному середовищі з допомогою мережних САЗ дозволяє з високим ступенем ефективності оцінити захищеність цього середовища.

Також мережні САЗ аналізують вразливості системного і прикладного програмного забезпечення, що відповідає за роботу з мережею, наприклад веб-, FTP- і поштові сервери, МЕ, браузери тощо. Крім аналізу програмного забезпечення, деякі пропоновані на ринку засоби проводять сканування і апаратних засобів. Як правило, це обладнання для комутації та маршрутизації.

Варто також зазначити, що мережні САЗ виконують перевірки по мережі дистанційно, можуть використовувати різні методи виявлення однієї і тієї ж вразливості і різні облікові записи для підключення до сканованих об'єктів: при аудиті це максимальні права, при імітації атаки – краще не давати обліковий запис взагалі.

Для вирішення раніше виділених завдань, що стоять під час проведення аналізу захищеності ресурсів інтранету, зазвичай вдаються до чотирьох основних варіантів розміщення агентів мережних САЗ – 2 зовні аналізованого середовища і 2 зсередини [11].

Зовні можливо проаналізувати тільки периметр інтранету або весь інтранет в цілому: з боку мереж філій з досить широкими правами доступу, з боку партнерів – з більш обмеженими правами доступу. Також може проводитись аналіз з довірених мереж або при підключенні через сервер віддаленого доступу на основі прийнятих в компанії спеціальних протоколів і програмно-апаратних рішень.

Зсередини можливий аналіз внутрішньої частини інтранету з ДМЗ або з інших внутрішніх частин цього ж інтранету. Також з внутрішньої мережі можливо здійснити аналіз самої ДМЗ.

Найбільш повне уявлення про стан захисту аналізованої відкритої інформаційної системи, звичайно ж, дає комплексний аналіз всіх зазначених схем.

Існує 2 основних механізми, за допомогою яких мережевий сканер перевіряє наявність в мережі вразливості – сканування і зондування.

Сканування, як завжди перший і важливий крок при аналізі захищеності мережі, являє собою найбільш швидкий і простий для реалізації метод перевірки присутності вразливості на сканованому об'єкті. Це пасивний аналіз, за допомогою якого сканер намагається визначити наявність вразливості за непрямими ознаками. У термінах компаній даний метод отримав назву "логічний висновок". Для цього, згідно з дослідженнями компанії Cisco, здійснюється ідентифікація відкритих портів, знайдених на кожному мережному пристрої, а також збираються і аналізуються банери (заголовки відповідей на запити сканерів або відповідні привітання) доступних сервісів, знайдені при скануванні кожного порту. Кожен отриманий заголовок порівнюється з базою даних визначення мережних пристроїв, ОС і потенційних вразливостей. На основі проведеного порівняння робиться висновок про наявність або відсутність вразливості. Сканування не призводить до порушення функціонування сервісів або вузлів мережі – для цього використовується інформація, що «добровільно» розсилається досліджуваною системою без підключення до неї (це особливо актуально для бездротових мереж).

У даного механізму є і ряд очевидних недоліків. По-перше, ефективність перевірок заголовків недостатньо висока - адміністратор для ряду служб може при бажанні їх змінити. По-друге, часто версія, що вказується в заголовку відповіді на запит, не завжди говорить про наявність неусуненої вразливості програмного забезпечення. І, нарешті, усунення вразливості в одній версії програмного забезпечення ще не означає, що в наступних версіях ця вразливість буде відсутньою.

Другий вид аналізу – зондування. Це активний аналіз, який дозволяє переконатися, присутня чи ні на аналізованому об'єкті вразливість. Згідно компанії Cisco цей процес використовує інформацію, отриману в процесі сканування для детального аналізу кожного мережного пристрою. Цей метод заснований не на перевірці версій програмного забезпечення в заголовках, а на порівнянні «відбитка» його фрагмента зі «зліпком» відомої вразливості. Цей принцип аналогічний до роботи антивірусів, які порівнюють фрагменти сканованого програмного продукту з сигнатурами вірусів в базі даних. Для цього на систему здійснюються ключові впливи, що використовують перевірку вразливості, з явним підключенням до системи і аналізуються відгуки. У даного процесу, під яким розуміється послідовність дій, спрямованих на підтвердження наявності і використання виявлених вразливостей системи, є ще 2 назви: «етичне хакерство» або «тест на проникнення». Якщо в результаті роботи сканера у відповідь приходить командний рядок, то це означає, що вразливість в системі присутня. Мета тесту – це пошук способів отримання доступу до системи за допомогою інструментів і прийомів, використовуваних зловмисником. Іншими словами, тест на проникнення покликаний оцінити, наскільки легко суб'єкту, що виконує тест, отримати несанкціонований доступ до інформаційних і мережних ресурсів компанії.

Зондування рекомендується проводити для особливо критичних систем, з попереднім повідомленням IT-персоналу або без нього. Причому тестування найкраще здійснювати зовні і зсередини (з певним рівнем привілеїв і оцінкою можливості підвищення цих привілеїв).

Іноді зондування дозволяє виявити інші уразливості, які не можуть бути виявлені пасивними методами. Одним з різновидів зондування є перевірка контрольних сум або дати сканованого програмного забезпечення, які реалізуються в сканерах, що працюють на рівні ОС.

Роботи з проведення тестування можуть мати також вторинні цілі, наприклад тестування процедури ідентифікації та реакції на інциденти, перевірки інформованості користувачів, відповідності системи політиці безпеки тощо.

Цей метод більш повільний і трудомісткий, ніж пасивне сканування, але майже завжди більш точний та надійний. Також зондування може створити значне навантаження на мережу. Також до недоліків відносять те, що перевірка деяких вразливостей, які запускають реальні атаки, призводить до виведення з ладу сервісу або комп'ютера. Часто такі вразливості не можуть бути протестовані в ситуаціях, коли тест призводить до відмови в обслуговуванні аналізованого вузла або мережі, або коли вразливість в принципі не придатна для реалізації атаки на мережу. Якщо є ризик виведення з ладу тестованих вузлів, тоді в багатьох компаніях потрібно отримати письмовий дозвіл на проведення тестування.

В даному проекті у зв’язку з обмеженістю ресурсів тестування функціоналу мережі буде проводитись простішими реалізаціями. Так для перевірки працездатності мережі будуть використані 3 віртуальні машини на базі ОС Windows XP та Windows 7, по одній в кожному офісі спрощеної топології. За їх допомоги буде можливість як доступність відповідних мереж, так і доступність візуальної складової веб-сервера.

Що ж до перевірки захисту, то тут буде використана віртуальна машина на базі ОС Kali Linux. Дана ОС створена спеціально для атак як на мережне обладнання, так і на кінцеві пристрої. Ще одною перевагою Kali Linux для даних дій є те, що більшість популярних додатків для атак є встановленими за замовчуванням.

Висновки до розділу 2

Була спроектована мережа організації, що складається з шести офісів. Обґрунтовано дослідження трьох офісів. Сформовані таблиці параметрів інтерфейсів пристроїв та адресації підмереж для трьох офісів.

Обрані пристрої, на яких базуватиметься підсистема периметрового захисту. Описані можливості обладнання, які можуть використовуватись для поставленого завдання, обрані та обґрунтовані основні з них.

Сформоване уявлення про поняття «політика безпеки інформації». Розроблена базова політика безпеки організації, реалізація якої дозволить забезпечити надійний інформаційний захист кожного з офісів.

Проаналізовані різні САЗ та обрана САЗ на базі Kali Linux. Спроектований сценарій тестування функціоналу та захищенності підсистеми.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ

3.1. Базове налагодження пристроїв мережі

В даному пункті розглянуто базові налаштування пристроїв спрощеної мережі. Для повного розуміння, який пристрій налаштовується, зручності конфігурування та перевірки зв'язку між пристроями по імені стандартні імена елементів мережі були змінені на ті, які відповідають проекту (рис. 3.1).

```
Switch#en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host Switch1-1
Switch1-1(config)#
```

Рис. 3.1. Налаштування імені на комутаторі Switch1-1

Основою будь-якої мережі є адресація, тому після зміни імен було налаштовано статичну адресацію інтерфейсів мережі. За відповідною адресою пристрої будуть знаходити один одного у мережі.

Розрізняють «білі» та «сірі» IP-адреси. Перші застосовуються в глобальній мережі і є загальнодоступними для зв'язку з Інтернету. Другі – зазвичай застосовуються для внутрішніх (локальних) мереж і існують тільки там. Через це вони, навідміну від «білих» адрес, можуть повторюватись. У фрагменті лістингу показане налаштування «білої» адреси на інтерфейсі GigabitEthernet0/0 маршрутизатора Router2 для з'єднання з глобальною мережею (рис. 3.2).

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#int g1/0
Router2(config-if)#ip add 2.2.2.2 255.255.255.252
Router2(config-if)#no sh
Router2(config-if)#
*May  6 14:16:45.227: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*May  6 14:16:46.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
Router2(config-if)#ex
Router2(config)#
```

Рис. 3.2. Налаштування статичної IP-адреси на маршрутизаторі Router2

Також статичні IP-адреси використовуються для ідентифікації пристрою у процесі віддаленого керування. Для зручності віддаленого керування

комутаторами були налаштовані IP-адреси інтерфейсів VLAN1 на кожному з них (рис. 3.3).

```
Switch1-1(config)#int vlan 1
Switch1-1(config-if)#ip add 193.2.3.126 255.255.255.252
Switch1-1(config-if)#no sh
Switch1-1(config-if)#ex
Switch1-1(config)#
```

Рис. 3.3. Налаштування статичної IP-адреси для інтерфейсу VLAN1 на комутаторі Switch1-1

За рахунок відповідних масок IP-адрес підмереж віддалене підключення можливе до комутаторів можливе лише з одного пристрою та лише зсередини віднопідної локальної мережі. Це робиться для зменшення ймовірності зловмисних дій щодо корегування роботи комутаторів.

Далі на комутаторах було зроблене розділення внутрішньої мережі на підмережі. Для цього були налаштовані віртуальні локальні мережі (VLAN). Дана структрура реалізується за допомогою тегування трафіка, де вказується приналежність до тієї чи іншої VLAN. Детальний опис цього є у відкритому стандраті IEEE 802.1Q. В подальшому використання VLAN дозволить контролювати трафік між ними за рахунок пристроїв маршрутизації, та у разі потреби – блокувати/дозволяти його. Приклад налагодження VLAN представлений на рис. 3.4.

```
Switch1-1(config)#vlan 10
Switch1-1(config-vlan)#name LAN_VM
Switch1-1(config-vlan)#exit
Switch1-1(config)#int e0/0
Switch1-1(config-if)#switchport mode access
Switch1-1(config-if)#switchport access vlan 10
Switch1-1(config-if)#ex
```

Рис. 3.4. Налаштування VLAN 10 та прив'язка порта до нього на комутаторі Switch1-1

Для доступності обміну всіх VLAN між собою та іншими мережами, в тому числі і глоабльними, на комутаторах були налагоджені транкові канали зв’язку. Дані канали допускають проходження трафіку з вибраних VLAN, що і дозволяє досягти вищесказаного. Приклад налагодження подібного каналу показаний на рис. 3.5.

```
Switch1-1(config)#int range e1/2-3
Switch1-1(config-if-range)#switchport trunk encapsulation dot1q
Switch1-1(config-if-range)#switchport mode trunk
Switch1-1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch1-1(config-if-range)#
```

Рис. 3.5. Налаштування транкового каналу на комутаторі Switch1-1

Відповідно з боку обладнання маршрутизації також були проведені налаштування транкових каналів зв'язку. Задля цього були визначені та сконфігуровані мережні підінтерфейси на інтерфейсах, що підключені до комутаторів. В налаштуваннях підінтерфейсів вказується метод інкапсуляції та приналежність до відповідної VLAN. Подібне налаштування на маршрутизаторах та МЕ дещо відрізняється, що видно на рис. 3.6-3.7.

```
Router3(config)#int g0/0
Router3(config-if)#no ip add
Router3(config-if)#no sh
Router3(config-if)#int g0/0.10
Router3(config-subif)#encapsulation dot1q 10
Router3(config-subif)#ip add 195.2.3.1 255.255.255.240
Router3(config-subif)#ex
```

Рис. 3.6. Налаштування підінтерфейса на маршрутизаторі Router3

```
Firewall1# conf t
Firewall1(config)# int g0/0
Firewall1(config-if)# no shut
Firewall1(config-if)# int g0/0.10
Firewall1(config-subif)# vlan 10
Firewall1(config-subif)# ip add 193.2.3.1 255.255.255.240
Firewall1(config-subif)# ex
```

Рис. 3.7. Налаштування підінтерфейса на МЕ Firewall1

Далі були сконфігуровані IP-адреси кінцевих пристроїв. Вони були згенеровані за рахунок протокол динамічного конфігурування вузлів DHCP. Даний протокол дозволяє автоматично видавати для кінцевого пристрою всі потрібні налаштування мережі – IP-адресу, маску підмережі, шлюз за замовчуванням, адресу DNS (Domain Name Server) та ім'я домену підмережі. Для реалізації відповідних дій на маршрутизуючих пристроях Router3, Firewall1 та Firewall2, які мають підключення до підмереж через комутатори, даний був налагоджений цей протокол. Синтаксис даної конфігурації маршрутизатора та МЕ також дещо відрізняється (рис. 3.8-3.9).

