

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 корпоративної
мережі на базі рішень Cisco ASA»

Виконав студент 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 А.С. Чевкота

Керівник к.т.н., доцент, доцент кафедри КІ та КБ

 Ю.М. Россінський

Рецензент к.т.н., доцент, доцент кафедри КІ та КБ

 І.В. Пулеко

Житомир – 2021

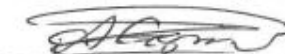
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

СПЕЦІАЛЬНІСТЬ 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри комп'ютерної
інженерії та кібербезпеки



Єфіменко А.А.

« 12 » квітня 20 21 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Чевкоти Андрія Сергійовича

Тема роботи: Проект підсистеми захисту корпоративної мережі на базі рішень Cisco ASA

Затверджена Наказом університету від «12» квітня 2021 р. № 133\С

Термін здачі студентом закінченої роботи 16.06.2021 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження) процес проектування,
розробки та налагодження підсистеми захисту корпоративної мережі; міжмережні екрани
Cisco ASA як основа підсистеми захисту корпоративної мережі;

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	12.04.21	15.06.21
2	Єфіменко А.А.	12.04.21	15.06.21
3	Єфіменко А.А.	12.04.21	15.06.21

Керівник  Роєїнський Ю.М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.21	<i>Виконано</i>
2	Розробка плану роботи	15.04.21 – 17.04.21	<i>Виконано</i>
3	Розробка розгорнутого плану	18.04.21 – 19.04.21	<i>Виконано</i>
4	Подача чернетки керівнику для перевірки	25.04.21	<i>Виконано</i>
5	Доопрацювання роботи та перевірка керівником	26.04.21 – 30.05.21	<i>Виконано</i>
6	Затвердження графічних матеріалів у керівника	01.06.21 – 04.06.21	<i>Виконано</i>
7	Проведення попереднього захисту	05.06.21	<i>Виконано</i>
8	Отримання відгуку керівника	16.06.21	<i>Виконано</i>
9	Допуск завідувача кафедри	16.06.21	<i>Виконано</i>
10	Подання роботи на рецензування	16.06.21	<i>Виконано</i>
11	Захист	18.06.21	

Студент  Чевкота А.С

Керівник  Россінський Ю.М.

АНОТАЦІЯ

Випускна кваліфікаційна робота представляє з себе проект підсистеми захисту корпоративної комп'ютерної мережі. Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 86 сторінок, 37 рисунків та 6 таблиць. Список використаних джерел містить 22 найменування і займає 3 сторінки.

Метою випускної кваліфікаційної роботи є розробка підсистеми захисту корпоративної мережі на базі рішень Cisco ASA та забезпечення функціонування даної мережі.

В роботі визначено основні завдання для побудови корпоративної мережі та підсистеми захисту до неї, проаналізовано базові підходи до побудови корпоративної мережі з використанням продукції компанії Cisco та міжмережних екранів Cisco ASA. Наведено розробку, налагодження функціонування підсистеми захисту корпоративної мережі за допомогою міжмережних екранів Cisco ASA та тестування її працездатності й виконання поставлених задач.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, МІЖМЕРЕЖНІ ЕКРАНИ, FIREWALL, CISCO, CISCO ASA, ПІДСИСТЕМА ЗАХИСТУ, ЗАХИСТ.

					KI.KP.B – 123 – 21 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту корпоративної мережі на базі рішень Cisco ASA Пояснювальна записка	Літ.	Арк.	Аркушів
Розроб.		Чевкота А.С.		16.06.21				
Керівник		Роханський Ю.М.		16.06.21			4	86
Реценз		Пулєко І.В.		16.06.21		Житомирська політехніка, група KI-3		
Н. контр.								
Зав. каф.		Єфіменко А.А.		16.06.21				

ANNOTATION

The bachelor's thesis is a project of corporate computer network security subsystem. The explanatory note to the final diploma qualification work contains 86 pages, 37 figures and 6 tables. The list of used sources contains 22 names and occupies 3 pages.

The purpose of the final thesis is to develop a subsystem for corporate network protection based on Cisco ASA solutions and ensure the functioning of this network.

The main tasks for the construction of the corporate network and the subsystem of protection to it are defined, the basic approaches to the construction of the corporate network using Cisco products and Cisco ASA firewalls are analyzed. Development, adjustment of functioning of a subsystem of protection of a corporate network by means of Cisco ASA firewalls and testing of its operability and performance of the set tasks are resulted.

Keywords: CORPORATE NETWORK, FIREWALL, CISCO, CISCO ASA, SECURITY SUBSYSTEM, PROTECTION.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	9
1.1 Базові підходи до побудови корпоративних комп'ютерних мереж	9
1.2 Технології та технічні рішення для побудови корпоративних комп'ютерних мереж від компанії Cisco	11
1.3 Побудова корпоративних комп'ютерних мереж на базі рішень Cisco ASA	12
1.4 Зони та рівні безпеки, додаткові функції Cisco ASA	15
1.5 Постановка технічного завдання	23
РОЗДІЛ 2. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	25
2.1 Розробка загального проекту корпоративної комп'ютерної мережі	25
2.2 Розробка проекту фізичної та логічної топологій мережі	26
2.3 Розробка політик підсистеми захисту міжзональної взаємодії корпоративної комп'ютерної мережі	31
2.4 Структура Windows мережі.....	33
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОЕКТУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	34
3.1 Вибір обладнання та програмного забезпечення.....	34
3.2 Налагодження корпоративної комп'ютерної мережі	35
3.3 Тестування функціоналу корпоративної мережі	46
ВИСНОВКИ.....	61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	64
ДОДАТКИ.....	67

ВСТУП

Все більше і більше корпоративних організацій зустрічаються з новими викликами ІТ-безпеки через нові методи атак на їх мережі, які можуть коштувати організаціям надзвичайно дорого. Майже кожен місяць з'являється новина про те, як величезні компанії стають жертвами мережових атак і втрачають величезні обсяги інтелектуальної власності й конфіденційних даних, які можуть бути дуже цінними не тільки в плані матеріального.

Компанія Cisco щодня працює над поліпшенням безпеки мережі не тільки за допомогою введення нових технологій та протоколів, а й за допомогою спеціалізованих пристроїв, які мають змогу відслідковувати та аналізувати трафік, який через них проходить. Одним з таких пристроїв є міжмережний екран Cisco ASA. Даний пристрій чудово виконує роль захисника мережі, аналізуючи весь трафік, який через нього проходить та поділяє мережу на зони безпеки задля кращого розуміння, що в мережі найважливіше, а що ні.

Актуальність теми обумовлена впровадженням нових технологій та технологічних рішень для захисту мереж будь-яких розмірів як відповідь на різні мережні атаки, ціль яких може бути не тільки викрадення інформації, а й руйнування всієї мережі. Одним з ефективних технологічних рішень для надійного захисту мережі є саме міжмережний екран Cisco ASA

Метою кваліфікаційної роботи є розробка проекту підсистеми захисту корпоративної мережі на базі рішень Cisco ASA.

Досягнення даної мети включає в себе рішення наступних завдань:

- проведення аналізу базових підходів для побудови корпоративних комп'ютерних мереж;
- проведення аналізу та вивчення технологій та технологічних рішень для побудови корпоративних мереж від компанії Cisco;
- аналіз побудови корпоративної мережі на базі рішень Cisco ASA, аналіз переваг використання міжмережних екранів Cisco ASA;

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

- вивчення основних та додаткових функцій захисту на міжмережних екранах Cisco ASA;
- розробка загального проекту корпоративної мережі;
- розробка проекту фізичної та логічної топологій;
- розробка політик підсистеми захисту міжзональної взаємодії корпоративної мережі;
- вибір моделей міжмережних екранів Cisco ASA та комутаторів для побудови корпоративної мережі;
- налагодження мережевого обладнання та тестування працездатності корпоративної мережі й коректного виконання поставлених задач на кваліфікаційну роботу.

Об'єктом дослідження є міжмережні екрани Cisco ASA, які є основою підсистеми захисту корпоративної мережі.

Предметом дослідження є процес проектування, розробки та налагодження підсистеми захисту корпоративної мережі.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Базові підходи до побудови корпоративних комп'ютерних мереж

Корпоративна мережа - це структурна мережа будь-якої організації, основною метою якої є забезпечення ефективної внутрішньої та зовнішньої роботи цієї організації. Насправді це взаємопов'язаний набір локальних мереж, які взаємодіють через глобальну мережу. Користувачі цієї мережі є виключно працівниками цієї організації. Часто корпоративна мережа включає також офіси, філії, підрозділи та інші організаційні структури в різних містах та країнах.

Локальні корпоративні мережі кожного відділу пов'язані між собою транспортною мережею. Завдяки широкомасштабній організації, коли філії та офіси компанії розташовані в різних містах та країнах, вже існуючі глобальні мережі передачі даних, а саме Інтернет, можуть використовуватися як транспортні мережі. Основний обмін даними здійснюється в локальних мережах, а транспортна мережа призначена для координації проектів, результатів роботи, отриманих у різних офісах організації. Цьому сприяє ієрархічна структура мережі, тим самим зменшуючи трафік у каналах передачі даних. [9]

Основне завдання для організації корпоративної мережі – канали зв'язку. Існує кілька варіантів організації каналів зв'язку між відділами, офісами або філіями:

- приватний власний канал зв'язку;
- зв'язок через VPN.

У першому способі канали зв'язку будуються між офісами за допомогою мідних та оптоволоконних кабелів, каналів радіозв'язку тощо. Основні переваги даного способу полягають у контролі і безпеці корпоративної мережі та гнучкості. Але є й недоліки: саме розгортання каналу зв'язку,

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

обслуговування і даний спосіб побудови каналу зв'язку краще робити, коли існує невелика відстань між офісами.

У другому способі побудови каналу зв'язку, а саме зв'язку через VPN, використовується глобальна мережа Інтернет. Існують два методи організації об'єднання корпоративної комп'ютерної мережі через VPN:

- за допомогою послуг інтернет-провайдера, який використовується корпоративною мережею;
- за допомогою використання власних ресурсів (обладнання).

У першому випадку, якщо один інтернет-провайдер використовується всією корпоративною мережею і він надає послугу VPN, то можна розраховувати на оренду виділених ліній для даного зв'язку. Основні переваги даного методу полягає у простоті використання, так як обслуговування і все налаштування виконує провайдер, та в універсальному розмірі каналу. Але поверх цих переваг є й недоліки, такі як безконтрольність (організація не може контролювати трафік, який проходить вже на стороні провайдера) та висока вартість, так як відділи (офіси) корпоративної мережі можуть бути дуже далеко один від одного і це напряму впливає на ціну оренди каналів зв'язку.

У другому випадку, якщо є можливість, організація може використовувати власне обладнання для побудови зв'язку через VPN. Основні переваги цього способу в низькій вартості, бо гроші організації витрачаються лише на оплату Інтернету та в можливості продумати зв'язок з ростом масштабів діяльності. Попри дані переваги навіть в даному способі є один недолік, який може бути критичним (залежить від роду діяльності організації), а саме швидкість передачі даних, вона може бути різною. [9]

Виділимо основні елементи локальної мережі (одного офісу, філії тощо), яка входить в корпоративну комп'ютерну мережу:

- робочі станції;
- мережеве обладнання;
- головні сервери, такі як головний та додатковий контролери домену, тощо;
- допоміжні сервери (WEB-сервер, FTP-сервер, тощо). [6]

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

1.2 Технології та технічні рішення для побудови корпоративних комп'ютерних мереж від компанії Cisco

Компанія Cisco - світовий лідер у галузі мережевих технологій і інтернет, що змінюють способи людського спілкування, зв'язку, співпраці. IP-рішення Cisco можна з повним правом назвати фундаментальною основою цих мереж. Для побудови корпоративної комп'ютерної мережі можна в повному обсязі використовувати мережеве обладнання від компанії Cisco, адже в них найбільший вибір різних пристроїв мережі, за допомогою яких можливо побудувати будь-яку корпоративну мережу будь-яких масштабів для різного роду діяльності.

Корпоративну мережу можна побудувати використовуючи сучасні маршрутизатори, які використовують найновіші технології в оптимізації та захисту даних, наприклад маршрутизатори Cisco, які діляться на групи по способу використання, наприклад:

- для філіалів (Catalyst 8300, Catalyst 8200, Catalyst 8200 Edge uCPE, ISR1000);
- для агрегації глобальних мереж (NCS 500, NCS 5000, NCS 5500, NCS 5700, Catalyst 8500, ASR 900, ASR 1000);
- для операторів зв'язку (8000, NCS 500, NCS 5500, NCS 5700, ASR 9000, ASR 900);
- для промисловості (IR1101 ISR Rugged, 800 Industrial ISR, CGR1000, WPAN IR 500). [7]

Використовуючи дані маршрутизатори можна не перейматися за масштабованість мережі, так як вони забезпечують це в повній мірі.

Для кращого, більш суворого захисту корпоративної мережі при побудові можна використати міжмережні екрани Cisco ASA, які є спеціалізованими пристроями мережі для захисту даних мережі. Наразі є різні сучасні моделі міжмережних екранів Cisco ASA, які відрізняються пропускнуою можливістю та швидкістю й підтримкою масштабованості корпоративної комп'ютерної мережі.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

1.3 Побудова корпоративних комп'ютерних мереж на базі рішень Cisco ASA

Cisco ASA (Adaptive Security Appliances, пристрої адаптивної безпеки) – пристрої компанії Cisco з лінійки мережевої безпеки.