```
Router3(config)#ip dhcp exc 195.2.3.1
Router3(config)#ip dhcp pool LAN-VM
Router3(dhcp-config)#network 195.2.3.0 255.255.255.240
Router3(dhcp-config)#def 195.2.3.1
Router3(dhcp-config)#domain office3.com
Router3(dhcp-config)#dns 8.8.8.8
Router3(dhcp-config)#exit
```

Рис. 3.8. Налаштування DHCP на маршрутизаторі Router3

```
Firewall2(config)# dhcpd dns 8.8.8.8
Firewall2(config)# dhcpd dom office2.com
Firewall2(config)# dhcpd add 194.2.3.2-194.2.3.14 inside1
Firewall2(config)# dhcpd enable inside1
Firewall2(config)#
```

Рис. 3.9. Налаштування DHCP на ME Firewall2

Для взаємодії різних мереж між собою використовуються статичні маршрути або динамічні протоколи маршрутизації. Так як мережа одного офісу складається лише з одної підмережі, то немає сенсу використовувати останні. Тому між граничними пристроями мереж та глобальною мережею Internet були налаштовані статичні маршрути за замовчуванням (див. рис. 3.10-3.11). Даний статичний маршрут ще називають «шлюзом останньої надії». Сенс значення в тому, що коли маршрутизуюче обладнання «не знаходить» підмережу в таблиці маршрутизації, воно пересилає пакет на даний статичний маршрут. Даний принцип розрахований на те, що віддалений пристрій маршрутизації, який і є цим шлюзом, має цю адресу в таблиці маршрутизації. Якщо ж ні, то пакет пересилається далі до тих пір, поки не знайдеться потрібна адреса.

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1
Router2(config)#
```

Рис. 3.10. Налаштування статичного маршруту за замовчуванням на маршрутизаторі Router2

```
Firewall2# conf t
Firewall2(config)# route outside 0.0.0.0 0.0.0.0 194.168.1.2
Firewall2(config)#
```

Рис. 3.11. Налаштування статичного маршруту за замовчуванням на ME Firewall2

Для маршрутизації в мережі Інтернет на сьогодні зазвичай використовується протокол динамічної маршрутизації BGP (Border Gateway Protocol). Даний протокол відноситься до класу протоколів зовнішнього шлюзу. При використанні протоколів даного класу таблиці маршрутизації не розсилаються сусідам, так як це робиться у внутрішньошлюзових протоколах (OSPF, EIGRP), що дозволяє істотно знизити навантаження на апаратну частину маршрутизаторів. Щоб забезпечити взаємодію локальної мережі із глобальною слід «розповісти» про свою мережу сусідньому маршрутизатору із глобальної мережі (рис. 3.12-3.13).

```
Router2(config)#router bgp 2200
Router2(config-router)#neighbor 2.2.2.1 remote-as 5500
Router2(config-router)#ex
Router2(config)#
```

Рис. 3.12. Налаштування протоколу динамічної маршрутизації BGP на маршрутизаторі Router2

```
Firewall1(config)# router bgp 1100
Firewall1(config-router)# address-family ipv4 unicast
Firewall1(config-router-af)# neighbor 1.1.1.1 remote-as 5500
Firewall1(config-router-af)# neighbor 1.1.1.1 activate
Firewall1(config-router-af)# ex
Firewall1(config-router)# ex
Firewall1(config)#
```

Рис. 3.13. Налаштування протоколу динамічної маршрутизації BGP на МЕ Firewall1

Також для зручності подальшого налаштування на маршрутизуючому обладнанні були створені об'єкти мережі. Це дозволить замінити IP-адреси підмереж чи окремих кінцевих пристроїв назвами. Подібні принципи діють у об’єктно-орієнтованому програмуванні, де вже не раз довели свою перевагу. Дане налаштування одноманітне на маршрутизаторах та МЕ (рис. 3.14).

```
Router3(config-network-group)#object-group network inside5
Router3(config-network-group)#195.2.3.64 255.255.255.240
```

Рис. 3.14. Створення об’єктів мережі на маршрутизаторі Router3

3.2. Налагодження підсистеми периметрового захисту

Будь-яка політика безпеки мережі починається з захисту підключення до мережних пристроїв. Даний проект не є вийнятком, тому був налагоджений захист консольного та віддаленого підключення до комутаторів за допомогою протоколу віддаленого підключення Telnet (рис. 3.15-3.17).

```
Switch1-1(config)#banner motd #Switch 1-1 / Location - Office1#
Switch1-1(config)#line console 0
Switch1-1(config-line)#password toor
Switch1-1(config-line)#login
Switch1-1(config-line)#exit
Switch1-1(config)#
```

Рис. 3.15. Налаштування повідомлення-банера та паролю на консольне підключення на комутаторі Switch1-1

```
Switch3(config)#username admin privilege 15 secret adminpass
Switch3(config)#username technic privilege 5 secret technicpass
Switch3(config)#enable secret cisco
Switch3(config)#login block-for 300 attempts 3 within 3
Switch3(config)#login delay 5
Switch3(config)#login on-failure log
Switch3(config)#login on-success log
Switch3(config)#ip domain-name office3.com
```

Рис. 3.16. Конфігурування облікових записів та налаштувань віддаленого підключення на комутаторі Switch3

```
Switch2(config)#service password-encryption
Switch2(config)#service tcp-keepalives-in
Switch2(config)#service tcp-keepalives-out
Switch2(config)#ip telnet hidden addresses
Switch2(config)#ip telnet quiet
Switch2(config)#line vty 0 4
Switch2(config-line)#login local
Switch2(config-line)#transport input telnet
Switch2(config-line)#transport output telnet
Switch2(config-line)#logging synchronous
Switch2(config-line)#exi
Switch2(config)#
```

Рис. 3.17. Конфігурування шифрування та каналу віддаленого підключення на комутаторі Switch2

На маршрутизаторах та ME був налагоджений подібний захист. Так як ці пристрої є граничними в своїх мережах, а отже потребують вищого рівня захисту, то для віддаленого підключення буде використовуватись більш захищений протокол – SSH (Secure Shell) (див. рис. 3.18-3.19).

Даний протокол, на відміну від Telnet, шифрує повідомлення віддаленого доступу, а не передає їх в відкритому вигляді. Це знижує ризик того, що дана інформація буде доступна зловмисникам.

```
Router3(config)#username admin privilege 15 secret adminpass
Router3(config)#username technic privilege 5 secret technicpass
Router3(config)#enable secret cisco
Router3(config)#login block-for 300 attempts 3 within 3
Router3(config)#login delay 5
Router3(config)#login on-failure log
Router3(config)#login on-success log
Router3(config)#ip domain-name office3.com
Router3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Router3.office3.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router3(config)#
*May 13 09:11:58.327: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router3(config)#ip ssh version 2
Router3(config)#ip ssh time-out 60
Router3(config)#ip ssh authentication-retries 5
Router3(config)#ip ssh maxstartups 5
Router3(config)#ip ssh logging events
Router3(config)#line vty 0 4
Router3(config-line)#login local
Router3(config-line)#transport input ssh
Router3(config-line)#transport output ssh
Router3(config-line)#logout-warning 30
Router3(config-line)#absolute-timeout 10
Router3(config-line)#logging synchronous
Router3(config-line)#exit
Router3(config)#
```

Рис. 3.18. Налаштування захисту віддаленого підключення на маршрутизаторі Router3

```
Firewall2(config)# banner motd Firewall 2 / Location Office2
Firewall2(config)# domain-name office2.com
Firewall2(config)# ssh 194.2.3.120 255.255.255.248 management
Firewall2(config)# ssh timeout 60
Firewall2(config)# ssh version 2
Firewall2(config)# username technic password technicpass privilege 5
Firewall2(config)# username admin password adminpass privilege 15
Firewall2(config)# aaa authentication ssh console LOCAL
Firewall2(config)# enable password cisco
Firewall2(config)# crypto key generate rsa general-keys modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
Firewall2(config)#
```

Рис. 3.19. Налаштування захисту віддаленого підключення на ME Firewall2

В першому офісі для захисту мережі використовується два МЕ експертного рівня Cisco ASA у відмовостійкому режимі. Це забезпечить захист периметра мережі від апаратних збоїв.

Перед налагодженням даного режиму конфігурація інтерфейсів, що з'єднують два апаратних МЕ, була очищена. З усіх налаштувань залишилась лише активація самого інтерфейсу. Для налагодження відмовостійкого режиму на МЕ слід вказати його порядковий номер словами «primary» чи «secondary», а також відповідний інтерфейс, за яким МЕ буде шукати свого «сусіда». Конфігурація проводиться однаково з обох сторін і відрізняється лише порядковим номером пристрою (рис. 3.20).

```
Firewall1(config)# failover
Firewall1(config)# failover lan unit primary
Firewall1(config)# failover lan interface STATE g0/1
INFO: Non-failover interface config is cleared on GigabitEthernet0/1 and its sub-interfaces
Firewall1(config)# failover polltime unit 1 holdtime 3
Firewall1(config)# failover link STATE g0/1
Firewall1(config)# failover interface ip STATE 1.1.2.1 255.255.255.252 standb$
```

Рис. 3.20. Налаштування режиму відмовостійкості на МЕ Firewall1

Після цього вся конфігурація МЕ primary буде скопійована на МЕ secondary. Далі за замовчуванням перший МЕ залишиться в активному режимі, а другий – в пасивному. При бажанні це можна змінити відповідною командою.

В додаток до різного синтаксису налаштування, на МЕ для взаємодії кінцевих пристроїв, що знаходяться в різних віртуальних мережах слід дозволити трафік між підінтерфейсами (див. рис. 3.21). Ця різниця налаштувань за замовчуванням з'являється із-за різного підходу до захисту мережі на маршрутизаторах та МЕ. Маршрутизатори застосовують принцип «дозволено все, що не заборонено», а МЕ – «заборонено все, що не дозволено».

```
Firewall1# conf t
Firewall1(config)# same-security-traffic permit inter-interface
Firewall1(config)#
```

Рис. 3.21. Налаштування дозволу трафіку між підінтерфейсами на МЕ Firewall1

Для обміну трафіком з глобальною мережею, окрім «шлюзу останньої надії», на маршрутизуючих пристроях була налаштована трансляція мережних адрес NAT (див. рис. 3.22-3.23). Трансляція виконає дві важливі функції:

1. забезпечить взаємодію між внутрішніми та зовнішньою підмережами;
2. «приховає» внутрішню мережу ззовні.

Таким чином глобальна мережа буде «бачити» лише одну зовнішню адресу офісу, що забезпечить кращий захист внутрішньої мережі від доступу ззовні.

```
Router3(config)#int g0/0.40
Router3(config-subif)#ip nat inside
Router3(config-subif)#exit
Router3(config)#int g1/0
Router3(config-if)#ip nat outside
Router3(config-if)#exit
Router3(config)#ip access-list standard NAT
Router3(config-std-nacl)#permit 195.2.3.0 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.16 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.32 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.48 0.0.0.15
Router3(config-std-nacl)#exit
Router3(config)#ip nat inside source list NAT interface g1/0 overload
```

Рис. 3.22. Налаштування NAT на маршрутизаторі Router3

```
Firewall1(config)# object network inside1
Firewall1(config-network-object)# subnet 193.2.3.0 255.255.255.240
Firewall1(config-network-object)# nat (inside1,outside) dynamic interface
Firewall1(config-network-object)# exit
Firewall1(config)#
```

Рис. 3.23. Налаштування NAT на ME Firewall1

Для того, щоб реалізувати частину політики безпеки що стосується ДМЗ, на ME слід скорегувати мережні об’єкти, додавши ще одну статичну трансляцію адрес (див. рис. 3.24). На даному етапі зовнішня адреса транслюється у адресу сервера, що міститься в офісі. Це робиться для того, щоб з мережі Інтернет був доступ до внутрішніх серверів, на яких містяться дані, які мають бути доступні в глобальній мережі. Але, щоб забезпечити безпеку серверу, трансляція проводиться лише за потрібними портами. Дане налаштування називають переадресацією портів (Port Forwarding) або ж «прокиданням» портів. В даному випадку для прикладу була налаштована переадресація портів для внутрішнього веб-сервера та порту 80, що відповідає протоколу HTTP – HyperText Transfer Protocol. Для реалізації подібного на реальному обладнанні слід використовувати захищений різновид HTTP – HTTPS.

```
Firewall1(config)# object network dmz
Firewall1(config-network-object)# host 193.2.3.130
Firewall1(config-network-object)# nat (dmz,outside) static interface service t$
Firewall1(config-network-object)# exit
Firewall1(config)#
```