Керування Cisco ASA можливе з використанням командного рядка (CLI) та за допомогою графічних засобів. Інтерфейс командного рядка Cisco ASA подібний до Cisco IOS, але є свої відмінності. Графічні засоби керування пристроєм Cisco ASA орієнтовані на використання WEB-технологій. Це програмні додатки ASDM (Adaptive Security Device Manager) та CSM (Cisco Security Manager). [8]

Основні функції міжмережних екранів Cisco ASA:

- SPI (Statefull Packet Inspection), DPI (Deep Packet Inspection) – глибокий аналіз пакетів зі збереженням стану;
- IDFW (Identity Firewall) – надання доступу до мережі на основі даних LDAP (Active Directory);
- TrustSec (Trusted Security) – більш гнучкий варіант IDFW, працює в поєднанні з Cisco ISE (Identity Service Engine);
- IDS (Intrusion Detection System) – система виявлення вторгнень;
- Cisco ASA CX – система безпеки з врахуванням контексту, яка контролює використання додатків для користувачів і груп та виконує WEB-фільтрацію з перевіркою репутації.

Міжмережними екранами Cisco ASA підтримуються такі основні функції маршрутизаторів, як:

- статична і динамічна маршрутизації (OSPF, EIGRP, RIP);
- технологія трансляції адрес (NAT);
- фільтрація трафіку за допомогою списків контролю доступу (ACL);
- віртуальні приватні мережі (VPN типу Site-to-Site, Remote Access VPN).

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Та додаткові функції такі як забезпечення роботи сервера DHCP та забезпечення віддаленого доступу (Telnet, SSH, HTTP).

Міжмережний екран Cisco ASA може функціонувати в режимах:

- маршрутизований режим (Router Firewall Mode);
- прозорий режим (Transparent Firewall Mode);
- змішаний режим (Mixed Firewall Mode).

У маршрутизованому режимі міжмережного екрану Cisco ASA передбачається налаштування пристрою як маршрутизатора, включаючи налаштування належності інтерфейсів до різних IP-мереж та маршрутизації, цей режим використовується за замовчуванням.

У прозорому режимі виконується налагодження Cisco ASA як прозорого моста. У цьому режимі інтерфейси пристрою належать до однієї IP-мережі.

У змішаному режимі використовуються два попередні режими для різних інтерфейсів. Цей режим використовується в останніх версіях Cisco ASA.

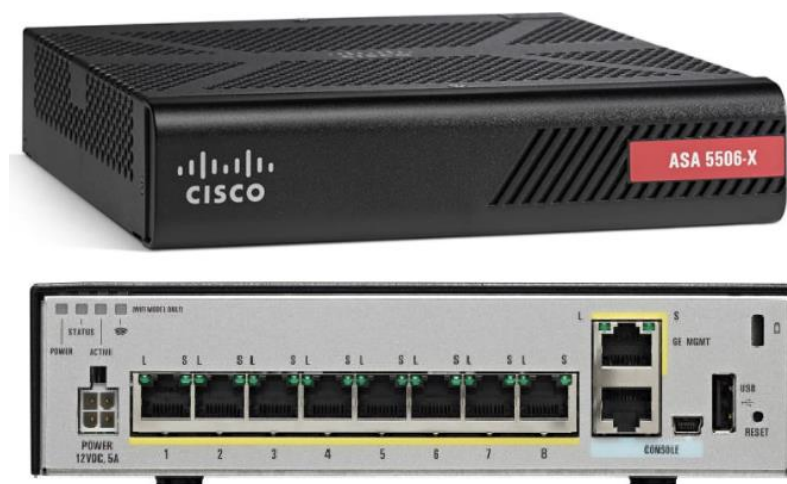


Рисунок 1.1 – Зовнішній вигляд міжмережного екрану Cisco ASA 5506-X

Особливістю Cisco ASA є наявність заводської конфігурації пристрою, яка може відрізнятись в залежності від версії Cisco ASA, однак у всіх випадках заводська конфігурація пристрою містить такі параметри:

- назва пристрою за замовчуванням: ciscoasa;
- пароль для консольного підключення та пароль на вхід у привілейований режим не встановлено;

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

– timeout для підключень telnet та ssh встановлено 5 хвилин. [8]

Фірмою Cisco розроблені моделі різної продуктивності, які орієнтовані на обслуговування як невеликих мереж (домашніх мереж чи мереж філіалів організацій) так і високошвидкісних мереж великого розміру (мереж провайдерів, кампусів, датацентрів тощо). Виділяють стару і нову серії Cisco ASA. Стара серія включає в себе пристрої Cisco ASA 5505, 5510, 5520, 5540, 5550, 5585. Нова серія включає в себе пристрої Cisco ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X і т.д.

Також розроблені спеціальні мережні модулі на основі Cisco ASA, які можуть використовуватися в високопродуктивних маршрутизаторах чи комутаторах для виконання міжмережного екранування.

Слід відмітити, що існує система ліцензування Cisco ASA Software в межах якої один і той же пристрій може надавати як базовий, так і розширений набір можливостей. Ці набори позначаються відповідно як Base License та Security Plus License.

Більш ефективні та нові моделі відносяться до лінійки ASA 5500-X з сервісами FirePOWER, які забезпечують пропускну здатність від 256 до 1750 Мбіт/сек, контроль загроз від 125 до 1250 Мбіт/сек, контроль стану сеансів, моніторинг і контроль роботи додатків, NGIPS, захист від тяжкого шкідливого ПЗ, фільтрація URL-адрес. Це все забезпечує чудовий захист та надійність мережі.

Для корпоративної комп'ютерної мережі рекомендується використовувати саме нові моделі ASA 5500-X, так як там реалізовано нові технології захисту мережі від можливих вторгнень, шкідливого ПЗ, тощо. Використовуючи старі моделі міжмережних екранів, організація ризикує втратити великі об'єми цінної інформації та контроль над мережею.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

1.4 Зони та рівні безпеки, додаткові функції Cisco ASA

Міжмережний екран Cisco ASA призначає рівні безпеки, щоб розрізняти внутрішні і зовнішні мережі. Рівні безпеки визначають рівні довіри інтерфейсів. Чим вище рівень безпеки, тим надійніше інтерфейс. Діапазон рівнів безпеки - від 0 (недовірених) до 100 (найдовіреніший). Кожному робочому інтерфейсу необхідно присвоїти назву і значення рівня безпеки в межах від 0 (нижчий) до 100 (вищий). [17]

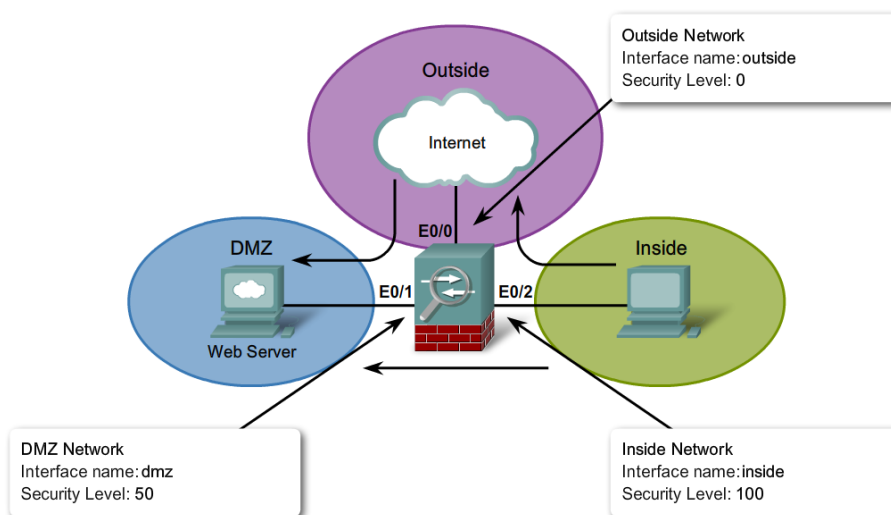


Рисунок 1.2 – Рівні безпеки на інтерфейсах міжмережного екрану Cisco ASA

Як показано на рис. 1.2, рівень 100 необхідно призначати найзахищенішій підмережі, наприклад внутрішній. Рівень 0, як правило, призначають зовнішній мережі, типово мережі, яка підключена до Інтернет. Зоні DMZ і іншим мережам можна призначати проміжні значення рівня безпеки в діапазоні від 0 до 100. Коли трафік поширюється від інтерфейсу з великим рівнем безпеки до інтерфейсу з меншим рівнем безпеки, він вважається вихідним. Трафік, який поширюється від інтерфейсу з меншим рівнем безпеки до інтерфейсу з великим рівнем безпеки, вважається вхідним. [18]

Рівні безпеки дозволяють контролювати багато різних аспектів мережевого трафіку. За замовчуванням передача вихідного трафіку дозволяється, і він при цьому піддається інспектуванню. Зворотний трафік

дозволяється після інспектування пакетів зі збереженням станів. Наприклад, користувачі з внутрішньої мережі, підключеної до внутрішнього інтерфейсу, можуть безперешкодно отримувати доступ до ресурсів в зоні DMZ. Також вони можуть ініціювати підключення до Інтернету без обмежень і без необхідності застосовувати додаткову політику безпеки або виконувати додаткові команди. Однак трафік, що надходить в зону DMZ або у внутрішню мережу з зовнішньої мережі, за замовчуванням відхиляється. Зворотний трафік, сформований спочатку у внутрішній мережі і повертається через зовнішній інтерфейс, дозволяється. Для будь-яких винятків із такого режиму роботи за замовчуванням необхідно конфігурувати список ACL, щоб явно дозволити поширення трафіку від інтерфейсу з більш низьким рівнем безпеки до інтерфейсу з більш високим рівнем безпеки, наприклад із зовнішньої мережі до внутрішньої.

DMZ – це демілітаризована область корпоративної мережі, що містить загальнодоступні вузли, які надаються відповідні послуги, наприклад:

- веб-сервіси;
- публічні сервери;
- поштові сервери,
- файлові сервери;
- сервери баз даних тощо.

Під загальнодоступними розуміннями таких сервісів, яким необхідний доступ, доступний не лише з локальної мережі, але й із зовнішньої мережі Інтернет. Логічно розміщувати такі сервіси в окремому сегменті, так як ризик взлому дуже великий. [10]

При цьому інші комп'ютери, що знаходяться в іншому сегменті, залишаються більш захищеними. Таким чином, мінімізується шкода від можливого зламу сервера.

Сервери, що знаходяться в DMZ, мають, як правило, публічні білі IP-адреси. Для повноцінної реалізації DMZ мережевий пристрій має мати

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

можливість запам'ятовування сесій. За допомогою інспектування трафіку можна заборонити серверам DMZ ініціювати з'єднання з локальною мережею. Тим самим ми захищаємо користувачів від зловмисників, які, можливо, зламали один із публічних серверів.

При цьому для самих користувачів локальних мереж сервери DMZ будуть доступні. DMZ можна організувати на міжмережному екрані Cisco ASA за допомогою команд `security-level`, `nameif` та трансляції адрес (NAT) з використанням списків ACL.

Взагалі технологія NAT використовується не лише для формування повноцінної зони DMZ. Дана технологія є невід'ємною частиною в налаштуванні інших зон безпеки за міжмережним екраном Cisco ASA, для яких потрібно забезпечити доступ до Інтернету.

NAT зазвичай використовується для перетворення IP-адрес з приватної мережі в публічні IP-адреси.

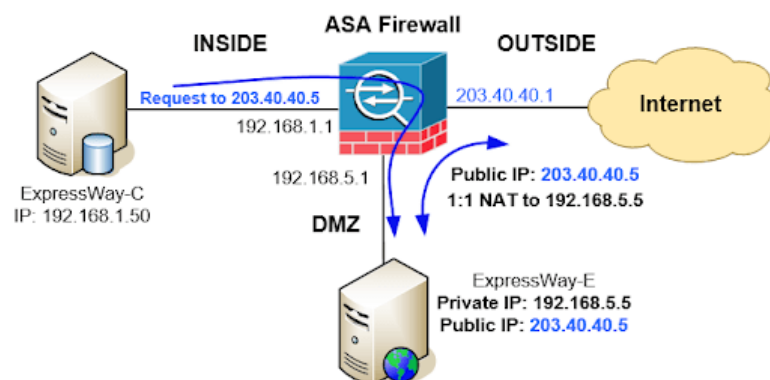


Рисунок 1.3 – Перетворення IP-адреси з зони DMZ в публічну IP-адресу
Зокрема, ASA підтримує такі найбільш поширені типи NAT [11]:

- динамічне перетворення NAT;
- динамічне перетворення PAT;
- статичне перетворення NAT;
- NAT на основі політики.

Динамічне перетворення NAT – це перетворення за схемою «багато з багатьма». Зазвичай для внутрішнього пулу приватних адрес потрібні публічні адреси з іншого пулу.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Динамічне перетворення PAT – це перетворення за схемою «багато до одного». Цей варіант називається також перевантаженням NAT. Зазвичай внутрішній пул приватних адрес працює через один зовнішній інтерфейс або зовнішню адресу.

Статичне перетворення NAT – це перетворення за схемою «один до одного». Зазвичай зовнішній адресі зіставляється внутрішній сервер.

NAT на основі політики –тип NAT, що ґрунтується на наборі правил. Ці правила визначають те, що перетворення виконується тільки для конкретних адрес джерела, зіставлених з конкретними адресами призначення і / або конкретними портами.

Чотири перерахованих вище типи NAT позначаються як NAT мережних об'єктів, так як для їх налаштування потрібно налаштувати мережні об'єкти.

Іншим варіантом NAT на ASA є «подвійний NAT». При подвійному NAT адреси джерела і призначення визначаються в одному правилі (команда nat). Подвійний NAT використовується при конфігуруванні мереж віддаленого доступу VPN з технологіями IPsec і SSL. [5]

Також для захисту локальних мереж за міжмережним екраном Cisco ASA за замовчуванням використовується глибока перевірка пакетів (DPI).