Рис. 3.24. Корегування мережного об’єкта ДМЗ на МЕ Firewall1

Також для забезпечення безпеки були налаштовані списки доступу. Це правила, за якими виконується фільтрація мережного трафіку, яка в свою чергу дозволяє чи забороняє проходження того чи іншого трафіку. Для більшої впевненості в захисті, фільтрація була налаштована не тільки на зовнішньому інтерфейсі, але й на тому, що прямує відповідно до сервера (рис. 3.25-3.27).

```
Router2(config)#ip access-list extended OUTFILTER
Router2(config-ext-nacl)#permit ip any any reflect IPTRAFFIC
Router2(config-ext-nacl)#ex
Router2(config)#ip access-list extended INFILTER
Router2(config-ext-nacl)#evaluate IPTRAFFIC
Router2(config-ext-nacl)#permit tcp any host 2.2.2.2 eq 80
Router2(config-ext-nacl)#ex
Router2(config)#int g1/0
Router2(config-if)#ip access INFILTER in
Router2(config-if)#ip access OUTFILTER out
Router2(config-if)#ex
Router2(config)#
```

Рис. 3.25. Налаштування списків доступу вхідного та вихідного трафіку на маршрутизаторі Router3

```
Firewall1(config)# access-list outside extended permit tcp any object dmz eq 80
Firewall1(config)# access-group outside in interface outside
Firewall1(config)#
```

Рис. 3.26. Налаштування списку доступу вихідного трафіку на МЕ Firewall1

```
Firewall2(config)# access-list DMZ extended permit tcp any object dmz eq www
Firewall2(config)# access-group DMZ out interface dmz
Firewall2(config)#
```

Рис. 3.27. Налаштування списків доступу вхідного трафіку на МЕ Firewall2

Також списки доступу були налаштовані для обміну трафіком робочих станцій з підмережею принтерів (див. рис. 3.28-3.29). Це зроблено для того, щоб забезпечити безпеку мережі на той випадок, коли зловмисник буде під’єднуватись з даної мережі. Для вхідного та вихідного трафіку для прикладу був дозволений для проходження лише один протокол – LPD (Line Printer Daemon), який відповідає порту 515.

```
Router3(config)#ip access-list extended PRINTERS
Router3(config-ext-nacl)#permit tcp object inside1 object inside5 eq lpd
Router3(config-ext-nacl)#permit tcp object inside2 object inside5 eq lpd
Router3(config-ext-nacl)#permit tcp object inside3 object inside5 eq lpd
Router3(config-ext-nacl)#permit tcp object inside4 object inside5 eq lpd
Router3(config-ext-nacl)#permit udp object inside5 host 195.2.3.65 eq bootpc
Router3(config-ext-nacl)#permit udp object inside5 host 195.2.3.65 eq bootps
Router3(config-ext-nacl)#ex
Router3(config)#int g0/0.50
Router3(config-subif)#ip access PRINTERS out
Router3(config-subif)#ex
```

Рис. 3.28. Налаштування списків доступу до підмережі принтерів на маршрутизаторі Router3

```
Firewall2# conf t
Firewall2(config)# access-list PRINTERS extended permit tcp object inside1 obj$
Firewall2(config)# access-list PRINTERS extended permit tcp object inside2 obj$
Firewall2(config)# access-list PRINTERS extended permit tcp object inside3 obj$
Firewall2(config)# access-list PRINTERS extended permit tcp object inside4 obj$
Firewall2(config)# access-group PRINTERS in interface inside5
Firewall2(config)# access-group PRINTERS out interface inside5
Firewall2(config)#
```

Рис. 3.29. Налаштування списків доступу до підмережі принтерів на ME Firewall2

Для взаємодії офісів між собою були створені приватні віртуальні мережі – VPN (Virtual Private Network). Це надасть змогу безпечно обмінюватись інформацією між офісами. В даному проекті був використаний розповсюджений та найбільш підтримуваний тип VPN для з'єднання типу «мережа-мережа» – IPSec Site-To-Site VPN. Налагодження, що стосуються створення таких мереж, мають в 2 етапи – створення тунелю та налагодження передачі шифрованого трафіку.

Для створення даної мережі необхідно, щоб налаштування на кожному з етапів були однаковими. Першим кроком є створення політики шифрування (рис. 3.30-3.31).

```
Router3(config)#crypto isakmp policy 1
Router3(config-isakmp)#hash sha
Router3(config-isakmp)#authentication pre-share
Router3(config-isakmp)#group 5
Router3(config-isakmp)#lifetime 3600
Router3(config-isakmp)#encryption aes 256
Router3(config-isakmp)#ex
Router3(config)#
```

Рис. 3.30. Створення політики шифрування на маршрутизаторі Router3

```
Firewall1(config)# crypto ikev1 policy 1
Firewall1(config-ikev1-policy)# hash sha
Firewall1(config-ikev1-policy)# authentication pre-share
Firewall1(config-ikev1-policy)# group 5
Firewall1(config-ikev1-policy)# lifetime 3600
Firewall1(config-ikev1-policy)# encryption aes-256
Firewall1(config-ikev1-policy)# ex
Firewall1(config)#
```

Рис. 3.31. Створення політики шифрування на ME Firewall1

Наступним кроком є створення тунелю по ключу автентифікації. В даному випадку для прикладу будуть створюватись по 2 тунеля від кожного офісу, щоб забезпечити повну взаємодію між трьома офісами. На реальному обладнанні їх може бути більше. Приклад налагодження показаний на рис. 3.32-3.33.

```
Router3(config)#crypto isakmp key Office1ToOffice3 add 1.1.1.2
Router3(config)#
```

Рис. 3.32. Створення ключа для тунелю на маршрутизаторі Router3

```
Firewall1(config)# tunnel-group 3.3.3.2 type ipsec-l2l
Firewall1(config)# tunnel-group 3.3.3.2 ipsec-attributes
Firewall1(config-tunnel-ipsec)# ikev1 pre-shared-key Office1ToOffice3
Firewall1(config-tunnel-ipsec)# ex
Firewall1(config)#
```

Рис. 3.33. Створення ключа для тунелю на ME Firewall1

Ще одним важливим кроком є відловлювання так званого «цікавого» трафіку – трафіку, який буде проходити між офісами. Тому слід створити відповідний список доступу для цього завдання (рис. 3.34-3.35).

```
Router3(config)#$ 103 permit ip 195.2.3.0 0.0.0.63 193.2.3.0 0.0.0.63
Router3(config)#
```

Рис. 3.34. Створення списку доступу для відловлювання «цікавого» трафіку на маршрутизаторі Router3

```
Firewall1(config)# access-list VPN extended permit ip object-group INSIDE obje$
Firewall1(config)#
```

Рис. 3.35. Створення списку доступу для відловлювання «цікавого» трафіку на ME Firewall1

Так як VPN налагоджуються на граничних пристроях мережі, на яких перед цим була налагоджена трансляція адрес, то слід спрямовувати «цікавий»

трафік повз трансляцію у тунелі, що створюються. Налагодження подібного обходу показане на рис. 3.36-3.37.

```
Router3(config)#ip access-list extended NAT
Router3(config-ext-nacl)#deny ip 195.2.3.0 0.0.0.63 193.2.3.0 0.0.0.63
Router3(config-ext-nacl)#permit ip 195.2.3.0 0.0.0.63 any
Router3(config-ext-nacl)#ex
Router3(config)#
```

Рис. 3.36. Налаштування обходу NAT на маршрутизаторі Router3

```
Firewall1(config)# nat (inside1,outside) source static inside1 inside1 destina$
Firewall1(config)# nat (inside2,outside) source static inside2 inside2 destina$
Firewall1(config)# nat (inside3,outside) source static inside3 inside3 destina$
Firewall1(config)# nat (inside4,outside) source static inside4 inside4 destina$
Firewall1(config)#
```

Рис. 3.37. Налаштування обходу NAT на ME Firewall1

На цьому перший етап налаштувань завершується. Надалі створюється правило шифрування трафіку, який буде проходити по створеним тунелям (рис. 3.38-3.39).

```
Router3(config)#crypto ipsec transform-set Offices esp-aes 256 esp-sha-hmac
Router3(cfg-crypto-trans)#mode tunnel
Router3(cfg-crypto-trans)#ex
Router3(config)#
```

Рис. 3.38. Створення правила шифрування трафіку на маршрутизаторі Router3

```
Firewall1(config)# crypto ipsec ikev1 transform-set Offices esp-aes-256 esp-sh$
Firewall1(config)#
```

Рис. 3.39. Створення правила шифрування трафіку на ME Firewall1

Останнім кроком є створення криптокарти, яка «збирає» всі налаштування разом – вказується цікавий трафік, правила шифрування та кінцева точка, куди спрямовується трафік. Для того, щоб застосувати криптокарту, слід вказати на якому інтерфейсі їй слід виконуватись. Як і всі інші налаштування, ці налаштування на маршрутизаторах та ME дещо відрізняються (рис. 3.40-3.41).

```
Router3(config)#crypto map OfficesMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router3(config-crypto-map)#match address 103
Router3(config-crypto-map)#set transform-set Office1-Office3
Router3(config-crypto-map)#set peer 1.1.1.2
Router3(config-crypto-map)#ex
Router3(config)#int g1/0
Router3(config-if)#crypto map OfficesMAP
Router3(config-if)#
*May  6 16:13:03.215: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router3(config-if)#ex
Router3(config)#
```

Рис. 3.40. Створення та застосування криптокарти на маршрутизаторі Router3

```
Firewall1(config)# crypto map OfficesMAP 1 match address 103
Firewall1(config)# crypto map OfficesMAP 1 set peer 3.3.3.2
Firewall1(config)# crypto map OfficesMAP 1 set ikev1 transform-set Office1-Off$
Firewall1(config)# crypto map OfficesMAP interface outside
Firewall1(config)#
```

Рис. 3.41. Створення та застосування криптокарти на ME Firewall1

3.3. Тестування підсистеми периметрового захисту

Тестування підсистеми периметрового захисту проводиться з метою перевірки налаштувань на відповідність до вимог політики безпеки. Тому і тестування доречно проводити відповідно до пунктів даної політики.

Перевірка на розділення на віртуальні підмережі доступна лише з мережного обладнання офісів. Як видно на рис. 3.42, дане розділення існує, тому при необхідності є можливість обмеження проходження трафіку між ними за допомогою маршрутизуючого обладнання.

```
Switch1-1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
10   LAN_VM                           active    Et0/0
20   LAN1                             active    Et0/1
30   LAN2                             active    Et0/2
40   LAN3                             active    Et0/3
50   PRINTERS                         active    Et1/0
60   DMZ                              active    Et1/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Рис. 3.42. Результат команди show vlan на комутаторі Switch1-1

Доступ з глобальної мережі імітуємо за допомогою віртуальної машини на базі Kali Linux, що підключена до того ж маршрутизатора, що імітує Інтернет. Перевіряємо доступність внутрішніх мереж офісів (рис. 3.43).

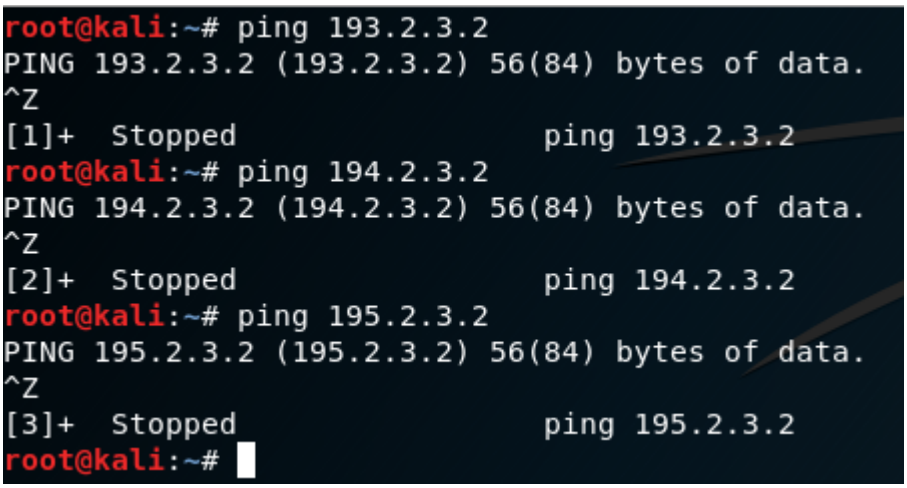


Рис. 3.43. Результат тестування доступності внутрішніх мереж на віртуальній машині RemoteUser

Глобальну мережу Інтернет змоделюємо за допомогою інтерфейса замикання на себе Loopback на маршрутизаторі Internet. Адреса даного інтерфейсу була обрана як 8.8.8.8. Перевірка з'єднання виконана з локальної робочої станції (рис. 3.44).

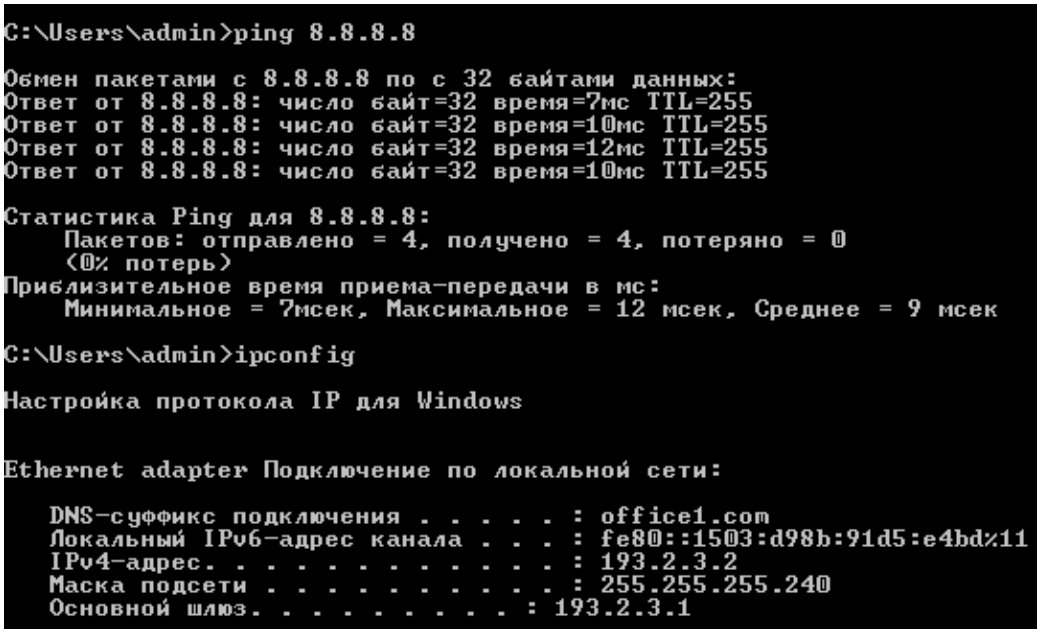


Рис. 3.44. Результат тестування доступності мережі Інтернет на віртуальній машині PC1-VM

Тепер з тієї ж віртуальної машини перевіримо доступність двох сусідніх офісів. Як видно на рис. 3.45, у відповідь на команду *ping <адреса>* приходить кількість переданих байт та час затримки – значить зв'язок є.