Глибока перевірка пакетів – це форма фільтрації пакетів, яка зазвичай здійснюється як функція міжмережного екрану Cisco ASA. Вона застосовується на рівні додатків Open Systems Interconnection. Глибока перевірка пакетів оцінює частину даних та заголовків пакета, який передається через точку перевірки, відсіваючи будь-які невідповідності протоколу, спаму, вірусам, вторгненням та будь-яким іншим визначеним критеріям, щоб заблокувати проходження пакету через точку перевірки. [12]

Глибока перевірка пакетів також використовується, щоб вирішити, чи перенаправляється певний пакет в інший пункт призначення, тобто може знаходити, виявляти, категоризувати, блокувати або перенаправляти пакети,

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

які мають певний код або корисні навантаження даних, які не виявляються, не розташовуються, не класифікуються, не блокуються та не перенаправляються за допомогою звичайної фільтрації пакетів. На відміну від звичайної фільтрації пакетів, глибока перевірка пакетів виходить за межі вивчення заголовків пакетів. [2]

Також дана перевірка оцінює вміст пакета, який проходить через контрольну точку. Використовуючи правила, призначені на пристрої ASA, визначає, що робити з цими пакетами в режимі реального часу. Вона може перевірити вміст цих пакетів, а потім з'ясувати, звідки він надійшов, наприклад служба або програма, яка його надіслала. Крім того, він може працювати з фільтрами, щоб знаходити та перенаправляти мережевий трафік з Інтернет-сервісу, такого як Twitter або Facebook, або з певної IP-адреси.

Якщо у організації є користувачі, які використовують свої ноутбуки для роботи, то DPI життєво необхідна для запобігання потраплянню червів, шпигунського програмного забезпечення та вірусів у вашу корпоративну мережу. Крім того, використання глибокої перевірки пакетів базується на правилах і політиках, визначених на пристрої Cisco ASA, що дозволяє мережі виявляти, чи є заборонене використання схвалених програм.

Cisco ASA підтримує побудову віртуальних приватних мереж через загальну мережну інфраструктуру.

VPN - це приватна мережа, яка створена через мережу загального користування, зазвичай через Інтернет. Замість застосування виділених фізичних підключень, в VPN використовуються віртуальні підключення, маршрутизовані через Інтернет з організації на віддалений майданчик.

VPN є середовищем зв'язку, в якій забезпечується суворий контроль доступу для організації рівноправних підключень в рамках певної спільноти. Конфіденційність забезпечується шляхом шифрування трафіку всередині VPN. Сьогодні під віртуальними приватними мережами розуміється захищена реалізація мережі VPN з функцією шифрування. [21]

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

У мережі VPN між двома пунктами хости відправляють і отримують звичайний трафік TCP / IP через VPN-шлюз, який може являти собою маршрутизатор, міжмережвий екран, концентратор Cisco VPN або пристрій Cisco ASA. VPN-шлюз відповідає за інкапсуляцію і шифрування вихідного трафіку з конкретного майданчика і відправку його через VPN-тунель через Інтернет на інший такий же VPN-шлюз на іншому майданчику. При прийомі трафіку інший VPN-шлюз видаляє заголовки, дешифрує контент і пересилає пакет в цільовий хост всередині своєї приватної мережі.

Топології мереж VPN між двома пунктами продовжують розвиватися. Як приклади більш складних топологій мереж VPN можна назвати VPN на основі багатопроTOCOLьної комутації по мітках (Multiprotocol Label Switching (MPLS)), динамічну багатоточкову VPN (Dynamic Multipoint VPN (DMVPN)) і транспортну VPN з груповим шифруванням (Group Encrypted Transport (GETVPN)).

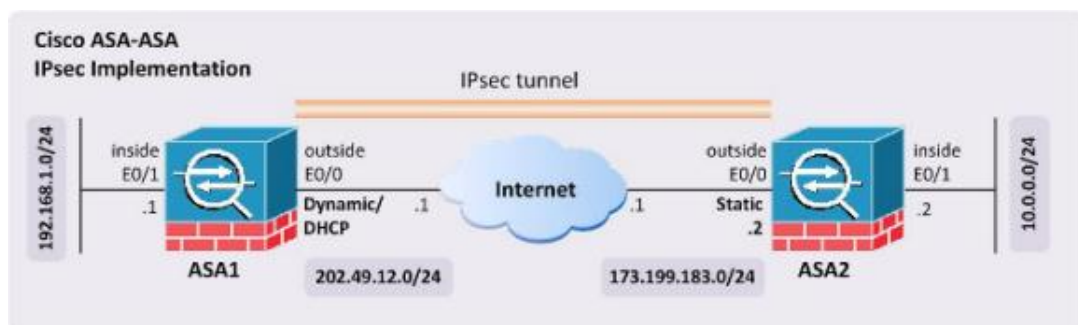


Рисунок 1.4 – Site-to-Site IPsec VPN між двома міжмережними екранами Cisco ASA

Site-to-site VPN – мережа, що має в наявності два пристрої (наприклад, пристрої Cisco ASA), між якими є тунель. [13] Користувачам, які знаходяться в локальних мережах, не потрібно установки будь-якого спеціального програмного забезпечення, так як VPN типу “Site-To-Site” розпізнає трафік з якої підмережі надходить і яка підмережа є отримувачем цього трафіку. VPN типу “Site-To-Site” можуть з’єднувати дві і більше мережі, які фізично знаходяться у різних місцях. VPN типу “Site-To-Site” використовують

загальнодоступний Інтернет для розширення корпоративної комп'ютерної мережі організації на кілька офісних місць і так як трафік, який проходить через VPN є зашифрованим, то організація може не перейматись за те, що інформація проходить через глобальну мережу.

Для того, щоб забезпечити зв'язок між підмережами філій через глобальну мережу, потрібно налаштувати маршрутизацію. На міжмережних екранах Cisco ASA може бути налаштована статична маршрутизація та динамічна за допомогою протоколу OSPF. Для легкого налаштування та забезпечення ефективної масштабованості корпоративної мережі краще налаштовувати динамічну маршрутизацію OSPF, яка є найбільш поширеною в глобальній мережі.

Протокол OSPF (Open Shortest Path First) – це внутрішній шлюзовий протокол, який використовується для поширення даних маршрутизації всередині однієї автономної системи. [20]

Даний протокол ґрунтується на стані каналу. Опис інтерфейсу має включати його IP-адресу, маску, тип мережі, до якої він підключений, сусідні маршрутизатори, підключені до мережі і так далі. Колекція всіх станів каналів являє собою базу даних станів каналів.

Протокол OSPF використовує алгоритм стану каналу для формування і підрахунку найкоротшого шляху до всіх відомих підмереж. Після ініціалізації і в результаті зміни маршрутних даних маршрутизатор генерує оголошення про стан каналу. Всі маршрутизатори обмінюються даними про стан каналу за допомогою “лавинної” розсилки. Після заповнення бази даних кожного маршрутизатора, протокол OSPF вираховує дерево найкоротших шляхів до всіх відомих підмереж.

Головні переваги використання протоколу OSPF:

- в OSPF число переходів немає ліміту;

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- OSPF використовує мультиадресну розсилку IP для відправки оновлень стану каналу;
- OSPF пропонує більш досконалу конвергенцію, RIP. Це пов'язано з тим, що зміни маршрутизації поширюються миттєво, а не періодично.;
- OSPF пропонує більш ефективне вирівнювання навантаження;
- OSPF пропонує логічне визначення мереж, що дозволяє поділ маршрутизаторів на області. Це дозволяє обмежити поширення оновлень по мережі. Крім того, ця можливість надає механізм агрегування маршрутів і скорочення непотрібного поширення даних підмережі;
- OSPF підтримує аутентифікацію маршрутизації з використанням різних методів аутентифікації на основі пароля;
- протокол OSPF забезпечує передачу і маркування зовнішніх маршрутів, введені в автономну систему.

ASA може одночасно запускати два процеси протоколу OSPF на різних наборах інтерфейсів. Можливо запустити два процеси, якщо є інтерфейси, що використовують однакові IP-адреси (NAT дозволяє цим інтерфейсам співіснувати, але OSPF не допускає перекриття адрес). Допускається запустити один процес всередині, а інший зовні - і перерозподілити підмножину маршрутів між двома процесами. [19]

Пристрої Cisco ASA підтримують наступні функції OSPF:

- внутрішні, міжобласні та зовнішні маршрути;
- віртуальні зв'язки;
- LSA flooding;
- аутентифікація для пакетів OSPF (як автентифікація пароля, так і MD5);
- налаштування ASA як призначеного маршрутизатора або призначеного резервного маршрутизатора.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

1.5 Постановка технічного завдання

Метою кваліфікаційної роботи є проектування та побудова підсистеми захисту корпоративної комп'ютерної мережі на базі рішень Cisco ASA, що включають наступні завдання:

- розробка загального проекту корпоративної комп'ютерної мережі для розуміння поставленої задачі та подальшого її вирішення;
- розробка проекту фізичної та логічної топологій мережі;
- аналіз та розробка політик підсистеми захисту міжзональної взаємодії корпоративної комп'ютерної мережі для ефективного захисту та правил проходження міжзонального трафіку;
- аналіз та розробка структури Windows-мережі
- аналіз та порівняння доступних моделей мережевого обладнання та обґрунтування вибору конкретних моделей для використання в корпоративній комп'ютерній мережі;
- налагодження мережевого обладнання;
- тестування працездатності налагодженої корпоративної мережі.

При розробці загального проекту мережі необхідно спроектувати загальну структуру корпоративної мережі, поділ на центральну мережу та мережі філій. Також необхідно розробити загальну схему взаємодії центральної мережі з мережами філій всіх пристроїв мережі у двох офісах корпоративної мережі (центральна мережа та мережа філії).

При розробці фізичної та логічної топології мережі потрібно врахувати особливості розташування пристроїв корпоративної комп'ютерної мережі та розробити схему їх підключень та IP-адресації. Потрібно розробити логіку взаємодії пристроїв мережі між мережами філії та центральною мережею.

При аналізі та розробці політик міжзональної взаємодії потрібно врахувати особливості розташування серверів та робочих станції в різних зонах, та, спираючись на ці особливості, розробити план взаємодії однієї зони

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

з іншою, правила проходження трафіку, який блокувати трафік, а який пропускати, тощо.

При аналізі та розробці структури Windows-мережі, потрібно врахувати особливості роботи серверів, які забезпечують працездатність домену. Проаналізувати поділ даних серверів на головний контролер та додаткові контролери домену. Розробити схему розташування та взаємодії між собою контролерів домену для успішної їх реплікації та балансування навантаження.

Після всіх аналізів та розробок загальних структур, схем та функцій корпоративної комп'ютерної мережі потрібно налагодити мережеве обладнання для досягнення мети, яка була поставлена на даній кваліфікаційній роботі.

Після налагодження мережевого обладнання провести тестування на працездатність корпоративної комп'ютерної мережі та правильність виконання всіх поставлених задач.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Розробка загального проекту корпоративної комп'ютерної мережі

При розробці загальної структури корпоративної мережі стоїть завдання розробити мережу, що у своєму складі містить: центральну мережу (головний офіс), мережу філії, віддалених користувачів, публічні та локальні сервери.

Потрібно також зауважити, що центральна мережа та мережі філій повинні мати доступ до Інтернету для забезпечення зв'язку між ними та забезпечувати підключення користувачів корпоративної мережі до Інтернету, забезпечувати зв'язок корпоративних WWW-, FTP-, WIN- та DNS-серверів.

Зв'язок між центральною мережею та мережами філій має бути зашифрованим та захищеним задля запобігання, при ймовірному перехопленні, розкриттю інформації організації корпоративної мережі, тому буде використано технологію VPN.

Публічні сервери мають бути лише в головному офісі, який виступає центральною мережею, а локальні сервери можуть бути використані як і в головному офісі, так і в мережах філій організації.

При проектуванні мережі буде використана трирівнева ієрархічна модель мережі, в якій використовуються три рівні:

- рівень ядра (Core layer);
- рівень розподілу (Distribution layer);
- рівень доступу (Access layer).

Частина загальної топології корпоративної мережі, де зображено центральну мережу та мережу філії, наведено на рис. А.1 додатку А.

Рівень ядра складається з міжмережних екранів Cisco ASA та з маршрутизаторів, які являють собою мережу Інтернет.

Рівні розподілу та доступу складаються з центральної мережі та мереж філій організації корпоративної мережі.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

2.2 Розробка проекту фізичної та логічної топологій мережі

Розглянемо детальніше структуру спроектованої частини топології загальної корпоративної мережі, яка показана в додатку А.

Структурою мережі головного офісу (OFFICE01) та мережі філії (OFFICE02) є ієрархічна зірка і зв'язок між робочими станціями та серверами здійснюється за допомогою центральних міжмережних екранів Cisco ASA двох офісів.

Головний офіс (центральна мережа) OFFICE01 складається з трьох різних приміщень, які з'єднані з міжмережним екраном Cisco ASA Office01_ASA, який виступає ядром для цього офісу, за допомогою комутаторів витою парою GigabitEthernet, яка забезпечує високошвидкісний якісний зв'язок в офісі при навантаженні на комутатори багатьма робочими станціями.

Перше приміщення є адміністративним, в ньому знаходяться локальні сервери Primary_Domain_Controller (Головний контролер домену), FTP_Server та три робочі станції. Всі вище перелічені пристрої, окрім сервера FTP_Server з'єднані з комутатором Office01_SW_1 витою парою FastEthernet для забезпечення високої швидкості передачі інформації. Сервер FTP_Server з'єднаний з комутатором витою парою GigabitEthernet.

Друге приміщення виступає робочим для персоналу офісу. Приміщення складається лише з робочих станцій, які з'єднані з комутатором Office01_SW_2 витою парою FastEthernet.

Останнє третє приміщення є серверним та вміщує в себе сервери: Secondary_DNS_Server (Вторинний DNS-сервер) та WEB_Server. Дані сервери з'єднані з комутатором Office01_SW_3 витою парою GigabitEthernet для забезпечення найкращої швидкості передачі даних.

З'єднання інтерфейсів пристроїв мережі головного офісу OFFICE01 наведено в табл. Б.1 додатку Б.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Мережі філій організації мають подібну або схожу структуру, для прикладу розглянемо мережу філії OFFICE02

Мережа філії OFFICE02 складається лише з одного приміщення, яке з'єднане з міжмережним екраном Cisco ASA Office02_ASA, який виступає ядром для цієї мережі. Підключення до міжмережного екрану Cisco ASA Office02_ASA здійснюється за допомогою комутатора Office02_SW_1 витою парою GigabitEthernet.