```
C:\Users\admin>ping 194.2.3.2

Обмен пакетами с 194.2.3.2 по с 32 байтами данных:
Ответ от 194.2.3.2: число байт=32 время=41мс TTL=128
Ответ от 194.2.3.2: число байт=32 время=44мс TTL=128
Ответ от 194.2.3.2: число байт=32 время=36мс TTL=128
Ответ от 194.2.3.2: число байт=32 время=30мс TTL=128

Статистика Ping для 194.2.3.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 44 мсек, Среднее = 37 мсек

C:\Users\admin>ping 195.2.3.3

Обмен пакетами с 195.2.3.3 по с 32 байтами данных:
Ответ от 195.2.3.3: число байт=32 время=61мс TTL=127
Ответ от 195.2.3.3: число байт=32 время=73мс TTL=127
Ответ от 195.2.3.3: число байт=32 время=28мс TTL=127
Ответ от 195.2.3.3: число байт=32 время=38мс TTL=127

Статистика Ping для 195.2.3.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 28мсек, Максимальное = 73 мсек, Среднее = 50 мсек

C:\Users\admin>ipconfig

Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . : office1.com
   Локальный IPv6-адрес канала . . . : fe80::1503:d98b:91d5:e4bd%11
   IPv4-адрес. . . . . . . . . . . . : 193.2.3.2
   Маска подсети . . . . . . . . . . : 255.255.255.240
   Основной шлюз. . . . . . . . . : 193.2.3.1
```

Рис. 3.45. Результат тестування доступності сусідніх офісів на віртуальній машині PC1-VM

Так як роль мережного принтера виконує VPCS, то відправити документ на друк не є реальним. Тому перевірка робиться за допомогою доступності відповідного порту та адресі. Як видно на рис. 3.46, з'єднання по іншому порту не є вдалим.

```
PC1-1> ping 193.2.3.66 -3 -p 515
Connect   515@193.2.3.66 seq=1 ttl=64 time=5.899 ms
SendData  515@193.2.3.66 seq=1 ttl=64 time=5.468 ms
Close     515@193.2.3.66 seq=1 ttl=64 time=8.282 ms
Connect   515@193.2.3.66 seq=2 ttl=64 time=5.778 ms
SendData  515@193.2.3.66 seq=2 ttl=64 time=5.891 ms
Close     515@193.2.3.66 seq=2 ttl=64 time=5.850 ms
Connect   515@193.2.3.66 seq=3 ttl=64 time=4.528 ms
SendData  515@193.2.3.66 seq=3 ttl=64 time=4.046 ms
Close     515@193.2.3.66 seq=3 ttl=64 time=7.434 ms
Connect   515@193.2.3.66 seq=4 ttl=64 time=8.465 ms
SendData  515@193.2.3.66 seq=4 ttl=64 time=4.418 ms
Close     515@193.2.3.66 seq=4 ttl=64 time=8.232 ms
Connect   515@193.2.3.66 seq=5 ttl=64 time=5.979 ms
SendData  515@193.2.3.66 seq=5 ttl=64 time=4.557 ms
Close     515@193.2.3.66 seq=5 ttl=64 time=5.338 ms

PC1-1> ping 193.2.3.66
193.2.3.66 icmp_seq=1 timeout
193.2.3.66 icmp_seq=2 timeout
193.2.3.66 icmp_seq=3 timeout
193.2.3.66 icmp_seq=4 timeout
193.2.3.66 icmp_seq=5 timeout
```

Рис. 3.46. Результат тестування доступності принтера на VPCS PC1-1

Перевірка зворотнього зв’язку (від принтера до робочих станцій) дає результат, що показаний на рис. 3.47.

```
Printer1> ping 193.2.3.18
193.2.3.18 icmp_seq=1 timeout
193.2.3.18 icmp_seq=2 timeout
193.2.3.18 icmp_seq=3 timeout
193.2.3.18 icmp_seq=4 timeout
193.2.3.18 icmp_seq=5 timeout

Printer1> ping 193.2.3.18 -3 -p 515
Connect   515@193.2.3.18 timeout
Connect   515@193.2.3.18 timeout
Connect   515@193.2.3.18 timeout
Connect   515@193.2.3.18 timeout
Connect   515@193.2.3.18 timeout