У самому приміщенні розміщені робочі станції персоналу та сервер Backup_Domain_Controller (Резервний/додатковий контролер домену), які з'єднані з комутатором витою парою FastEthernet.

З'єднання інтерфейсів пристроїв мережі офісу OFFICE02 наведено в табл. 2.1.

Таблиця 2.1

Підключення пристроїв мережі OFFICE02

Пристрій	Інтерфейс	Підключення до пристрою/Мережі	Підключення до інтерфейсу
Міжмережний екран Office02_ASA	Gig0/1	Internet	Gig
	Gig0/0	Комутатор Office02_SW_1	Gig0/1
Комутатор Office02_SW_1	Gig0/1	Міжмережний екран Office02_ASA	Gig0/0
	Gig0/1	Сервер Backup_Domain_Controller	Fa0
	Gig0/2	Робоча станція Office02_PC1	Fa0
	... Gig0/5	... Робоча станція Office02_PC5	... Fa0

З'єднання пристроїв мережі філії OFFICE02, яке показано в табл. 2.1, застосовується і до всіх інших мереж філій, так як вони дуже схожі між собою або подібні.

З'єднання центральної мережі з мережами філій відбувається через глобальну мережу Інтернет, тобто використовуються послуги провайдера, який забезпечує всю корпоративну мережу зв'язком. Саме з'єднання центральної мережі та мереж філій з пристроями провайдера забезпечується через міжмережні екрани Cisco ASA витою парою GigabitEthernet для забезпечення якісного, надійного та швидкого зв'язку.

Потрібно визначити адресний простір для пристроїв корпоративної мережі. Для адресації використаємо протокол IPv4. Для всієї мережі будемо використовувати префікс /24, маска якого 255.255.255.0.

Так як міжмережні екрани Cisco ASA двох мереж корпоративної мережі являються центральними пристроями для забезпечення зв'язку між двома офісами та до Інтернету, то вони будуть працювати в змішаному режимі, який поєднує в собі маршрутизований та прозорий. На міжмережних екранах буде працювати технологія NAT, тому щодо економії адрес питання випадає.

Центральна мережа або головний офіс OFFICE01 складається з трьох приміщень. Кожне приміщення являє собою унікальну для загальної корпоративної мережі підмережу. Суть роботи міжмережного екрану Cisco ASA в тому, що пристрій ділить мережу на зони, які необхідні для розуміння пристроєм політики базового захисту, тому для головного офісу OFFICE01 будуть три внутрішні зони: inside01, inside02 та DMZ. Зона, яка сполучає мережу головного офісу з Інтернетом, буде outside.

Для серверів Secondary_DNS_Server та WEB_Server буде використана статична IP-адресація як і для підмережі зони DMZ, так і для доступу з Інтернету через технологію NAT.

В табл. Б.2 додатку Б наведено схему адресації пристроїв мережі головного офісу OFFICE01 (центральна мережа).

Так як мережі філій корпоративної мережі складаються з одного приміщення, то вони лише й будуть у вигляді зони inside для міжмережних екранів Cisco ASA.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

В табл. 2.2 наведено схему адресації пристроїв мережі офісу OFFICE02 (мережа філії).

Таблиця 2.2

Схема адресації пристроїв мережі OFFICE02

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Міжмережний екран Office02_ASA	Gig0/1	100.6.1.1	255.255.255.224	/27
	Gig0/0	192.168.3.0	255.255.255.0	/24
Сервер Backup_Domain_Controller	Fa0	192.168.3.254	255.255.255.0	/24
Робоча станція Office02_PC1	DHCP			
... Робоча станція Office02_PC4				

Функціонування корпоративної комп'ютерної мережі забезпечується не лише самим фізичним з'єднанням та ІР-адресацією пристроїв мережі, а й логікою взаємодії центральної мережі з мережами філій для забезпечення їх зв'язку між собою. У даній кваліфікаційній роботі логічна топологія проєктованої мережі формується за рахунок з'єднань, що базуються на технологіях VPN. Технології VPN дають забезпечують захист при передачі даних центральною мережею та мережами філій за рахунок шифрування, автентифікації, контролю цілісності та інших механізмів безпеки.

З'єднання мереж за допомогою VPN діляться на такі типи [22]:

- Full Mesh VPN (з'єднання всіх зі всіма);
- Partial Mesh VPN (з'єднання багато-до-багатьох);
- Hub & Spoke VPN (з'єднання одного зі всіма);

Тип з'єднання мереж Full Mesh VPN забезпечує найнадійніший зв'язок, адже всі мережі організації з'єднані повністю між собою (всі мережі зі всіма). Це дозволяє підтримувати зв'язок зі всіма працюючими мережами, якщо одна або навіть кілька мереж якось втратять зв'язок VPN, наприклад, через поломку

мережевого обладнання. Але є один суттєвий недолік, який полягає в масштабованості корпоративної мережі, яка використовує даний тип з'єднання мереж філій, тощо. Додання нової філії мережі вимагає налаштування мережевих обладнань до всіх інших мереж, тобто при великій кількості зв'язаних між собою мереж організації, додання нової буде проблемою через важкість налаштування зв'язку.

Тип з'єднань мереж організації Partial Mesh VPN забезпечує менш надійний зв'язок. Всі мережі в даному випадку не з'єднані повністю між собою, а лише частково. Масштабованість корпоративної мережі з даним типом з'єднання легша ніж якщо використовувати Full Mesh VPN, так як одна мережа може з'єднуватись лише з мережами, які потрібні для ефективної роботи, а не зі всіма відразу.

Останній тип з'єднання Hub and Spoke VPN є найненадійнішим, так як всі мережі філій з'єднуються лише з центральним офісом. Але даний тип з'єднання мереж організації має велику перевагу в масштабованості корпоративної мережі, так як при даному типі це зробити найлегше. При доданні нової філії мережі потрібно налаштовувати зв'язок VPN лише з центральною мережею, але слід зауважити, що при цьому на центральній мережі буде найбільше навантаження, яке залежить від кількості мереж філій. Але якщо, наприклад, при поломці мережевого обладнання, яке забезпечує зв'язок VPN, то зв'язок з центральною мережею відновиться лише після відновлення обладнання.

Для спроектованої корпоративної мережі буде використаний тип з'єднання Partial Mesh VPN так як даний тип є “Золотою серединою” в надійності та масштабованості корпоративної комп'ютерної мережі.

У загальному зв'язок між мережами офісів буде забезпечуватися за допомогою IPSec VPN типу “Site-To-Site”, а саме між зонами inside01 центральної мережі OFFICE01 та inside мереж філій, наприклад, мережі філії OFFICE02. Далі зв'язок між мережами філій буде забезпечуватись між

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

найближчими іншими філіями для забезпечення надійності. Якщо буде поломка мережевого обладнання центральної мережі, то зв'язок між сусідніми мережами філії буде існувати.

Адресація логічних з'єднань мережі через VPN частини загальної топології (додаток А) показано в табл. 2.3:

Таблиця 2.3

Логічне з'єднання центральної мережі OFFICE01 з мережею філії OFFICE02

Мережа	IP-адреса мережі призначення VPN	Підключення до мережі	Підключення до IP-адреси мережі призначення VPN
Центральна мережа OFFICE01	100.1.1.1	Мережа філії OFFICE02	100.6.1.1
Мережа філії OFFICE02	100.6.1.1	Центральна мережа OFFICE01	100.1.1.1

2.3 Розробка політик підсистеми захисту міжзональної взаємодії корпоративної комп'ютерної мережі

Для забезпечення надійного захисту не лише від шкідливого трафіку глобальної мережі Інтернет, а й всередині організації, тобто в локальних мережах корпоративної мережі, потрібно розробити та застосувати політики безпеки на мережевому обладнанні організації, що дадуть змогу контролювати та фільтрувати весь трафік, який через них проходить.

Політика або політики безпеки – це правила проходження трафіку, які забороняють або дозволяють проходження певного трафіку для забезпечення більш надійного захисту ресурсів організації не тільки від глобальної мережі Інтернет, а й від локальних мереж, через які могла б бути можливість доступу до даних ресурсів.

Для міжмережних екранів Cisco ASA політики безпеки можуть визначатися через поділ локальної мережі на зони та рівні безпеки, тому для коректної роботи пристрою Cisco ASA потрібно поділити мережу на зони безпеки, опираючись на вимоги до побудови мережі для забезпечення захисту.

Міжзональний трафік повинен бути розроблений в головному офісі корпоративної мережі, так як там використовуються різні зони для забезпечення безпеки, а саме:

- зона inside01 з рівнем безпеки 100;
- зона inside02 з рівнем безпеки 100;
- зона dmz з рівнем безпеки 85;
- зона outside з рівнем безпеки 0.

Однаковий рівень безпеки зон inside01 та inside02 зумовлений особливістю роботи міжмережного екрану Cisco ASA, потрібно, щоб робочі станції зони inside02 мали доступ до серверів FTP_Server, Primary_Domain_Controller й водночас і до зони DMZ та до Інтернету. Адже коли за допомогою розширених списків доступу ACL дозволити проходження трафіку з зони з рівнем безпеки меншим ніж до зони з вищим рівнем, то буде автоматично блокуватися весь інший трафік, тому для коректної роботи потрібно забезпечити однаковий рівень безпеки та присвоювати розширені списки доступу ACL до інтерфейсу на вихідний трафік зони, до якої потрібен доступ.

Отже, всі робочі станції зони inside02 центральної мережі OFFICE01 повинні мати доступ лише до серверів зони inside01. Водночас всі робочі станції зони inside01 мають доступ до всіх зон центральної мережі повністю, так як зона inside01 являється адміністративною. Зона inside01 повинна мати доступ ще й до мережі філії, а саме до зони inside для забезпечення зв'язку між офісами та доменною мережею Windows для повного контролю мережі філії.

Для забезпечення повної працездатності центральної мережі, потрібен дозвіл на проходження трафіку з зони DMZ до зони inside01, а саме сервера Secondary_DNS_Server до сервера Primary_Domain_Controller відповідно, щоб всі записи DNS коректно оновлювалися та надавалися публічно.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

2.4 Структура Windows мережі

Поверх корпоративної мережі потрібно забезпечити функціонування Windows мережі для контролю робочих станцій та важливих серверів центральної мережі OFFICE01 та мереж філій.

Центральна мережа OFFICE01 має в зоні inside01 сервер Primary_Domain_Controller, який являється головним контролером домену та який буде регулювати роботу всіх робочих станцій та серверів всіх мереж філій та центральної мережі, підключених до домену officescorp.com. Для забезпечення контролю до мереж філій та додання робочих станцій даних мереж, будуть використовуватись додаткові або резервні контролери домену, які будуть розташовані в мережах філій, наприклад, сервер Backup_Domain_Controller мережі філії OFFICE02.

Для реплікації з'єднань між головним контролером домену центральної мережі та додатковими контролерами домену мереж філії буде використовуватись зв'язок VPN, так як даний зв'язок має бути захищеним та зашифрованим.

У центральній мережі OFFICE01 зони DMZ є публічний сервер Secondary_DNS_Server. Для забезпечення його інформацією про записи DNS, він має бути доданим в домен officescorp.com та налаштований на отримання копії зони DNS officescorp.com. Сам головний контролер домену також має бути налаштований на надання копії зони DNS лише довіреним хостам.

Дана структура домену буде мати чудовий баланс навантаження, так як робота не забезпечується лише самим головним контролером домену, що дає змогу не перенавантажувати центральну мережу роботою домену та розподіляти дану роботу між всіма контролерами. Структура даної Windows мережі має ще й високу надійність роботи, так як якщо, наприклад, з якихось причин головний контролер домену центральної мережі перестане працювати, то додаткові контролери домену продовжать свою роботу і далі будуть розподіляти навантаження між сусідніми філіями при працюючому з'єднанні VPN.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОЕКТУ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Вибір обладнання та програмного забезпечення

Для побудови корпоративної мережі організації можна використати дуже багатий інструментарій у вигляді пристроїв мережі компанії Cisco. Існують безліч різних комутаторів, маршрутизаторів, концентраторів, пристроїв безпеки, тощо, для вирішення потреб захисту, доступності, швидкості передачі даних корпоративної мережі.

Для реалізації проекту захищеної корпоративної комп'ютерної мережі організації було обрано міжмережні екрани Cisco ASA та комутатори тієї ж компанії.

Для реалізації підсистеми мережі потрібен сучасний міжмережний екран Cisco ASA з достатньою потужністю, якої б вистачало для мережі, та не було її надмірності. Існують багато моделей міжмережного екрану Cisco ASA, розглянемо та порівняємо кілька з них, а саме моделі: 5506-х, 5525-х та 5555-Х. Порівняння моделей Cisco ASA наведено в табл. В.1 додатка В.

З даних таблиці можна зробити висновок, що для розробки корпоративної комп'ютерної мережі з можливістю її подальшого масштабування модель Cisco ASA 5506-Х підходить менше всього через низьку пропускну здатність, невелику кількість VPN-тунелів між вузлами і інших характеристик, які недостатні для побудови повноцінної комп'ютерної мережі. Тому вибір моделі міжмережного екрану постає між Cisco ASA 5525-Х та Cisco ASA 5555-Х. Без сумніву, модель 5555-Х краща ніж 5525-Х, але є надмірність в деяких характеристиках і дана модель на ринку дуже дорога, тому в цілях використання ресурсів без надмірності в характеристиках і в цілях економії було обрано модель Cisco ASA 5525-Х.

Для розподілу трафіку між кінцевими вузлами потрібно обрати комутатори, які мають велику кількість портів для забезпечення якісного,

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

швидкого зв'язку в корпоративній мережі. Самі комутатори повинні бути сучасними з підтримкою останніх технологій для забезпечення додаткового захисту мережі.