Printer1> ping 193.2.3.130
193.2.3.130 icmp_seq=1 timeout
193.2.3.130 icmp_seq=2 timeout
193.2.3.130 icmp_seq=3 timeout
193.2.3.130 icmp_seq=4 timeout
193.2.3.130 icmp_seq=5 timeout
```

Рис. 3.47. Результат тестування доступності робочої станції та веб-сервера на принтері Printer1

Щодо ДМЗ, то тут ситуація трохи складніша, тому що веб-сервер на разі доступний за двома адресами – причиною того є NAT. Із-за останнього сервер у внутрішній мережі має внутрішню адресу, а у зовнішній – зовнішню адресу

граничного маршрутизуючого обладнання (див. рис. 3.48-3.49). Але політику безпеки цей варіант задовольняє.

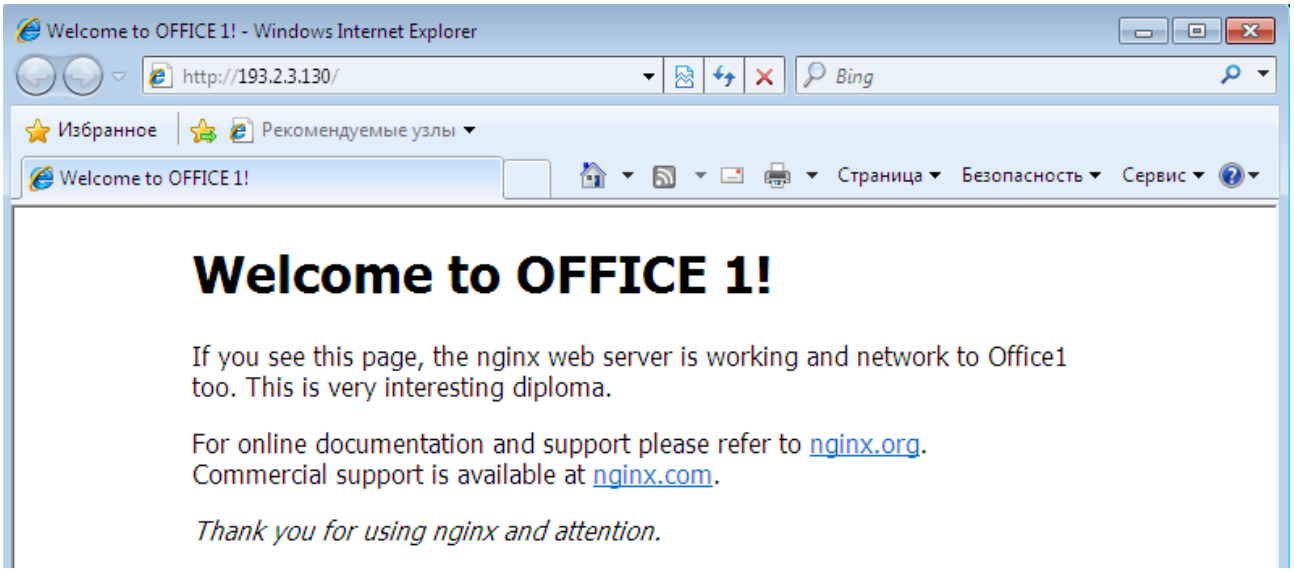


Рис. 3.48. Результат тестування доступності веб-сервера на віртуальній машині PC1-VM

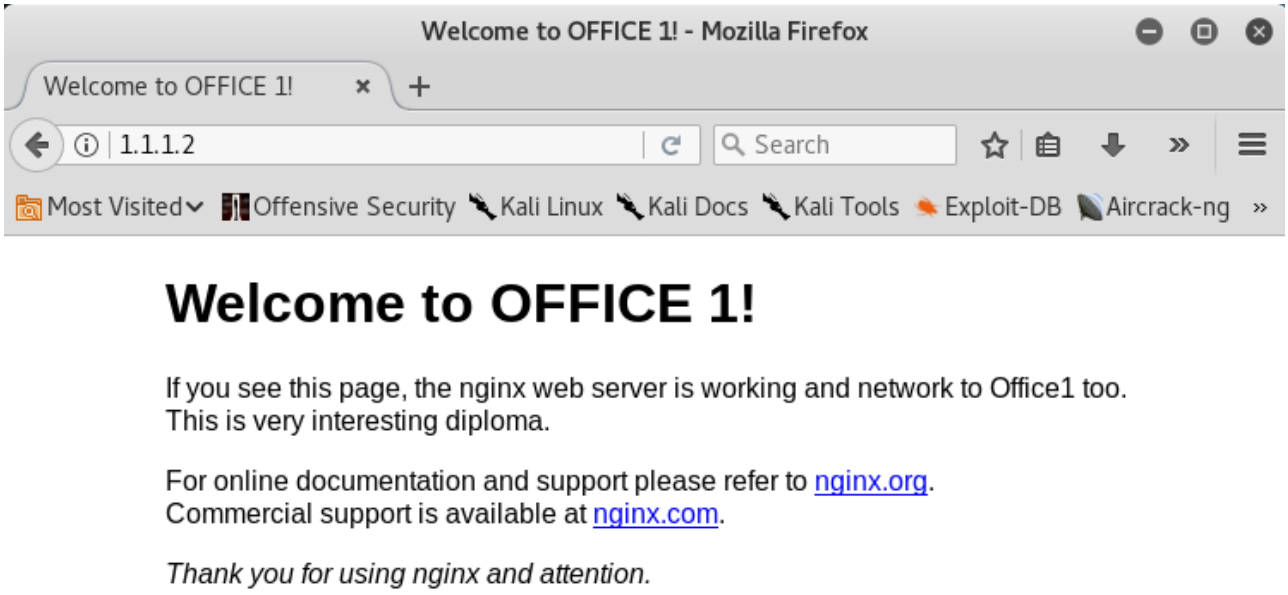


Рис. 3.49. Результат тестування доступності веб-сервера на віртуальній машині RemoteUser

Фізичний доступ до мережного обладнання перевірити неможливо з логічних причин. Тому слід перейти до перевірки віддаленого доступу. Його перевірятимемо за допомогою програмного додатку Putty встановленого на віртуальну машину (рис. 3.50-3.51).

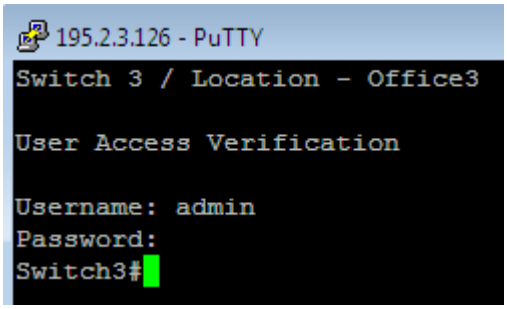


Рис. 3.50. Результат тестування доступності віддаленого доступу до комутатора Switch3

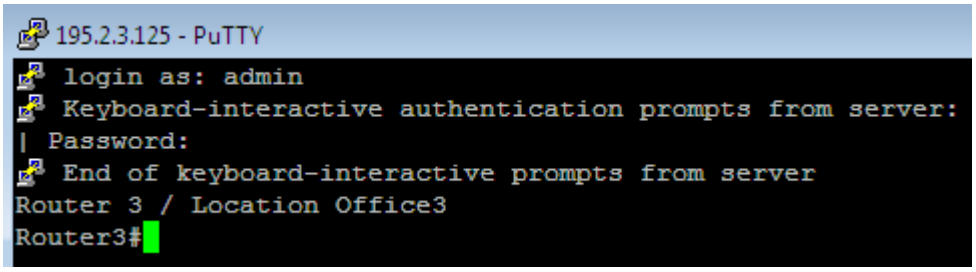


Рис. 3.51. Результат тестування доступності віддаленого доступу до комутатора Router3

Як видно, при підключенні обладнання потребує авторизації користувача, що є одною з потреб політики безпеки.

Тепер спробуємо здійснити розповсюджені атаки на мережу. Першою з них спробуємо атаку за допомогою додатку Cisco Audit Tool або CAT (рис. 3.52).

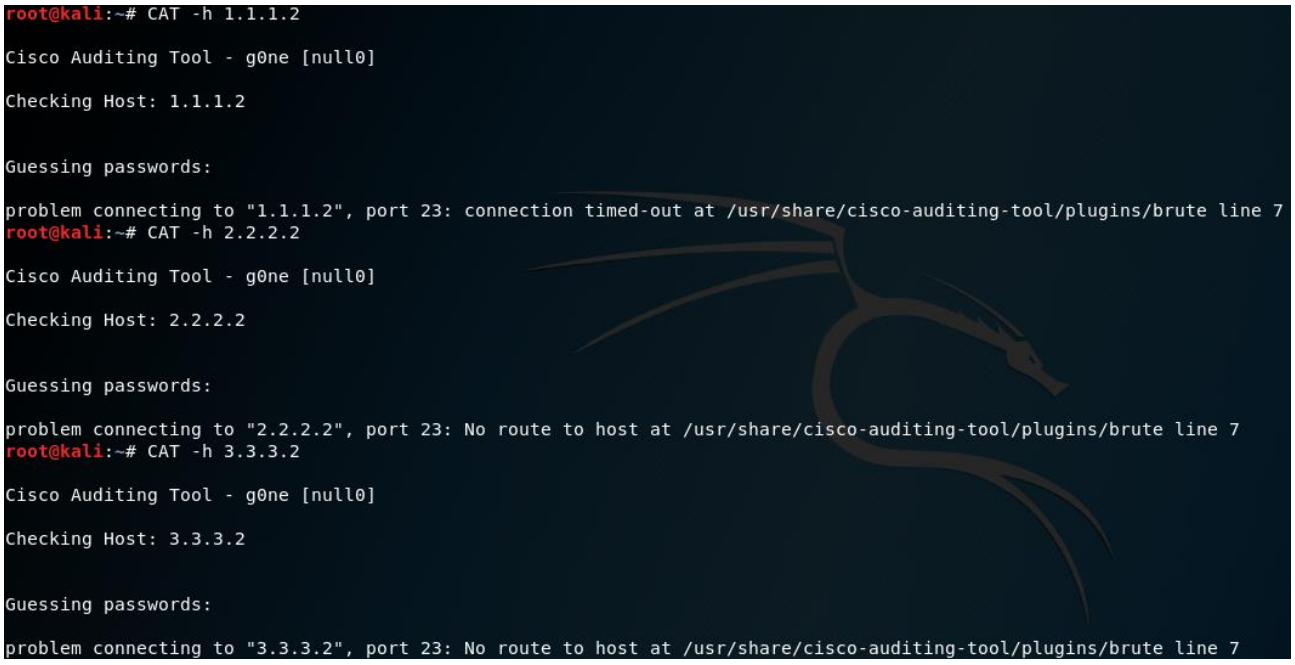


Рис. 3.52. Результат атаки CAT на граничне маршрутизуюче обладнання

Дана атака використовується для брутфорса пароля при вимкненому режимі aaa-mode, брутфорса SNMP community-рядків і перевірки на вразливість IOS History bug.

Наступним використаємо збірник атак, що використовується для експлуатації відомих вразливостей, Cisco Global Exploiter або CGE (рис. 3.53).

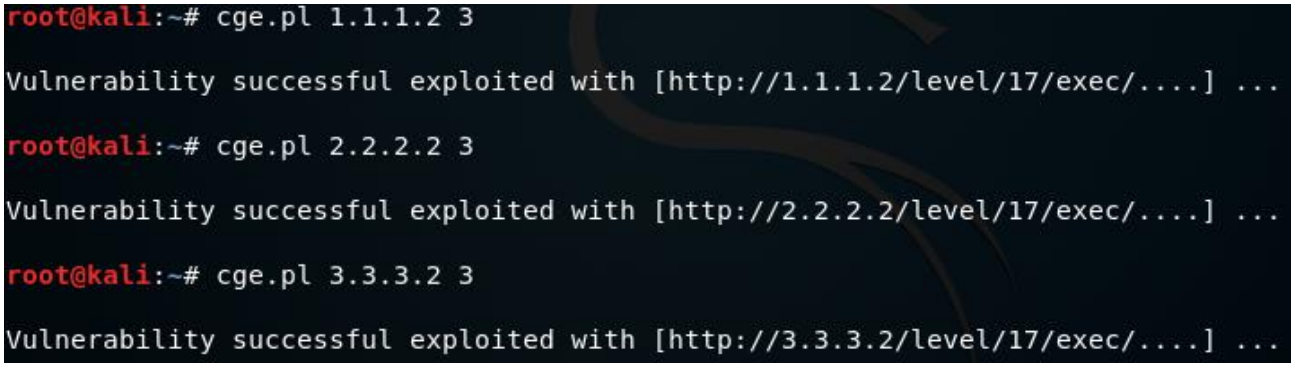


Рис. 3.53. Результат атаки CGE на граничне маршрутизуюче обладнання

Ще одним багатофункціональним сканером вразливостей для обладнання Cisco є cisco-torch. Даний сканер має можливість сканувати кілька IP-адрес одночасно, підвантажуючи їх з текстового файлу. Результат атаки можна побачити на рис. Б.1.

Останньою в переліку буде атака з допомогою додатку copy-router-config.pl. Це інструмент для завантаження поточної конфігурації маршрутизатора Cisco при відомому community-рядку на свій TFTP-сервер. Надалі можна модифікувати конфігурацію і знову завантажити на сервер за допомогою спорідненого додатку merge-copy-config.pl.

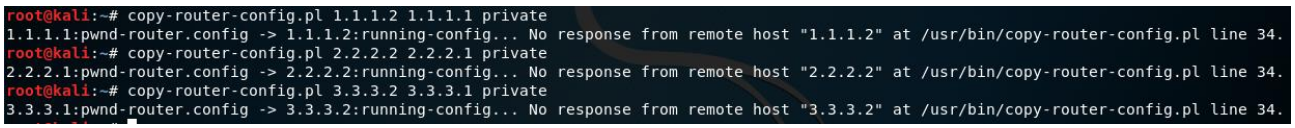


Рис. 3.54. Результат атаки copy-router-config.pl на граничне маршрутизуюче обладнання

3.4. Аналіз результатів тестування

Як і планувалось, усі вимоги політики інформаційної безпеки успішно дотримуються, що видно з результатів атак в попередньому підпункті. Надалі

дана політика може бути модернізована для більш конкретних потреб кожного з офісів. Так, наприклад, якщо в ДМЗ з’являться інші види загальнодоступних серверів, то, відповідно, додатково може бути реалізована переадресація більшої кількості портів до ДМЗ. Або ж, навпаки, усі порти локальної мережі можуть бути заблоковані, якщо відсутня ДМЗ як така.

Що ж до розповсюджених атак, що були проведені, то бачимо, що усі три досліджувані мережі показали себе однаково захищеними в результаті аналогічних досліджень. Як і припускалось, виявлена вразливість веб-сервера, але це досить легко пояснюється. Справа в тому, що в даному проекті не розглядався безпосередньо захист веб-сервера. Даний сервер був обраний для прикладу, тому для простоти конфігурування використовувався незахищений протокол HTTP. При побудові реальної мережі це слід врахувати та використовувати HTTPS, котрий вирішить проблему даної вразливості, тим самим забезпечить більш надійний захист веб-сервера.

Результат усіх інших проведених атак виявився невтішним. Це свідчить про те, що дана мережа має достатню захищеність від зловмисних дій ззовні, а отже, матиме високу стабільність в роботі.

З точки зору логіки, найзахищенішим є другий офіс, так як в ньому використаний подвійний захист – і екрануючий маршрутизатор, і МЕ експертного рівня. Це дозволяє забезпечити захищеність внутрішньої мережі навіть в тих умовах, коли перша лінія оборони, екрануючий маршрутизатор, буде виведена з ладу чи опиниться в руках зловмисника. Але в цьому випадку, виявиться вагомий недолік даної підсистеми захисту: при втраті контролю над екрануючим маршрутизатором відбудеться пошкодження або повна відсутність обміну трафіком з глобальною мережею. Тому основною модернізацією даної підсистеми буде прокладання резервного каналу зв'язку з зовнішньою мережею. При цьому бажано, щоб даний канал надавався іншим провайдером. Це дозволить отримати безперервний зв’язок з мережею Internet навіть тоді, коли будуть наявні системні збої в одного з провайдерів. Також, щоб не один канал не

залишався в пасивному стані, слід було б налаштувати балансування трафіку між ними.

Ще одним недоліком даного типу захисту є його собівартість. Так, як і в будь-якій сфері, чим професійніше обладнання, тим вища його якість, а відповідно і його вартість. Також високою має бути і заробітна плата працівника, який проводитиме його налаштування та обслуговування, у зв'язку з його висококваліфікаційністю. Для невеликої компанії сумарна ціна підсистеми захисту може стати вагомим фактором не на її користь. Тому більшість таких компаній відмовляться від даної підсистеми на користь більш дешевих її аналогів.

З аналогічними проблемами може стикнутись і керівництво компаній, що подібні до першого офісу даного проекту. Ще одною проблемою, з якою можна стикнутись в першому та третьому офісі, є відсутність попереднього захисту, який наявний в другому офісі.

Але є у підсистеми захисту першого офісу і переваги. Найвагомішою з них є те, що при DOS-атаках (відмова в обслуговуванні) мережа залишиться дієздатною. Це можливо за рахунок того, що резервований МЕ експертного рівня підхопить весь вхідний та вихідний трафік мережі, що проходив через МЕ, що відмовив. Також за рахунок цього може залишитись і доступ до мережі Інтернет. Але для того, щоб цей сценарій став можливим, повинна виконуватись ще одна додаткова умова: підключення до глобальної мережі має проводитись по паралельним каналам, а не через комутатор, як це реалізовано в даному проекті підсистеми. Це пояснюється тим, що при DOS-атаках саме комутатор першим дасть збій, чим заблокує весь трафік. Але це, свого роду, є ще одною ланкою захисту локальної мережі.

Найбільш дешевою буде мережа подібна до третього офісу. Але існує складність в налаштуванні її якісного захисту. Вона полягає в тому, що продумати і втілити весь захист з нуля, так як це доводиться робити з екрануючим маршрутизатором, що складає периметр мережі, – досить важка задача, яка потребує уваги, зосередженості та достатнього досвіду системного

адміністратора. Досить часто вразливості даних мереж проявляються через те, що адміністратор не має цих якостей і тому не може налаштувати повноцінний захист.

Висновок до розділу 3

В даному розділі були описані базові налаштування пристроїв мережі: статична та динамічна адресація, статична маршрутизація та маршрутизація по протоколу BGP, транкові канали зв’язку. Для зручності роботи з обладнанням також були налаштовані імена пристроїв та мережні об’єкти.

На мережних пристроях було проведене налагодження віддаленого доступу. Також налаштовані трансляція внутрішніх адрес, віртуальні приватні мережі між офісами, налагоджені списки доступу в мережі.

Проведено тестування функціонування мережі: обмін трафіком всередині підмереж, обмін трафіком з глобальною мережею, доступність веб-серверів. Також проведені розповсюджені атаки на підмережі для перевірки коректності та стабільності роботи підсистеми захисту.

Проведено аналіз результатів тестування та сформовано висновки щодо модернізації та можливостей покращення роботи мережі.

ВИСНОВКИ

В даній кваліфікаційній роботі за результатами аналізу організації периметрового захисту сучасних мереж визначено основні принципи захисту внутрішніх мереж та обрано периметровий захист на базі МЕ. Розроблено підсистему захисту локальних мереж від зовнішніх зловмисних дій.