Найдоступнішими комутаторами, які продає компанія Cisco та які підходять для побудови корпоративних мереж, є комутатори серії Cisco Catalyst 9300, які дозволяють розгортати доступ як для невеликих, так і для великих філій, офісів, тощо. На сьогоднішній день майже всі сучасні комутатори не використовують порти FastEthernet, всі націлені на користування в основному портів GigabitEthernet. Це стосується і комутаторів серії Cisco Catalyst 9300. Для забезпечення великої кількості кінцевих вузлів якісним, швидким зв'язком та забезпечення масштабованості мережі було обрано комутатори моделі Cisco Catalyst C9300-48T, який має сорок вісім портів GigabitEthernet, що дає змогу підключати велику кількість кінцевих вузлів або підключати нові мережеві пристрої.

3.2 Налагодження корпоративної комп'ютерної мережі

Так як немає змоги налагодити корпоративну комп'ютерну мережу на реальному обладнанні через її відсутність та дороговизну, то саме налагодження корпоративної комп'ютерної мережі буде проведено в програмному симуляторі GNS3.

Враховуючи недоліки використання програмного симулятора GNS3 та в цілях економії ресурсів комп'ютера, на якому буде запущена симуляція корпоративної мережі, для налагодження мережі будуть використовуватися міжмережні екрани Cisco ASA 5506-X й некеровані комутатори та саме налагодження буде проводитись для центральної мережі OFFICE01 та мережі філії OFFICE02. Налагодження міжмережних екранів Cisco ASA на всіх моделях лінійки Cisco ASA 5500-X однакове, тому сценарії налагодження можна застосувати на реальному обладнанні для інших моделей Cisco ASA

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

5500-Х. Загальне налагодження підсистеми захисту корпоративної мережі загалом можна розбити на два етапи: налагодження основних головних функцій мережі на міжмережних екранах Cisco ASA та налагодження додаткових функцій.

До налагодження роботи основних функцій корпоративної комп'ютерної мережі на міжмережних екранах Cisco ASA можна віднести:

- налагодження параметрів зон безпек та IP-адресації;
- налагодження мережевих об'єктів та трансляції адрес NAT для доступу користувачів мереж філій та центральної мережі до глобальної мережі Інтернет;

- налагодження політик міжзональної взаємодії через розширені списки ACL;

- налагодження захищеного зв'язку між центральною мережею та мережею філії за допомогою технології IPSec VPN типу "Site-To-Site".

До налагодження роботи додаткових функцій корпоративної комп'ютерної мережі на міжмережних екранах Cisco ASA можна віднести:

- налагодження серверів DHCP;
- налагодження динамічної маршрутизації OSPF;
- налагодження роботи глибокої перевірки пакетів DPI;
- задання парольного доступу до міжмережних екранів Cisco ASA та забезпечення доступу до них через протокол SSH.

Налагодження структури Windows-мережі відбувається на контролерах домену, які розташовані в офісах організації.

Першим кроком в налагодженні підсистеми захисту корпоративної комп'ютерної мережі є налагодження зон безпек та IP-адресації на міжмережних екранах Cisco ASA.

Сценарій налагодження параметрів зон безпеки та IP-адресації на міжмережному екрані Cisco ASA Office01_ASA наведено нижче:

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

```

...
// Задання імен та рівнів безпеки зонам на інтерфейсах
Office01-ASA# configure terminal
Office01-ASA(config)# interface GigabitEthernet0/0
Office01-ASA(config-if)# nameif inside01
Office01-ASA(config-if)# security-level 100
Office01-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
Office01-ASA(config-if)# no shutdown
Office01-ASA(config-if)# exit
Office01-ASA(config)# interface GigabitEthernet0/1
Office01-ASA(config-if)# nameif inside02
Office01-ASA(config-if)# security-level 100
Office01-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
Office01-ASA(config-if)# no shutdown
Office01-ASA(config-if)# exit
Office01-ASA(config)# interface GigabitEthernet0/2
Office01-ASA(config-if)# nameif dmz
Office01-ASA(config-if)# security-level 85
Office01-ASA(config-if)# ip address 192.168.10.1 255.255.255.0
Office01-ASA(config-if)# no shutdown
Office01-ASA(config-if)# exit
Office01-ASA(config)# interface GigabitEthernet0/3
Office01-ASA(config-if)# nameif outside
Office01-ASA(config-if)# ip address 100.1.1.1 255.255.255.224
Office01-ASA(config-if)# no shutdown
Office01-ASA(config-if)# exit
...

```

Сценарій налагодження параметрів зон безпеки та IP-адресації на міжмережному екрані Cisco ASA Office02_ASA наведено нижче:

```

...
Office02-ASA# configure terminal
Office02-ASA(config)# interface GigabitEthernet0/0
Office02-ASA(config-if)# nameif inside
Office02-ASA(config-if)# security-level 100
Office02-ASA(config-if)# ip address 192.168.3.1 255.255.255.0
Office02-ASA(config-if)# no shutdown
Office02-ASA(config-if)# exit
Office02-ASA(config)# interface GigabitEthernet0/1
Office02-ASA(config-if)# nameif outside
Office02-ASA(config-if)# ip address 100.6.1.1 255.255.255.224
Office02-ASA(config-if)# no shutdown
Office02-ASA(config-if)# exit
...

```

Після налагодження параметрів зон безпеки та IP-адресації потрібно забезпечити користувачів локальних мереж корпоративної мережі доступом

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

до Інтернету. Тому далі було налагоджено мережеві об'єкти та трансляцію адрес NAT.

Сценарій налагодження мережевих об'єктів та трансляції адрес NAT на міжмережному екрані Office01_ASA наведено нижче:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# object network INSIDE01-NET
Office01-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
Office01-ASA(config-network-object)# nat (inside01,outside) dynamic interface
Office01-ASA(config-network-object)# exit
Office01-ASA(config)# object network INSIDE02-NET
Office01-ASA(config-network-object)# subnet 192.168.2.0 255.255.255.0
Office01-ASA(config-network-object)# nat (inside02,outside) dynamic interface
Office01-ASA(config-network-object)# exit
Office01-ASA(config)# object network DMZ-NET
Office01-ASA(config-network-object)# subnet 192.168.10.0 255.255.255.0
Office01-ASA(config-network-object)# nat (DMZ,outside) dynamic interface
Office01-ASA(config-network-object)# exit
Office01-ASA(config)# exit
...
```

Сценарій налагодження мережевого об'єкту та трансляції адрес NAT на міжмережному екрані Office02_ASA наведено нижче:

```
...
Office02-ASA# configure terminal
Office02-ASA(config)# object network INSIDE-NET
Office02-ASA(config-network-object)# subnet 192.168.3.0 255.255.255.0
Office02-ASA(config-network-object)# nat (inside,outside) dynamic interface
Office02-ASA(config-network-object)# exit
Office02-ASA(config)# exit
...
```

Після надання доступу користувачів локальних мереж до Інтернету та налагодження перетворення адрес через NAT потрібно налагодити взаємодію глобальної мережі Інтернет з публічними серверами зони DMZ, а саме задати серверам статичну IP-адресацію через NAT.

Сценарій задання статичних IP-адрес публічним серверам на міжмережному екрані Office01_ASA наведено нижче:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# object network DNS_SERVER-EXTERNAL-IP
Office01-ASA(config-network-object)# host 192.168.10.2
```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

```
Office01-ASA(config-network-object)# nat (DMZ,outside) static 100.1.1.3
Office01-ASA(config-network-object)# exit
Office01-ASA(config)# object network WEB_SERVER-EXTERNAL-IP
Office01-ASA(config-network-object)# host 192.168.10.3
Office01-ASA(config-network-object)# nat (dmz,outside) static 100.1.1.4
Office01-ASA(config-network-object)# exit
...
```

Задавши статичну IP-адресацію публічним серверам, все одно не буде доступу до них з глобальної мережі Інтернет, так як потрібно задати політику міжзональної взаємодії через розширені списки ACL на міжмережному екрані Office01_ASA та задати дозвіл на проходження контролюючих пакетів ICMP для коректної роботи команди tracer, щоб відслідковувати проходження пакетів.

Сценарій налагодження політики міжзональної взаємодії та дозвіл на проходження контролюючих пакетів ICMP через розширені списки ACL на міжмережному екрані Office01_ASA:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit ip
any host 192.168.10.2
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit tcp
any host 192.168.10.3 eq www
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
icmp any any unreachable
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
icmp any any time-exceeded
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
icmp any any source-quench
Office01-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
icmp any any echo-reply
Office01-ASA(config)# access-group ALLOW_TRAFFIC_INSIDE in interface
outside
Office01-ASA(config)# access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONLY
extended permit ip 192.168.2.0 255.255.255.0 host
192.168.1.253
Office01-ASA(config)# access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONLY
extended permit ip 192.168.2.0 255.255.255.0 host
192.168.1.254
Office01-ASA(config)# access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONLY
extended permit ip host 192.168.10.2 host 192.168.1.254
```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

```
Office01-ASA(config)# access-group
    ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONLY
    out interface inside01
Office01-ASA(config)# access-list ALLOW_DNS_SERVER_TRAFFIC_TO_PDC
    extended permit ip host 192.168.10.2 host 192.168.1.254
Office01-ASA(config)# access-group ALLOW_DNS_SERVER_TRAFFIC_TO_PDC
    in interface dmz
Office01-ASA(config)# exit
...
```

Сценарій налагодження розширених списків ACL для задання дозволу на проходження контролюючих пакетів ICMP на міжмережному екрані Office02_ASA:

```
...
Office02-ASA# configure terminal
Office02-ASA(config)# access-list LAN2_LAN1 extended permit ip 192.168.3.0
    255.255.255.0 192.168.1.0 255.255.255.0
Office02-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
    icmp any any echo-reply
Office02-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
    icmp any any source-quench
Office02-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
    icmp any any unreachable
Office02-ASA(config)# access-list ALLOW_TRAFFIC_INSIDE extended permit
    icmp any any time-exceeded
Office02-ASA(config)# access-group ALLOW_TRAFFIC_INSIDE in interface
    outside
Office02-ASA(config)# exit
...
```

Останнім кроком в налагодженні основних функцій корпоративної комп'ютерної мережі на міжмережних екранах Cisco ASA є налагодження взаємодії центральної мережі з мережею філії, тобто забезпечити захищеним зашифрованим зв'язком між цими двома мережами за допомогою IPSec VPN типу "Site-To-Site".

Сценарій налагодження зв'язку VPN між центральною мережею та мережею філії на міжмережному екрані Office01_ASA:

```
...
// Налаштування політики шифрування ikev1
Office01-ASA# configure terminal
Office01-ASA(config)# crypto ikev1 policy 10
Office01-ASA(config-ikev1-policy)# authentication pre-share
Office01-ASA(config-ikev1-policy)# encryption aes
```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

```

Office01-ASA(config-ikev1-policy)# hash sha
Office01-ASA(config-ikev1-policy)# group 2
Office01-ASA(config-ikev1-policy)# lifetime 7200
Office01-ASA(config-ikev1-policy)# exit
Office01-ASA(config)# crypto ikev1 enable outside
Office01-ASA(config)# crypto isakmp identity address
// Налаштування тунелів з ключем шифрування
Office01-ASA(config)# tunnel-group 100.6.1.1 type ipsec-l2l
Office01-ASA(config)# tunnel-group 100.6.1.1 ipsec-attributes
Office01-ASA(config-tunnel-ipsec)# ikev1 pre-shared-key officesecretkey
Office01-ASA(config-tunnel-ipsec)# exit
// Налаштування крипто-карти для заданих підмереж в розширеному листі ACL
Office01-ASA(config)# access-list LAN1_LAN2 extended permit ip 192.168.1.0
255.255.255.0 192.168.3.0 255.255.255.0
Office01-ASA(config)# crypto map CRYP_MAP 10 match address LAN1_LAN2
Office01-ASA(config)# crypto map CRYP_MAP 10 set peer 100.6.1.1
Office01-ASA(config)# crypto ipsec ikev1 transform-set TRANS_SET
esp-aes esp-sha-hmac
Office01-ASA(config)# crypto map CRYP_MAP 10 set ikev1 transform-set
TRANS_SET
Office01-ASA(config)# crypto map CRYP_MAP 10 set security-association lifetime
seconds 7200
Office01-ASA(config)# crypto map CRYP_MAP interface outside
Office01-ASA(config)# exit
...

```

Сценарій налагодження зв'язку VPN між мережею філії та центральною мережею на міжмережному екрані Office02_ASA:

```

...
Office02-ASA# configure terminal
Office02-ASA(config)# crypto ikev1 policy 10
Office02-ASA(config-ikev1-policy)# authentication pre-share
Office02-ASA(config-ikev1-policy)# encryption aes
Office02-ASA(config-ikev1-policy)# hash sha
Office02-ASA(config-ikev1-policy)# group 2
Office02-ASA(config-ikev1-policy)# lifetime 7200
Office02-ASA(config-ikev1-policy)# exit
Office02-ASA(config)# crypto ikev1 enable outside
Office02-ASA(config)# crypto isakmp identity address
Office02-ASA(config)# tunnel-group 100.1.1.1 type ipsec-l2l
Office02-ASA(config)# tunnel-group 100.1.1.1 ipsec-attributes
Office02-ASA(config-tunnel-ipsec)# ikev1 pre-shared-key officesecretkey
Office02-ASA(config-tunnel-ipsec)# exit
Office02-ASA(config)# access-list LAN2_LAN1 extended permit ip 192.168.3.0
255.255.255.0 192.168.1.0 255.255.255.0
Office02-ASA(config)# crypto map CRYP_MAP 10 match address LAN2_LAN1
Office02-ASA(config)# crypto map CRYP_MAP 10 set peer 100.1.1.1
Office02-ASA(config)# crypto ipsec ikev1 transform-set TRANS_SET

```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