Було розглянуто 4 існуючих різновида МЕ та проаналізовані їх переваги та недоліки. Дослідження даних різновидів МЕ показали, що для даного проекту слід використовувати екрануючі маршрутизатори та МЕ експертного рівня.

Також були розглянуті вироби провідного виробника мережного обладнання – корпорації Cisco. Проаналізований асортимент, можливості налаштувань та експлуатації обладнання для периметрового захисту локальних мереж.

Також в роботі була спроектована мережа організації, що складається з шести офісів. Обґрунтовано дослідження трьох основних офісів. Сформовані таблиці параметрів інтерфейсів пристроїв та адресації підмереж для трьох офісів.

Обрані пристрої, на яких базується підсистема периметрового захисту. Описані можливості обладнання, які використовуються для поставленого завдання, обрані та обґрунтовані основні з них.

Було сформоване уявлення про поняття «політика безпеки інформації». Розроблена базова політика безпеки організації, реалізація якої дозволить забезпечити надійний інформаційний захист кожного з офісів.

До того ж були проаналізовані різні САЗ та обрана та, що базується на Kali Linux. Спроектований сценарій тестування функціоналу та захищенності підсистеми.

Були описані базові налаштування пристроїв мережі: статична та динамічна адресація, статична маршрутизація та маршрутизація по протоколу BGP, транкові канали зв’язку. Для зручності роботи з обладнанням були налаштовані імена пристроїв та мережні об’єкти.

На мережних пристроях було проведене налагодження віддаленого доступу. До того ж налаштовані трансляція внутрішніх адрес, віртуальні приватні мережі між офісами, налагоджені списки доступу в мережі.

Проведено тестування функціонування мережі: обмін трафіком всередині підмереж, обмін трафіком з глобальною мережею, доступність веб-серверів. Також проведені розповсюджені атаки на підмережі для перевірки коректності та стабільності роботи підсистеми захисту.

Проведено аналіз результатів тестування та сформовано висновки щодо модернізації та можливостей покращення роботи мережі.

Реалізована мережа є повністю готовим макетом реальної реалізації проекту. Конфігурації можуть бути застосовані для налаштування реального обладнання мережі. Макет може використовуватись для дослідження різних атак на подібні або аналогічні мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Информационная безопасность открытых систем. Средства защиты в сетях / С. В.Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – Москва: Горячая линия-Телеком, 2008. – 558 с. – (Горячая линия-Телеком).
2. Основы организации сетей Cisco / Вито Амато., 2004. – 464 с. – ("Вильямс").
3. Access control list [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Access_control_list
4. Configuring IP Access Lists [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html
5. Носов В. В. Технології міжмережних екранів [Електронний ресурс] / В. В. Носов – Режим доступу до ресурсу: http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=98037
6. Калашніков С. Что поставить на периметр сети: Cisco маршрутизатор или Cisco ASA? [Електронний ресурс] / Сергій Калашніков. – 2016. – Режим доступу до ресурсу: https://habr.com/ru/company/cbs/blog/279857/
7. Василенко В. Міжмережні екрани як основа багаторівневого захисту від загроз в комунікаціях розподілених мереж [Електронний ресурс] / Вячеслав Василенко. – 2009. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/9768/3/13.pdf
8. Злом і захист локальної мережі [Електронний ресурс] – Режим доступу до ресурсу: http://pro-computer.pp.ua/3085-zlom-zahist-lokalnoyi-merezh.html
9. Основи захисту периметру корпоративних мереж [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: http://5fan.ru/wievjob.php?id=17306
10. Демілітаризована зона (комп'ютерні мережі) [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Демілітаризована_зона_(комп%27ютерні_мережі)
11. Система обнаружения вторжений [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Система_обнаружения_вторжений

12. NAT [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/NAT
13. Розвивайте бізнес за допомогою IT-рішень Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/dam/global/uk_ua/solutions/small-business/pdf/Cisco_SMB_Buyers_Guide_final.pdf
14. Cisco 7200 Series Routers [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html
15. Cisco 7200 [Електронний ресурс] – Режим доступу до ресурсу: https://www.nstor.ru/ru/catalog/net/oborudovanie-cisco/marshrutizatory-cisco/2026.html
16. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
17. Cisco Catalyst 2960-X - возможности и преимущества [Електронний ресурс] – Режим доступу до ресурсу: http://stornet.ru/articles/cisco_catalyst_2960x_vozmojnosti_i_preimushestva/
18. Cisco ASA 5500 Series Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html
19. Политика безопасности [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Политика_безопасности
20. Носов В. В. Механізми захисту мережі від збору інформації, сканування та проникнення [Електронний ресурс] / В. В. Носов – Режим доступу до ресурсу: http://lib.univd.edu.ua/?controller=service&action=downloadRep&id=119247
21. Міжмережеві екрани [Електронний ресурс] – Режим доступу до ресурсу: https://ua.kursoviks.com.ua/metodychni_vkazivky/article_post/830-tema-mizhmerezhevi-yekrani-navchalniy-posibnik-internet-dlya-koristuvacha-chastina-2-nudpsu

22. Политика реализации межсетевых экранов [Електронний ресурс] – Режим доступу до ресурсу: https://helpiks.org/9-27381.html
23. Политика информационной безопасности — опыт разработки и рекомендации [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/174489/
24. Политика межсетевого экранирования [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/3009982/page:10/
25. Режим failover на Cisco ASA [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://deltaconfig.ru/failover-on-cisco-asa/
26. Распространенная настройка cisco ASA для предприятия [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: http://www.go-to-easyit.com/2013/07/cisco-asa-3.html
27. Настройка доступа в Интернет на маршрутизаторе Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://netclo.ru/nastroyka-dostupa-v-internet-na-marshr/#more-1671
28. Мілінський М. ACL: списки контроля доступа в Cisco IOS [Електронний ресурс] / Микола Мілінський. – 2011. – Режим доступу до ресурсу: https://habr.com/en/post/121806/?mobile=no.
29. Port forwarding: теория и настройка Cisco [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://wiki.merionet.ru/seti/14/port-forwarding-teoriya-i-nastrojka-cisco/
30. Configure IKEv1 IPsec Site-to-Site Tunnels with the ASDM or CLI on the ASA [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/119141-configure-asa-00.html#anc8
31. Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html#anc14

32. Cisco IPsec [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://arny.ru/education/ccna-security/cisco-ipsec/
33. Настройка Site-to-Site VPN в Cisco ASA и ISR с трансляцией адресов NAT/PAT [Електронний ресурс] – Режим доступу до ресурсу: https://netconfigure.net/index.php/ru/forum/12-konfiguratsiya-setevogo-oborudovaniya/152-nastrojka-site-to-site-vpn-v-cisco-asa-i-isr-s-translyatsiej-adresov-nat-pat
34. Налагодження та дослідження засобів віддаленого доступу та адміністрування [Електронний ресурс] – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/60583/mod_resource/content/1/KM_KIKB_LR-08-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf
35. Cisco ASA. Основы. Доступ в интернет. [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://deltaconfig.ru/cisco-asa-internet-access/
36. Основи роботи з керованими комутаторами Cisco та мережною операційною системою Cisco IOS [Електронний ресурс] – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/40477/mod_resource/content/1/KM_KIKB_LR-04-2018-2019_KI-2KB-1.pdf
37. Сафонов Л. Атаки на сетевое оборудование с Kali Linux [Електронний ресурс] / Лука Сафонов. – 2017. – Режим доступу до ресурсу: https://habr.com/ru/post/326968/.

ДОДАТКИ

Додаток А

Топологія мережі

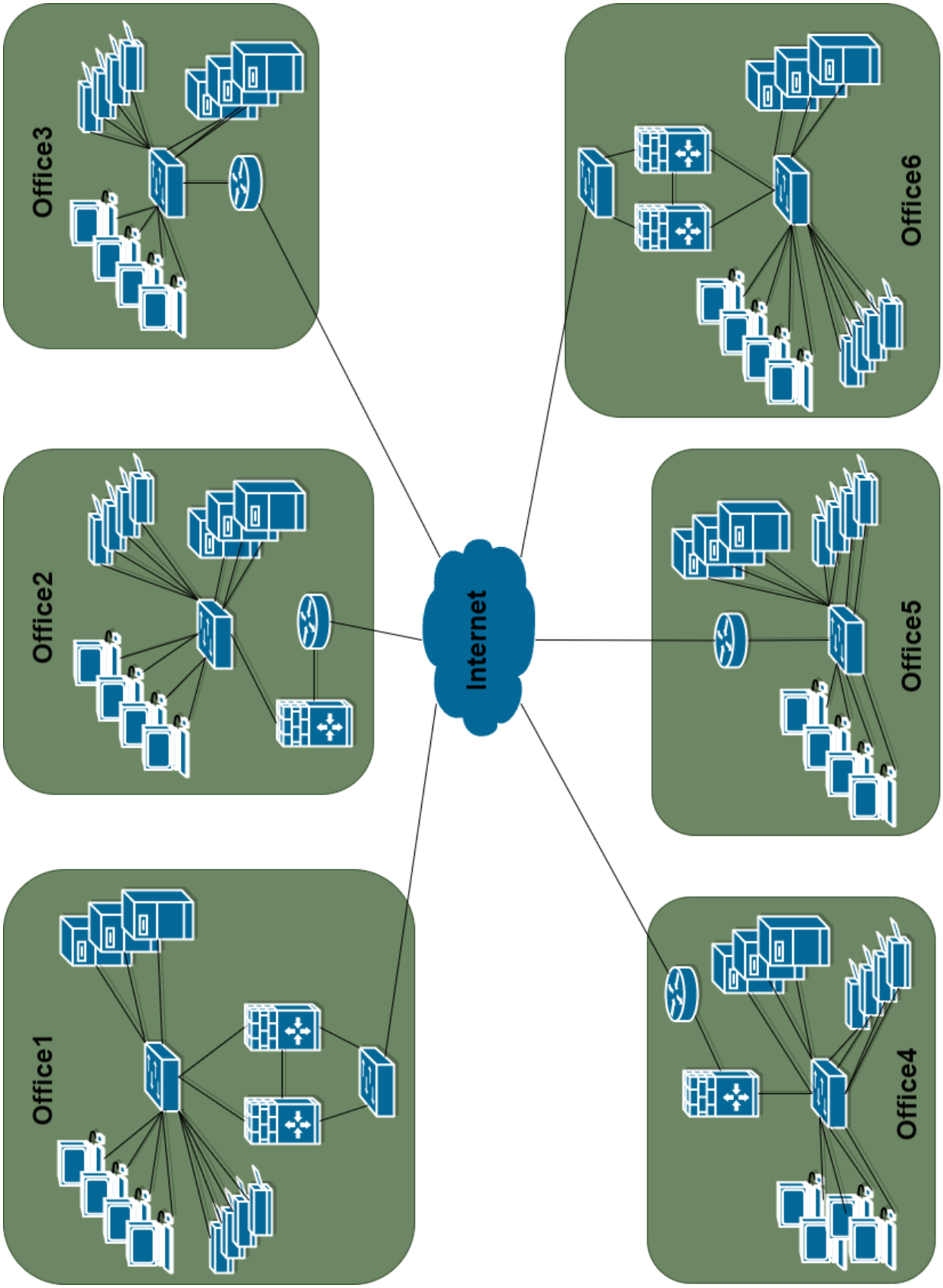


Рис. А.1. Повна топологія мережі

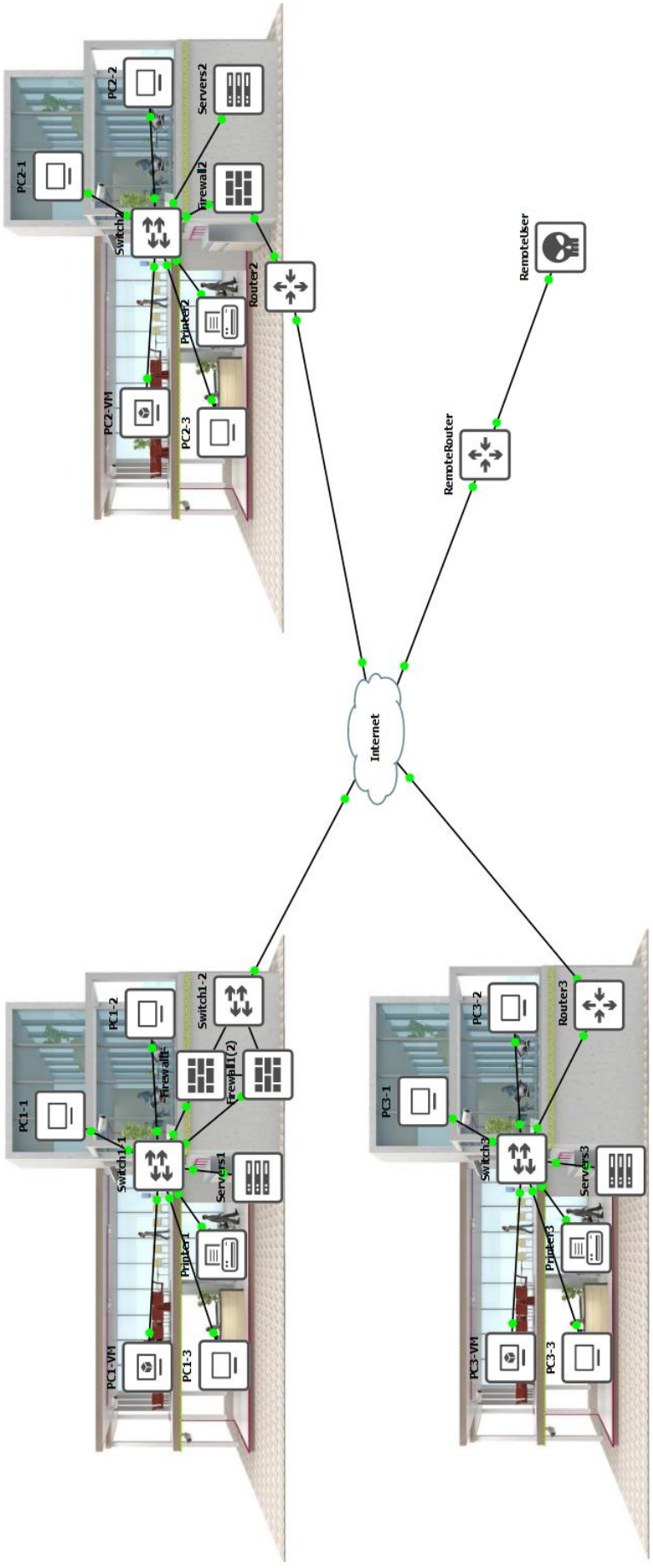


Рис. А.2. Спрощена топологія мережі

Додаток Б

Атака на мережу

```
root@kali:/usr/share/cisco-torch# cisco-torch -A 1.1.1.2
Using config file torch.conf...
Loading include and plugin ...

#################################################################
#   Cisco Torch Mass Scanner                    #
#   Becase we need it...                                        #
#   http://www.arhont.com/cisco-torch.pl                        #
#################################################################

List of targets contains 1 host(s)
2103:   Checking 1.1.1.2 ...
--->
- All scans done. Cisco Torch Mass Scanner  -
---> Exiting.
root@kali:/usr/share/cisco-torch# cisco-torch -A 2.2.2.2
Using config file torch.conf...
Loading include and plugin ...

#################################################################
#   Cisco Torch Mass Scanner                    #
#   Becase we need it...                                        #
#   http://www.arhont.com/cisco-torch.pl                        #
#################################################################

List of targets contains 1 host(s)
2104:   Checking 2.2.2.2 ...
--->
- All scans done. Cisco Torch Mass Scanner  -
---> Exiting.
root@kali:/usr/share/cisco-torch# cisco-torch -A 3.3.3.2
Using config file torch.conf...
Loading include and plugin ...

#################################################################
#   Cisco Torch Mass Scanner                    #
#   Becase we need it...                                        #
#   http://www.arhont.com/cisco-torch.pl                        #
#################################################################

List of targets contains 1 host(s)
2106:   Checking 3.3.3.2 ...
--->
- All scans done. Cisco Torch Mass Scanner  -
---> Exiting.
```

Рис. Б.1. Результат атаки cisco-torch на граничне маршрутизуюче обладнання

Додаток В

Лістинги конфігураційних файлів граничного маршрутизуючого обладнання

```
Firewall1# sh run
: Saved

:
: Serial Number: 9AV4PQ7S81E
: Hardware: ASAv, 2048 MB RAM, CPU
Pentium II 2600 MHz
:
ASA Version 9.5(2)204
!
hostname Firewall1
domain-name office1.com
enable password 2KFQnbNIdI.2KYOU
encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq
domain
xlate per-session deny udp any4 any6 eq
domain
xlate per-session deny udp any6 any4 eq
domain
xlate per-session deny udp any6 any6 eq
domain
names
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 no ip address
!
interface GigabitEthernet0/0.1
 vlan 1
 nameif management
 security-level 100
 ip address 193.2.3.125 255.255.255.248
!
interface GigabitEthernet0/0.10
 vlan 10
 nameif inside1
 security-level 100
 ip address 193.2.3.1 255.255.255.240
!
interface GigabitEthernet0/0.20
 vlan 20
 nameif inside2
 security-level 100
 ip address 193.2.3.17 255.255.255.240
!
interface GigabitEthernet0/0.30
 vlan 30
 nameif inside3
 security-level 100
 ip address 193.2.3.33 255.255.255.240
!
interface GigabitEthernet0/0.40
 vlan 40
 nameif inside4
 security-level 100
 ip address 193.2.3.49 255.255.255.240
!
interface GigabitEthernet0/0.50
 vlan 50
 nameif printers
 security-level 100
 ip address 193.2.3.65 255.255.255.240
!
interface GigabitEthernet0/0.60
 vlan 60
 nameif dmz
 security-level 50
 ip address 193.2.3.129 255.255.255.252
!
interface GigabitEthernet0/1
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/2
 nameif outside
 security-level 0
 ip address 1.1.1.2 255.255.255.252
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
banner motd Firewall 1 / Location Office1
ftp mode passive
dns server-group DefaultDNS
 domain-name office1.com
same-security-traffic permit inter-interface
object network inside1
 subnet 193.2.3.0 255.255.255.240
object network inside2
 subnet 193.2.3.16 255.255.255.240
object network inside3
 subnet 193.2.3.32 255.255.255.240
object network inside4
 subnet 193.2.3.48 255.255.255.240
object network OFFICE3
 subnet 195.2.3.0 255.255.255.192
object network dmz
 host 193.2.3.130
object network printers
 subnet 193.2.3.64 255.255.255.240
object-group network INSIDE
 network-object object inside1
 network-object object inside2
 network-object object inside3
 network-object object inside4
object-group network OFFICE2
 network-object 194.2.3.0 255.255.255.240
 network-object 194.2.3.16 255.255.255.240
 network-object 194.2.3.32 255.255.255.240
 network-object 194.2.3.48 255.255.255.240
object-group network REMOTE
 network-object object OFFICE3
 group-object OFFICE2
access-list VPN13 extended permit ip object-
group INSIDE object OFFICE3
access-list VPN12 extended permit ip object-
group INSIDE object-group OFFICE2
access-list OUTFILTER extended permit tcp
any object dmz eq www
access-list OUTFILTER extended permit tcp
host 1.1.1.1 host 1.1.1.2 eq bgp
access-list OUTFILTER extended permit udp
host 2.2.2.2 any eq isakmp
access-list OUTFILTER extended permit udp
host 2.2.2.2 any eq 4500
access-list OUTFILTER extended permit udp
host 3.3.3.2 any eq isakmp
access-list OUTFILTER extended permit udp
host 3.3.3.2 any eq 4500
access-list OUTFILTER extended permit esp
host 2.2.2.2 any
access-list OUTFILTER extended permit esp
host 3.3.3.2 any
access-list OUTFILTER extended permit
icmp host 2.2.2.2 any echo
access-list OUTFILTER extended permit
icmp host 3.3.3.2 any echo
access-list DMZ extended permit tcp any
object dmz eq www
access-list PRINTERS extended permit tcp
object-group INSIDE object printers eq lpd
access-list PRINTERS extended permit udp
object printers host 193.2.3.65 eq bootpc
access-list PRINTERS extended permit udp
object printers host 193.2.3.65 eq bootps
pager lines 23
mtu inside 1500
mtu management 1500
mtu inside1 1500
mtu inside2 1500
mtu inside3 1500
mtu inside4 1500
mtu printers 1500
mtu dmz 1500
mtu outside 1500
failover
failover lan unit primary
failover lan interface STATE
GigabitEthernet0/1
failover polltime unit 1 holdtime 3
failover link STATE GigabitEthernet0/1
failover interface ip STATE 1.1.2.1
255.255.255.252 standby 1.1.2.2
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
```

```
nat (inside3,outside) source static inside3
inside3 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside4,outside) source static inside4
inside4 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside1,outside) source static inside1
inside1 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside2,outside) source static inside2
inside2 destination static REMOTE
REMOTE no-proxy-arp route-lookup
!
object network inside1
 nat (inside1,outside) dynamic interface
object network inside2
 nat (inside2,outside) dynamic interface
object network inside3
 nat (inside3,outside) dynamic interface
object network inside4
 nat (inside4,outside) dynamic interface
object network dmz
 nat (dmz,outside) static interface service tcp
www www
access-group PRINTERS in interface printers
access-group PRINTERS out interface
printers
access-group DMZ out interface dmz
access-group OUTFILTER in interface
outside
router bgp 1100
 bgp log-neighbor-changes
 address-family ipv4 unicast
 neighbor 1.1.1.1 remote-as 5500
 neighbor 1.1.1.1 activate
 no auto-summary
 no synchronization
 exit-address-family
!
route outside 0.0.0.0 0.0.0.0 1.1.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-
invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
sysopt connection preserve-vpn-flows
crypto ipsec ikev1 transform-set Offices esp-
aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging
infinite
crypto map OfficesMAP 1 match address
VPN13
crypto map OfficesMAP 1 set pfs group5
crypto map OfficesMAP 1 set peer 3.3.3.2
crypto map OfficesMAP 1 set ikev1
transform-set Offices
crypto map OfficesMAP 2 match address
VPN12
crypto map OfficesMAP 2 set pfs group5
crypto map OfficesMAP 2 set peer 2.2.2.2
crypto map OfficesMAP 2 set ikev1
transform-set Offices
crypto map OfficesMAP interface outside
crypto ca trustpoint
_SmartCallHome_ServerCA
 no validation-usage
 crl configure
crypto ca trustpool policy
 auto-import
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 3600
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh 193.2.3.120 255.255.255.248
management
ssh timeout 60
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 8.8.8.8
dhcpd domain office1.com
```

```
!
dhcpd address 193.2.3.2-193.2.3.14 inside1
dhcpd enable inside1
!
dhcpd address 193.2.3.18-193.2.3.30 inside2
dhcpd enable inside2
!
dhcpd address 193.2.3.34-193.2.3.46 inside3
dhcpd enable inside3
!
dhcpd address 193.2.3.50-193.2.3.62 inside4
dhcpd enable inside4
!
dhcpd address 193.2.3.66-193.2.3.78 printers
dhcpd enable printers
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record
DfltAccessPolicy
username technic password ylR5K9lj7fidxeg.
encrypted privilege 5
username admin password
xEzlvgn4VssBkCva encrypted privilege 15
tunnel-group 3.3.3.2 type ipsec-l2l
tunnel-group 3.3.3.2 ipsec-attributes
 ikev1 pre-shared-key *****
tunnel-group 2.2.2.2 type ipsec-l2l
tunnel-group 2.2.2.2 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns
migrated_dns_map_1
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns migrated_dns_map_1
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect ip-options
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
 inspect icmp
 inspect http
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
 no active
 destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
 destination address email
callhome@cisco.com
 destination transport-method http
 subscribe-to-alert-group diagnostic
 subscribe-to-alert-group environment
 subscribe-to-alert-group inventory periodic
monthly
 subscribe-to-alert-group configuration
periodic monthly
 subscribe-to-alert-group telemetry periodic
daily
 profile License
 destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
 destination transport-method http
Cryptochecksum:393cf0369c58007a3e0513b
a72b946b4
: end
```

```
Router2#sh run
Building configuration...

Current configuration : 2978 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$REsu$YMe.csaHmGlHaulH335ob.
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name office2.com
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$vZ2P$zTPP978PSp4YgUs0h/XaG0
username technic privilege 5 secret 5
$1$FEE5$bIVLkYZ8.JYk/dee9.LfK/
archive
 log config
 hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 2.2.2.2 255.255.255.252
 ip access-group INFILTER in
 ip access-group OUTFILTER out
 ip nat outside
 ip virtual-reassembly
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 194.168.1.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
!
router bgp 2200
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.1 remote-as 5500
 no auto-summary
!
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 2.2.2.1
no ip http server
no ip http secure-server
!
!
ip nat inside source static esp 194.168.1.1
interface GigabitEthernet0/0
ip nat inside source list NAT interface
GigabitEthernet0/0 overload
ip nat inside source static tcp 194.168.1.1 80
2.2.2.2 80 extendable
ip nat inside source static udp 194.168.1.1
500 2.2.2.2 500 route-map MAP_ASA
extendable
ip nat inside source static udp 194.168.1.1
4500 2.2.2.2 4500 route-map MAP_ASA
extendable
!
ip access-list extended INFILTER
 evaluate IPTRAFFIC
 permit tcp any host 2.2.2.2 eq www
 permit tcp host 2.2.2.1 host 2.2.2.2 eq bgp
 permit udp host 1.1.1.2 any eq isakmp
non500-isakmp
 permit udp host 3.3.3.2 any eq isakmp
non500-isakmp
 permit esp host 1.1.1.2 any
 permit esp host 3.3.3.2 any
 permit icmp host 1.1.1.2 any echo
 permit icmp host 3.3.3.2 any echo
ip access-list extended NAT
 permit ip host 194.168.1.1 any
ip access-list extended OUTFILTER
 permit ip any any reflect IPTRAFFIC
timeout 300
!
access-list 1 permit 2.2.2.1
no cdp log mismatch duplex
!
!
!
!
route-map MAP_ASA permit 1
 match ip next-hop 1
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^CCRouter 3 / Location
Office3^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password toor
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 logout-warning 30
 absolute-timeout 10
 logging synchronous
 login local
 transport input ssh
 transport output ssh
!
end
```

```
Firewall2# sh run
: Saved

:
: Serial Number: 9AC5GNAUSL1
: Hardware: ASAv, 2048 MB RAM, CPU
Pentium II 2600 MHz
:
ASA Version 9.5(2)204
!
hostname Firewall2
domain-name office2.com
enable password 2KFQnbNIdI.2KYOU
encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq
domain
xlate per-session deny udp any4 any6 eq
domain
xlate per-session deny udp any6 any4 eq
domain
xlate per-session deny udp any6 any6 eq
domain
names
!
interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/0.1
 vlan 1
 nameif management
 security-level 100
 ip address 194.2.3.125 255.255.255.248
!
interface GigabitEthernet0/0.10
 vlan 10
 nameif inside1
 security-level 100
 ip address 194.2.3.1 255.255.255.240
!
interface GigabitEthernet0/0.20
 vlan 20
 nameif inside2
 security-level 100
 ip address 194.2.3.17 255.255.255.240
!
interface GigabitEthernet0/0.30
 vlan 30
 nameif inside3
 security-level 100
 ip address 194.2.3.33 255.255.255.240
!
interface GigabitEthernet0/0.40
 vlan 40
 nameif inside4
 security-level 100
 ip address 194.2.3.49 255.255.255.240
!
interface GigabitEthernet0/0.50
 vlan 50
 nameif printers
 security-level 100
 ip address 194.2.3.65 255.255.255.240
!
interface GigabitEthernet0/0.60
 vlan 60
 nameif dmz
 security-level 50
 ip address 194.2.3.129 255.255.255.252
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 194.168.1.1 255.255.255.252
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
banner motd Firewall 2 / Location Office2
ftp mode passive
dns server-group DefaultDNS
 domain-name office2.com
same-security-traffic permit inter-interface
object network inside1
 subnet 194.2.3.0 255.255.255.240
object network inside2
 subnet 194.2.3.16 255.255.255.240
object network inside3
 subnet 194.2.3.32 255.255.255.240
object network inside4
 subnet 194.2.3.48 255.255.255.240
object network Office3
 subnet 195.2.3.0 255.255.255.192
object network dmz
 host 194.2.3.130
object network printers
 subnet 194.2.3.64 255.255.255.240
object-group network INSIDE
 network-object object inside1
 network-object object inside2
 network-object object inside3
 network-object object inside4
object-group network Office1
 network-object 193.2.3.0 255.255.255.240
 network-object 193.2.3.16 255.255.255.240
 network-object 193.2.3.32 255.255.255.240
 network-object 193.2.3.48 255.255.255.240
object-group network REMOTE
 network-object object Office3
 group-object Office1
access-list VPN23 extended permit ip object-
group INSIDE object Office3
access-list VPN12 extended permit ip object-
group INSIDE object-group Office1
access-list WWW extended permit tcp any
object dmz eq www
access-list DMZ extended permit tcp any
object dmz eq www
access-list PRINTERS extended permit tcp
object-group INSIDE object printers eq lpd
access-list PRINTERS extended permit udp
object printers host 194.2.3.65 eq bootpc
access-list PRINTERS extended permit udp
object printers host 194.2.3.65 eq bootps
pager lines 23
mtu management 1500
mtu inside1 1500
mtu inside2 1500
mtu inside3 1500
mtu inside4 1500
mtu printers 1500
mtu dmz 1500
mtu outside 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside1,outside) source static inside1
inside1 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside2,outside) source static inside2
inside2 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside3,outside) source static inside3
inside3 destination static REMOTE
REMOTE no-proxy-arp route-lookup
nat (inside4,outside) source static inside4
inside4 destination static REMOTE
REMOTE no-proxy-arp route-lookup
!
object network inside1
 nat (inside1,outside) dynamic interface
object network inside2
 nat (inside2,outside) dynamic interface
object network inside3
 nat (inside3,outside) dynamic interface
object network inside4
 nat (inside4,outside) dynamic interface
object network dmz
 nat (dmz,outside) static interface service tcp
www www
access-group PRINTERS in interface printers
access-group PRINTERS out interface
printers
access-group DMZ out interface dmz
access-group WWW in interface outside
route outside 0.0.0.0 0.0.0.0 194.168.1.2 1
timeout xlate 3:00:00
```

```
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-
invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
no snmp-server location
no snmp-server contact
sysopt connection preserve-vpn-flows
crypto ipsec ikev1 transform-set Offices esp-
aes-256 esp-sha-hmac
crypto ipsec security-association pmtu-aging
infinite
crypto map OfficesMAP 1 match address
VPN12
crypto map OfficesMAP 1 set pfs group5
crypto map OfficesMAP 1 set peer 1.1.1.2
crypto map OfficesMAP 1 set ikev1
transform-set Offices
crypto map OfficesMAP 2 match address
VPN23
crypto map OfficesMAP 2 set pfs group5
crypto map OfficesMAP 2 set peer 3.3.3.2
crypto map OfficesMAP 2 set ikev1
transform-set Offices
crypto map OfficesMAP interface outside
crypto ca trustpoint
_SmartCallHome_ServerCA
 no validation-usage
 crl configure
crypto ca trustpool policy
 auto-import
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 3600
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh 194.2.3.120 255.255.255.248
management
ssh timeout 60
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 8.8.8.8
dhcpd domain office2.com
!
dhcpd address 194.2.3.2-194.2.3.14 inside1
dhcpd enable inside1
!
dhcpd address 194.2.3.18-194.2.3.30 inside2
dhcpd enable inside2
!
dhcpd address 194.2.3.34-194.2.3.46 inside3
dhcpd enable inside3
!
dhcpd address 194.2.3.50-194.2.3.62 inside4
dhcpd enable inside4
!
dhcpd address 194.2.3.66-194.2.3.78 printers
dhcpd enable printers
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy VPN internal
group-policy VPN attributes
 vpn-tunnel-protocol ikev1
 pfs enable
dynamic-access-policy-record
DfltAccessPolicy
username technic password ylR5K9lj7fidxeg.
encrypted privilege 5
username admin password
xEzlvgn4VssBkCva encrypted privilege 15
tunnel-group 3.3.3.2 type ipsec-l2l
tunnel-group 3.3.3.2 general-attributes
 default-group-policy VPN
tunnel-group 3.3.3.2 ipsec-attributes
 ikev1 pre-shared-key *****
tunnel-group 1.1.1.2 type ipsec-l2l
tunnel-group 1.1.1.2 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
!                                                    : end
policy-map type inspect dns
migrated_dns_map_1
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns migrated_dns_map_1
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect ip-options
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
 inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
 no active
 destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
 destination address email
callhome@cisco.com
 destination transport-method http
 subscribe-to-alert-group diagnostic
 subscribe-to-alert-group environment
 subscribe-to-alert-group inventory periodic
monthly
 subscribe-to-alert-group configuration
periodic monthly
 subscribe-to-alert-group telemetry periodic
daily
 profile License
 destination address http
https://tools.cisco.com/its/service/oddce/servi
ces/DDCEService
 destination transport-method http
Cryptochecksum:45e6a3055e3c32fd43d00c0
473a4244b
```

```
Router3#sh run
Building configuration...

Current configuration : 5921 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$10Sb$QHZIKslCGOeBPr99vfo2Z0
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 195.2.3.1
ip dhcp excluded-address 195.2.3.17
ip dhcp excluded-address 195.2.3.33
ip dhcp excluded-address 195.2.3.49
ip dhcp excluded-address 195.2.3.65
!
ip dhcp pool LAN-VM
 network 195.2.3.0 255.255.255.240
 default-router 195.2.3.1
 domain-name office3.com
 dns-server 8.8.8.8
!
ip dhcp pool LAN1
 network 195.2.3.16 255.255.255.240
 default-router 195.2.3.17
 domain-name office3.com
 dns-server 8.8.8.8
!
ip dhcp pool LAN2
 network 195.2.3.32 255.255.255.240
 default-router 195.2.3.33
 domain-name office3.com
 dns-server 8.8.8.8
!
ip dhcp pool LAN3
 network 195.2.3.48 255.255.255.240
 default-router 195.2.3.49
 domain-name office3.com
 dns-server 8.8.8.8
!
ip dhcp pool PRINTERS
 network 195.2.3.64 255.255.255.240
 default-router 195.2.3.65
 domain-name office3.com
 dns-server 8.8.8.8
!
!
no ip domain lookup
ip domain name office3.com
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
object-group network INSIDE
 195.2.3.0 255.255.255.192
!
object-group network printers
 195.2.3.64 255.255.255.240
!
username admin privilege 15 secret 5
$1$zemb$.Y3GuMGFIeO93Rjh5vzIU/
username technic privilege 5 secret 5
$1$jWH4$UFLW.Icz6R/KgRX7u9B7s0
archive
 log config
 hidekeys
!
!
crypto isakmp policy 1
```

```
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key Office1ToOffice3 address
1.1.1.2
crypto isakmp key Office2ToOffice3 address
2.2.2.2
!
!
crypto ipsec transform-set Offices esp-aes 256
esp-sha-hmac
!
crypto map OfficesMAP 1 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set Offices
 set pfs group5
 match address VPN13
crypto map OfficesMAP 2 ipsec-isakmp
 set peer 2.2.2.2
 set transform-set Offices
 set pfs group5
 match address VPN23
!
!
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 no ip address
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 195.2.3.125 255.255.255.248
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 195.2.3.1 255.255.255.240
 ip nat inside
 ip virtual-reassembly
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 195.2.3.17 255.255.255.240
 ip nat inside
 ip virtual-reassembly
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 195.2.3.33 255.255.255.240
 ip nat inside
 ip virtual-reassembly
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 195.2.3.49 255.255.255.240
 ip nat inside
 ip virtual-reassembly
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 195.2.3.65 255.255.255.240
 ip access-group PRINTERS out
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 195.2.3.129 255.255.255.252
 ip access-group DMZ out
 ip nat inside
 ip virtual-reassembly
!
interface GigabitEthernet1/0
 ip address 3.3.3.2 255.255.255.252
 ip access-group INFILTER in
 ip access-group OUTFILTER out
 ip nat outside
 ip virtual-reassembly
 negotiation auto
 crypto map OfficesMAP
!
router bgp 3300
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.1 remote-as 5500
 no auto-summary
!
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 3.3.3.1
no ip http server
no ip http secure-server
!
!
ip nat inside source route-map nonat interface
GigabitEthernet1/0 overload
ip nat inside source static tcp 195.2.3.130 80
3.3.3.2 80 extendable
!
ip access-list extended DMZ
 permit tcp any host 195.2.3.130 eq www
ip access-list extended INFILTER
 evaluate IPTRAFFIC
 permit tcp any host 3.3.3.2 eq www
 permit tcp host 3.3.3.1 host 3.3.3.2 eq bgp
 permit udp host 1.1.1.2 any eq isakmp
non500-isakmp
 permit udp host 2.2.2.2 any eq isakmp
non500-isakmp
 permit esp host 1.1.1.2 any
 permit esp host 2.2.2.2 any
 permit icmp host 1.1.1.2 any echo
 permit icmp host 2.2.2.2 any echo
ip access-list extended NAT
 deny ip 195.2.3.0 0.0.0.63 193.2.3.0 0.0.0.63
 deny ip 195.2.3.0 0.0.0.63 194.2.3.0 0.0.0.63
 permit ip 195.2.3.0 0.0.0.63 any
ip access-list extended OUTFILTER
 permit ip any any reflect IPTRAFFIC
timeout 300
ip access-list extended PRINTERS
 permit tcp object-group INSIDE object-group
printers eq lpd
 permit udp object-group printers host
195.2.3.65 eq bootpc
 permit udp object-group printers host
195.2.3.65 eq bootps
ip access-list extended VPN13
 permit ip 195.2.3.0 0.0.0.63 193.2.3.0
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 193.2.3.16
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 193.2.3.32
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 193.2.3.48
0.0.0.15
ip access-list extended VPN23
 permit ip 195.2.3.0 0.0.0.63 194.2.3.0
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 194.2.3.16
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 194.2.3.32
0.0.0.15
 permit ip 195.2.3.0 0.0.0.63 194.2.3.48
0.0.0.15
!
no cdp log mismatch duplex
!
!
!
!
route-map nonat permit 1
 match ip address NAT
!
!
!
control-plane
!
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^CRouter 3 / Location
Office3^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password toor
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 logout-warning 30
 absolute-timeout 10
 logging synchronous
 login local
 transport input ssh
 transport output ssh
!
end
```