```

esp-aes esp-sha-hmac
Office02-ASA(config)# crypto map CRYPT_MAP 10 set ikev1 transform-set
TRANS_SET
Office02-ASA(config)# crypto map CRYPT_MAP 10 set security-association lifetime
seconds 7200
Office02-ASA(config)# crypto map CRYPT_MAP interface outside
Office02-ASA(config)# exit
...

```

Для того, щоб налаштування NAT не перекривали весь зв'язок VPN потрібно налагодити подвійний NAT ("Twice NAT") на міжмережних екранах.

Сценарії налагодження подвійного NAT на міжмережних екранах Office01_ASA та Office02_ASA наведено нижче:

```

...
Office01-ASA# configure terminal
Office01-ASA(config)# object network LAN2
Office01-ASA(config-network-object)# subnet 192.168.3.0 255.255.255.0
Office01-ASA(config-network-object)# exit
Office01-ASA(config)# nat (inside01,outside) source static INSIDE01-NET
INSIDE01-NET destination static LAN2 LAN2
Office01-ASA(config)# exit
...

```

```

...
Office02-ASA# configure terminal
Office02-ASA(config)# object network LAN1
Office02-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
Office02-ASA(config-network-object)# exit
Office02-ASA(config)# nat (inside,outside) source static INSIDE-NET INSIDE-NET
destination static LAN1 LAN1
Office02-ASA(config)# exit
...

```

Після налагодження всіх основних функцій корпоративної комп'ютерної мережі на міжмережних екранах Cisco ASA потрібно перейти до налагодження всіх додаткових функцій.

Одна з додаткових функцій є налагодження DHCP-серверів на міжмережних екранах для локальних мереж.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Сценарії налагодження серверів DHCP на міжмережних екранах Office01_ASA та Office02_ASA наведено нижче:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# dhcpd address 192.168.1.2-192.168.1.200 inside01
Office01-ASA(config)# dhcpd enable inside01
Office01-ASA(config)# dhcpd address 192.168.2.2-192.168.2.254 inside02
Office01-ASA(config)# dhcpd enable inside02
Office01-ASA(config)# dhcpd dns 192.168.1.254
Office01-ASA(config)# exit
...
...
Office02-ASA# configure terminal
Office02-ASA(config)# dhcpd address 192.168.3.2-192.168.3.253 inside
Office02-ASA(config)# dhcpd dns 192.168.3.254
Office02-ASA(config)# dhcpd enable inside
Office02-ASA(config)# exit
...
```

Як видно зі сценаріїв налагодження, пул DHCP-адрес на міжмережних екранах Cisco ASA не досягав свого максимального розміру, так як локальним серверам було задано статичну IP-адресу, яка не має бути використана як динамічна.

Для того, щоб маршрутизувалися пакети до Інтернету та між мережами офісів, потрібно налагодити протокол динамічної маршрутизації OSPF з використанням аутентифікації пакетів на інтерфейсах на міжмережних екранах Cisco ASA.

Сценарій налагодження протоколу динамічної маршрутизації OSPF на міжмережному екрані Office01_ASA наведено нижче:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# interface GigabitEthernet0/3
Office01-ASA(config-if)# ospf authentication message-digest
Office01-ASA(config-if)# ospf message-digest-key 1 md5 office01secret
Office01-ASA(config-if)# exit
Office02-ASA(config)# router ospf 1
Office02-ASA(config-router)# network 192.168.1.0 255.255.255.0 area 1
Office02-ASA(config-router)# network 192.168.2.0 255.255.255.0 area 1
Office02-ASA(config-router)# network 192.168.10.0 255.255.255.0 area 1
Office02-ASA(config-router)# network 100.1.1.0 255.255.255.224 area 0
```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Office02-ASA(config-router)# exit

...

Сценарій налагодження протоколу динамічної маршрутизації OSPF на міжмережному екрані Office01_ASA наведено нижче:

...

Office02-ASA# configure terminal

Office02-ASA(config)# interface GigabitEthernet0/1

Office02-ASA(config-if)# ospf authentication message-digest

Office02-ASA(config-if)# ospf message-digest-key 1 md5 office02secret

Office02-ASA(config-if)# exit

Office02-ASA(config)# router ospf 1

Office02-ASA(config-router)# network 192.168.3.0 255.255.255.0 area 1

Office02-ASA(config-router)# network 100.6.1.0 255.255.255.224 area 0

Office02-ASA(config-router)# exit

...

Для більшої безпеки та проходженню зворотніх пакетів ехо-запитів з глобальної мережі Інтернет до локальних мереж центральної мережі OFFICE01 та мережі філії OFFICE02 та проходженню пакетів http, потрібно дописати до глибокої перевірки пакетів за замовчуванням, яка вже виконує свою роботу на міжмережних екранах, перевірку пакетів icmp та http.

Сценарії налагодження глибокої перевірки пакетів на міжмережних екранах Office01_ASA та Office02_ASA наведено нижче:

...

Office01-ASA# configure terminal

Office01-ASA(config)# policy-map global_policy

Office01-ASA(config-pmap)# class inspection_default

Office01-ASA(config-pmap-c)# inspect icmp

Office01-ASA(config-pmap-c)# inspect http

Office01-ASA(config-pmap-c)# inspect icmp error

Office01-ASA(config-pmap-c)# exit

...

...

Office02-ASA# configure terminal

Office02-ASA(config)# policy-map global_policy

Office02-ASA(config-pmap)# class inspection_default

Office02-ASA(config-pmap-c)# inspect icmp

Office02-ASA(config-pmap-c)# inspect http

Office02-ASA(config-pmap-c)# inspect icmp error

Office02-ASA(config-pmap-c)# exit

...

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Останнім кроком в налагодженні підсистеми захисту корпоративної комп'ютерної мережі є задання парольного доступу до міжмережних екранів Cisco ASA та забезпечення доступу до них через протокол віддаленого доступу SSH лише з локальної мережі.

Сценарії налагодження парольного доступу до міжмережних екранів Office01_ASA й Office02_ASA та забезпечення доступу до них через протокол віддаленого доступу SSH лише з локальної мережі наведено нижче:

```
...
Office01-ASA# configure terminal
Office01-ASA(config)# enable password Office01pass
Office01-ASA(config)# username admin password Admin157395 privilege 15
Office01-ASA(config)# crypto key generate rsa modulus 1024
Office01-ASA(config)# aaa authentication ssh console LOCAL
Office01-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside01
Office01-ASA(config)# exit
...
...
Office02-ASA# configure terminal
Office02-ASA(config)# enable password Office02pass
Office02-ASA(config)# username admin password Qzwxecrvtbyn123 privilege 15
Office02-ASA(config)# crypto key generate rsa modulus 1024
Office02-ASA(config)# aaa authentication ssh console LOCAL
Office02-ASA(config)# ssh 192.168.3.0 255.255.255.0 inside
Office02-ASA(config)# exit
...
```

Вивід конфігураційних файлів міжмережних екранів Cisco ASA Office01_ASA та Office02_ASA за допомогою команди show running-config наведено в додатку Г.

На рис. Г.1-Г.7 додатку Г зображено налагодження Windows-мережі для забезпечення більшого захисту та надійної роботи серверів та робочих станцій.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

3.3 Тестування функціоналу корпоративної мережі

Першим кроком у перевірці працездатності корпоративної мережі буде перевірка DHCP-серверів, налаштованих на міжмережних екранах Office01_ASA та Office02_ASA для різних внутрішніх зон центральної мережі OFFICE01 та однієї внутрішньої зони мережі філії OFFICE02:

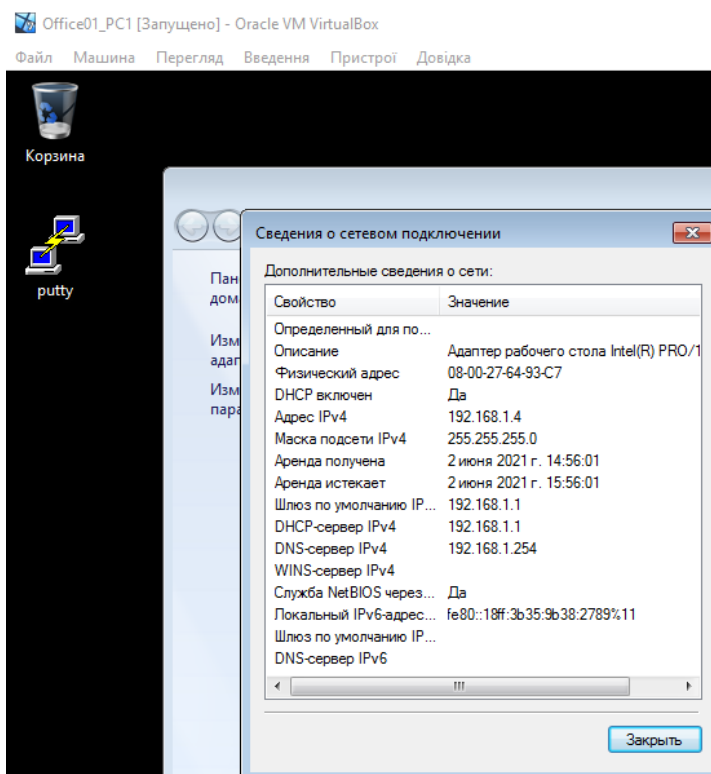


Рисунок 3.1 – Успішне отримання динамічної IP-адреси від DHCP-сервера міжмережного екрану Office01_ASA робочою станцією Office01_PC1 зони inside01

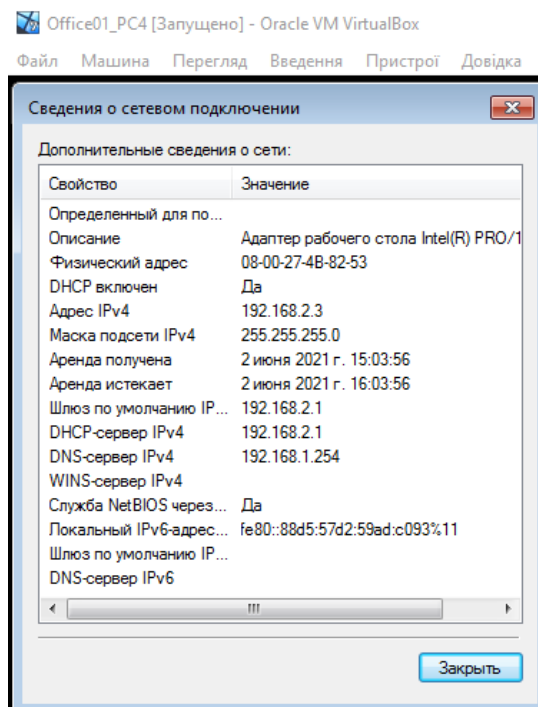


Рисунок 3.2 – Успішне отримання динамічної IP-адреси від DHCP-сервера міжмережного екрану Office01_ASA робочою станцією Office01_PC4 зони inside02

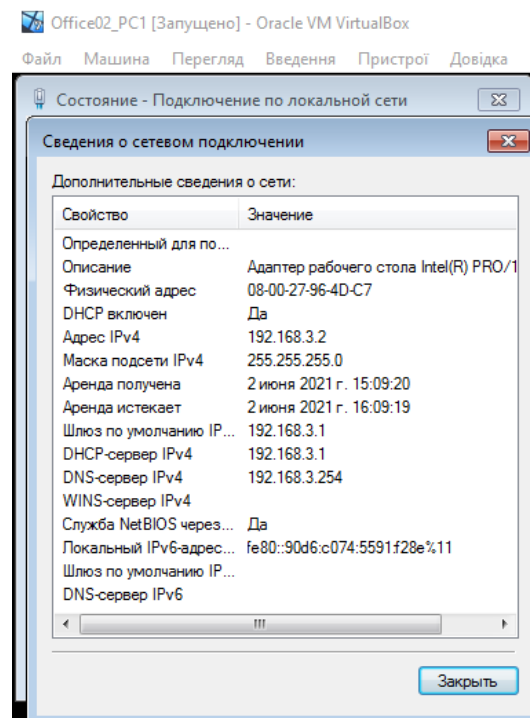


Рисунок 3.3 – Успішне отримання динамічної IP-адреси від DHCP-сервера міжмережного екрану Office02_ASA робочою станцією Office02_PC1 зони inside

Сервери DHCP, налаштовані на міжмережних екранах корпоративної мережі, працюють коректно.

Перевіримо налаштування протоколу динамічної маршрутизації OSPF на міжмережних екранах корпоративної комп'ютерної мережі. Спробуємо відправити ехо-запити та виконати команду tracert на віддалений хост з IP-адресою 200.188.231.2, який знаходиться в Інтернеті:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\admin>tracert 200.188.231.2

Трассировка маршрута к ADMINPK [200.188.231.2]
с максимальным числом прыжков 30:

  1      2 ms      *          1 ms    192.168.3.1
  2     13 ms     11 ms     9 ms    100.6.1.2
  3     13 ms     19 ms    20 ms    100.4.1.1
  4     35 ms     40 ms    53 ms    100.5.1.2
  5     61 ms     50 ms    50 ms    ADMINPK [200.188.231.2]

Трассировка завершена.
C:\Users\admin>_
  
```

Рисунок 3.4 – успішна відправка ехо-запитів на віддалений хост з робочої станції Office02_PC1, яка знаходиться в мережі філії OFFICE02 в зоні inside

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\admin>ping 200.188.231.2

Обмен пакетами с 200.188.231.2 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 200.188.231.2: число байт=32 время=47мс TTL=61
Ответ от 200.188.231.2: число байт=32 время=51мс TTL=61
Ответ от 200.188.231.2: число байт=32 время=37мс TTL=61

Статистика Ping для 200.188.231.2:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 37мсек, Максимальное = 51 мсек, Среднее = 45 мсек
  
```

Рисунок 3.5 – успішна відправка ехо-запитів на віддалений хост з робочої станції Office01_PC1, яка знаходиться в центральній мережі OFFICE01 в зоні inside01

Були успішно відправлені запити на віддалений хост Інтернету з робочої станції центральної мережі OFFICE01 та робочої станції філії OFFICE02.

Отже, протокол динамічної маршрутизації OSPF налаштований коректно на міжмережних екранах корпоративної комп'ютерної мережі.

Перевіримо роботу IPSec VPN типу “Site-To-Site”, налаштований на міжмережних екранах Office01_ASA та Office02_ASA, щоб був зв'язок між зоною inside01 центральної мережі OFFICE01 та зоною inside мережі філії OFFICE02:

```

Office01_PC1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

C:\Windows\system32\cmd.exe

Обмен пакетами с 192.168.3.2 по 32 байтам данных:
Ответ от 192.168.3.2: число байт=32 время=30мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=41мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=38мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=35мс TTL=126

Статистика Ping для 192.168.3.2:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потерь>
  Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 41 мсек, Среднее = 36 мсек

C:\Users\admin>tracert 192.168.3.2

Трассировка маршрута к OFFICE02_PC1 [192.168.3.2]
с максимальным числом прыжков 30:

  1      1 ms      *      1 ms    192.168.1.1
  2      *        *        *        Превышен интервал ожидания для запроса.
  3     37 ms     25 ms    30 ms    OFFICE02_PC1 [192.168.3.2]

Трассировка завершена.
  
```

Рисунок 3.6 – Успішний зв’язок робочої станції Office01_PC1 зони inside01 центральної мережі OFFICE01 з робочою станцією Office02_PC1 зони inside мережі філії OFFICE02

```

Office02_PC1 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\admin>ping 192.168.1.4

Обмен пакетами с 192.168.1.4 по 32 байтам данных:
Ответ от 192.168.1.4: число байт=32 время=49мс TTL=128
Ответ от 192.168.1.4: число байт=32 время=43мс TTL=128
Ответ от 192.168.1.4: число байт=32 время=40мс TTL=128
Ответ от 192.168.1.4: число байт=32 время=28мс TTL=128

Статистика Ping для 192.168.1.4:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потерь>
  Приблизительное время приема-передачи в мс:
    Минимальное = 28мсек, Максимальное = 49 мсек, Среднее = 40 мсек
  
```

Рисунок 3.7 – Успішний зв’язок робочої станції Office02_PC1 зони inside мережі філії OFFICE02 з робочою станцією Office01_PC1 зони inside01 центральної мережі OFFICE01

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\admin>ping 192.168.2.3

Обмен пакетами с 192.168.2.3 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.2.3:
  Пакетов: отправлено = 4, получено = 0, потеряно = 4
  (100% потеря)

```

Рисунок 3.8 – Спроба встановити зв’язок робочою станцією Office02_PC1 зони inside мережі філії OFFICE02 з робочою станцією Office01_PC4 зони inside02 центральної мережі OFFICE01

IPSec VPN типу “Site-To-Site” налаштований коректно. Є зв’язок між двома зонами inside01 й inside центральної мережі та мережі філії відповідно та недопустимість будь-яких інших зв’язків між цими двома мережами корпоративної комп’ютерної мережі.

Перевіримо підсистему політик міжзонального обміну центральної мережі OFFICE01. Зона inside01 повинна мати доступ до Інтернету та до всіх внутрішніх зон (inside02, DMZ):

```

C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.1.253

Обмен пакетами с 192.168.1.253 по 32 байтами данных:
Ответ от 192.168.1.253: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.253: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.253: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.253: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.1.253:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потеря)
  Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 2 мсек, Среднее = 1 мсек

C:\Users\admin>ping 192.168.1.254

Обмен пакетами с 192.168.1.254 по 32 байтами данных:
Ответ от 192.168.1.254: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.254: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.254: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=1мс TTL=128

Статистика Ping для 192.168.1.254:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потеря)
  Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

```

Рисунок 3.9 – Успішна відправка ехо-запитів з робочої станції Office01_PC1 зони inside01 до серверів Primary_Domain_Server та FTP_Server цієї ж зони

```

C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.2.3

Обмен пакетами с 192.168.2.3 по с 32 байтами данных:
Ответ от 192.168.2.3: число байт=32 время=6мс TTL=128
Ответ от 192.168.2.3: число байт=32 время=2мс TTL=128
Ответ от 192.168.2.3: число байт=32 время=4мс TTL=128
Ответ от 192.168.2.3: число байт=32 время=3мс TTL=128

Статистика Ping для 192.168.2.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 6 мсек, Среднее = 3 мсек

C:\Users\admin>ping 192.168.10.2

Обмен пакетами с 192.168.10.2 по с 32 байтами данных:
Ответ от 192.168.10.2: число байт=32 время=3мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=3мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=4мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=3мс TTL=128

Статистика Ping для 192.168.10.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 4 мсек, Среднее = 3 мсек

C:\Users\admin>ping 192.168.10.3

Обмен пакетами с 192.168.10.3 по с 32 байтами данных:
Ответ от 192.168.10.3: число байт=32 время=4мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=3мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=4мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=3мс TTL=128

Статистика Ping для 192.168.10.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 4 мсек, Среднее = 3 мсек
  
```

Рисунок 3.10 – Успішна відправка ехо-запитів з робочої станції Office01_PC1 зони inside01 до робочої станції Office01_PC4 зони inside02 та до серверів Secondary_DNS_Server і WEB_Server зони DMZ

Зона inside02 має доступ до Інтернету, зони DMZ та лише тільки до серверів Primary_Domain_Controller і FTP_Server зони inside01.

Зона DMZ має доступ лише до Інтернету, окрім сервера Secondary_Domain_Controller. Даний сервер має доступ до сервера Primary_Domain_Controller зони inside01, так як копіює записи DNS з головного контролера домену для відкриття їх до публічного доступу, Інтернету:

```

C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.1.253

Обмен пакетами с 192.168.1.253 по с 32 байтами данных:
Ответ от 192.168.1.253: число байт=32 время=4мс TTL=128
Ответ от 192.168.1.253: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.253: число байт=32 время=3мс TTL=128
Ответ от 192.168.1.253: число байт=32 время=3мс TTL=128

Статистика Ping для 192.168.1.253:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 4 мсек, Среднее = 3 мсек

C:\Users\admin>ping 192.168.1.254

Обмен пакетами с 192.168.1.254 по с 32 байтами данных:
Ответ от 192.168.1.254: число байт=32 время=4мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128

Статистика Ping для 192.168.1.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 4 мсек, Среднее = 2 мсек
  
```

Рисунок 3.11 – Успішний зв’язок робочої станції Office01_PC4 зони inside02 з серверами Primary_Domain_Controller та FTP_Server зони inside01

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\admin>ping 192.168.1.4

Обмен пакетами с 192.168.1.4 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.1.4:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\admin>
  
```

Рисунок 3.30. Неможливість зв’язку робочої станції Office01_PC4 зони inside02 з робочою станцією Office01_PC1 та й з іншими робочими станціями зони inside01

```

Office01_PC4 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.10.2

Обмен пакетами с 192.168.10.2 по 32 байтам данных:
Ответ от 192.168.10.2: число байт=32 время=3мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=2мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=1мс TTL=128
Ответ от 192.168.10.2: число байт=32 время=2мс TTL=128

Статистика Ping для 192.168.10.2:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
  Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\admin>ping 192.168.10.3

Обмен пакетами с 192.168.10.3 по 32 байтам данных:
Ответ от 192.168.10.3: число байт=32 время=3мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=2мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=2мс TTL=128
Ответ от 192.168.10.3: число байт=32 время=2мс TTL=128

Статистика Ping для 192.168.10.3:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
  Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\admin>ping 200.188.231.2

Обмен пакетами с 200.188.231.2 по 32 байтам данных:
Превышен интервал ожидания для запроса.
Ответ от 200.188.231.2: число байт=32 время=38мс TTL=61
Ответ от 200.188.231.2: число байт=32 время=38мс TTL=61
Ответ от 200.188.231.2: число байт=32 время=34мс TTL=61

Статистика Ping для 200.188.231.2:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потерь)
  Приблизительное время приема-передачи в мс:
    Минимальное = 34мсек, Максимальное = 38 мсек, Среднее = 36 мсек

```

Рисунок 3.12 – Успішний зв’язок робочої станції Office01_PC4 зони inside02 з серверами Secondary_DNS_Server та WEB_Server зони DMZ та з віддаленим хостом із Інтернету

```

Secondary_DNS_Server [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор>ping 192.168.1.254

Обмен пакетами с 192.168.1.254 по 32 байтам данных:
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128
Ответ от 192.168.1.254: число байт=32 время=2мс TTL=128

Статистика Ping для 192.168.1.254:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
  Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек

C:\Users\Администратор>ping 192.168.1.253

Обмен пакетами с 192.168.1.253 по 32 байтам данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

```

Рисунок 3.13 – Успішний зв’язок сервера Secondary_DNS_Server зони DMZ з сервером Primary_Domain_Server зони inside01 та неможливість зв’язку з іншими хостами різних зон

Перевірка політик міжзональної взаємодії, які налаштовані на міжмережному екрані Cisco ASA Office01_ASA, пройшла успішно, все працює коректно.

Перевіримо зв'язок робочих станцій з головним контролером домену Primary_Domain_Controller центральної мережі OFFICE01 та додатковим контролером домену Backup_Domain_Controller мережі філії OFFICE02 через міжмережні екрани Cisco ASA:

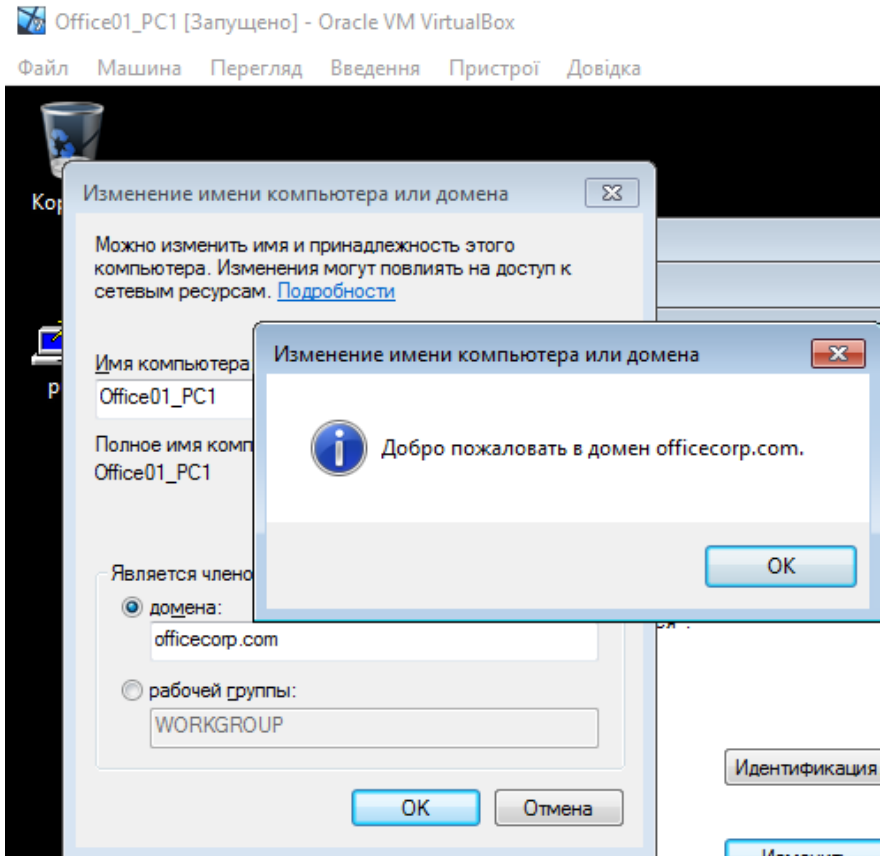


Рисунок 3.14 – Успішне додання робочої станції Office01_PC1 зони inside01 центральної мережі OFFICE01 до домену officecorp.com

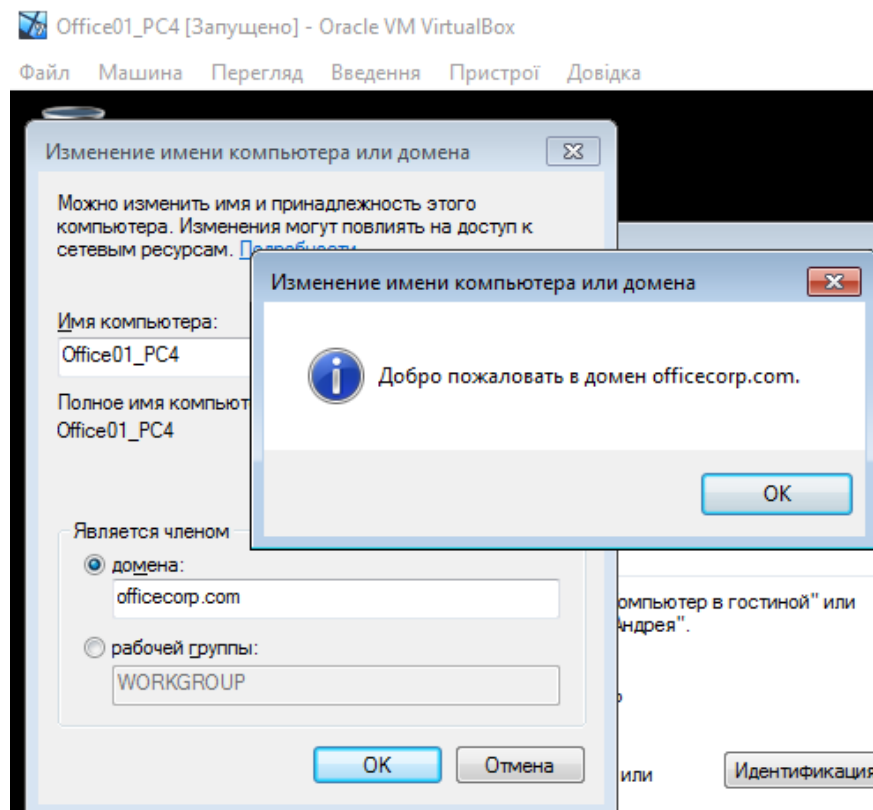


Рисунок 3.15 – Успішне додання робочої станції Office01_PC4 зони inside02 центральної мережі OFFICE01 до домену officescorp.com

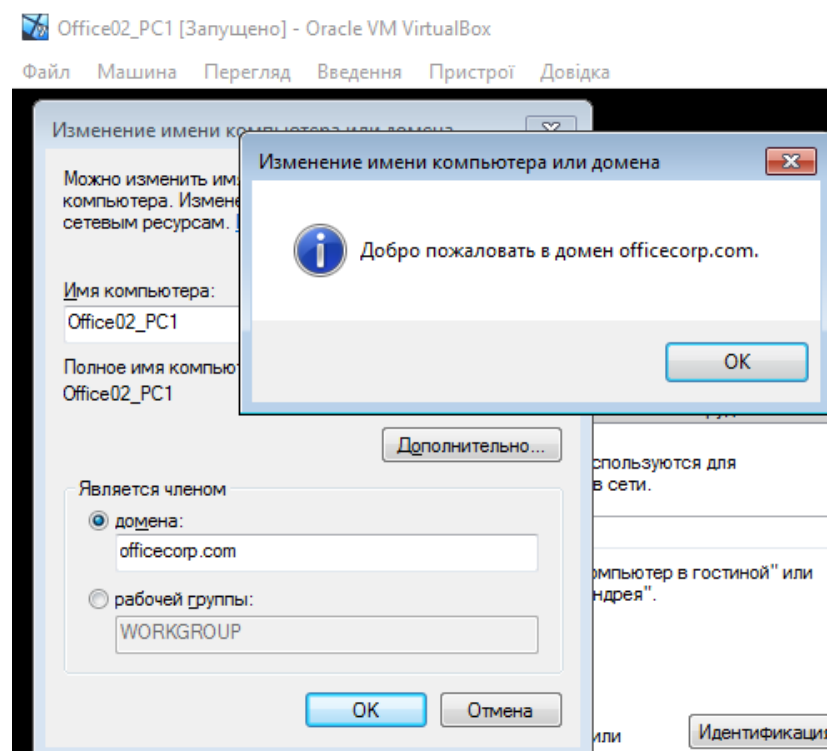


Рисунок 3.16 – Успішне додання робочої станції Office02_PC1 зони inside мережі філії OFFICE02 до домену officescorp.com

Приєднання робочих станції різних зон та мереж до домену officescorp.com пройшло успішно, політика міжзонального обміну на міжмереному екрані Office01_ASA працює коректно.

Перевіримо чи є зв'язок через VPN між контролерами домену, а саме чи реплікуються підключення між ними:

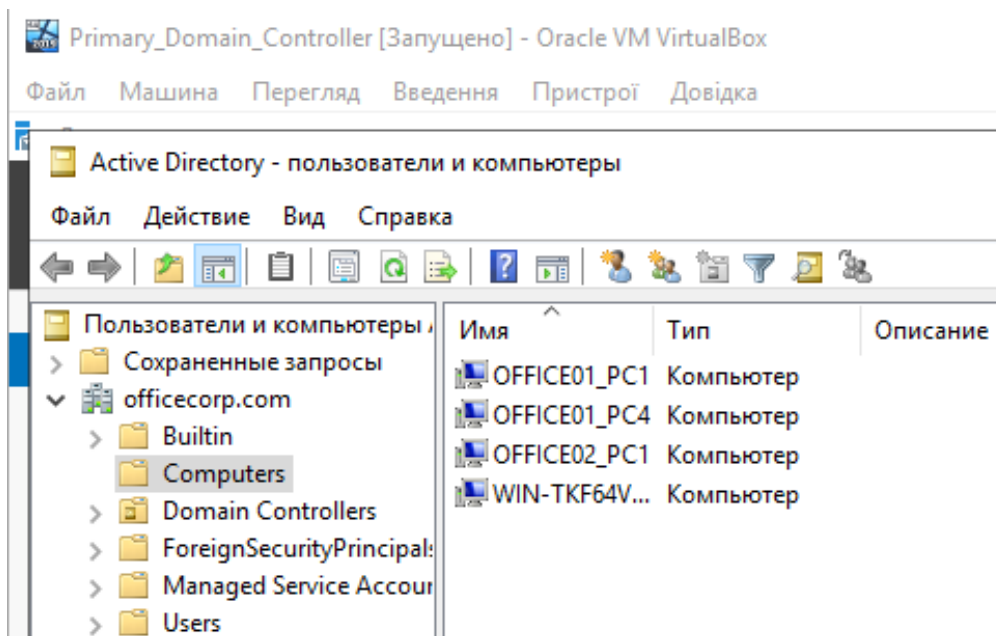


Рисунок 3.17 – Успішний вивід списку робочих станцій не тільки в центральній мережі, а й в мережі філії на головному контролері домену Primary_Domain_Controller

Зв'язок між контролерами домену успішний, вони успішно синхронізують всю інформацію, необхідну для роботи домена.

Перевіримо чи коректно працює вторинний DNS-сервер Secondary_Domain_Controller зони DMZ центральної мережі, який має статичну адресу 100.1.1.3 для публічного доступу, налаштовану на міжмережному екрані Office01_ASA. В Інтернеті є WEB-сервер з IP-адресою, якому через головний контролер домену Primary_Domain_Controller присвоїмо доменне ім'я internetweb.officescorp.com та з віддаленого хоста Інтернету спробуємо отримати доступ до даного сервера за доменним ім'ям:

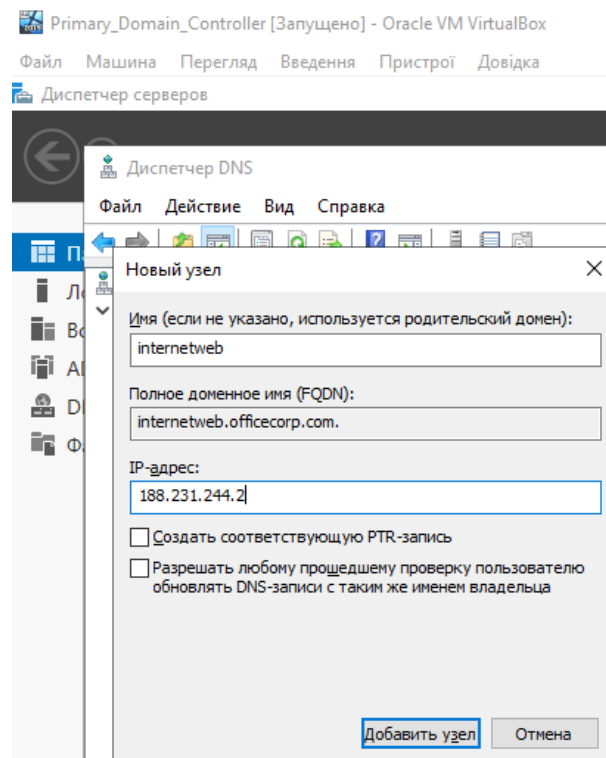


Рисунок 3.18 – Задання доменного імені IP-адресі WEB-сервера, який знаходиться в Інтернеті на головному контролері домену Primary_Domain_Controller

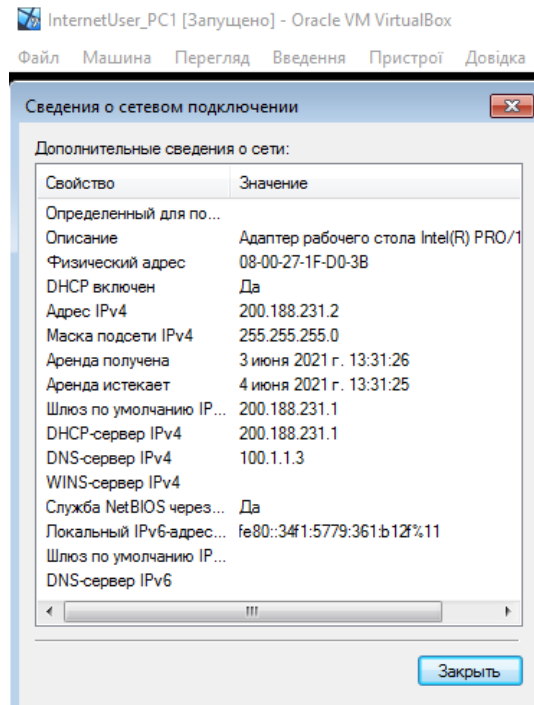


Рисунок 3.19 – Отримання віддаленим хостом з Інтернету динамічної IP-адреси від DHCP-сервера та отримання IP-адреси DNS-сервера (100.1.1.3)

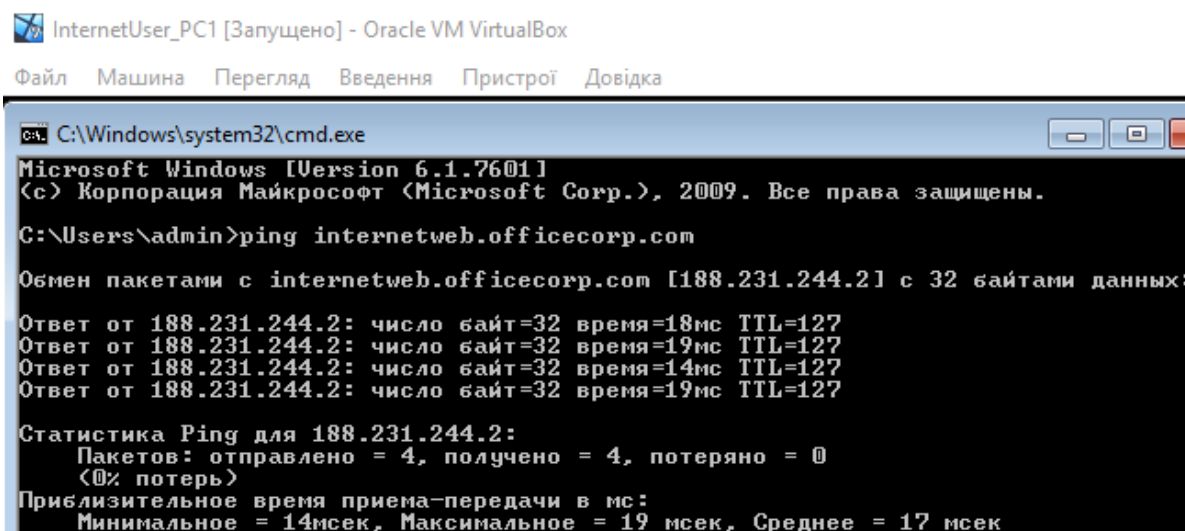


Рисунок 3.20 – Успішний зв’язок віддаленого хоста з WEB-сервером за доменним іменем в Інтернеті

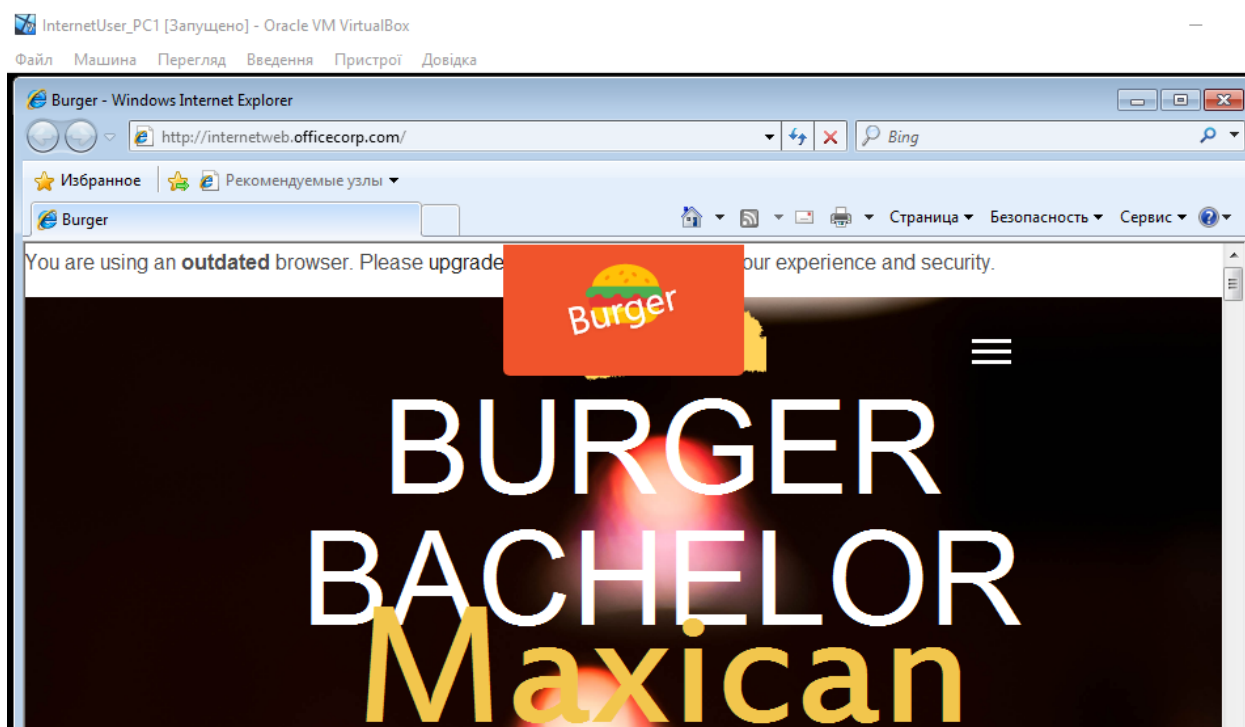


Рисунок 3.21 – Успішний вхід на сайт віддаленим хостом за доменним іменем WEB-сервера з Інтернету

Вторинний DNS-сервер Secondary_DNS_Server зони DMZ працює коректно, він отримує інформацію з головного контролера домену Primary_Domain_Server зони inside01 про записи DNS. Працює коректно налаштована публічна IP-адреса для Secondary_DNS_Server, яка налаштована на міжмережному екрані Office01_ASA.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк. 58
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевіримо доступ до міжмережних екранів Office01_ASA та Office02_ASA через протокол віддаленого доступу SSH та з'ясуємо чи можна підключитись до міжмережних екранів лише з локальних мереж:

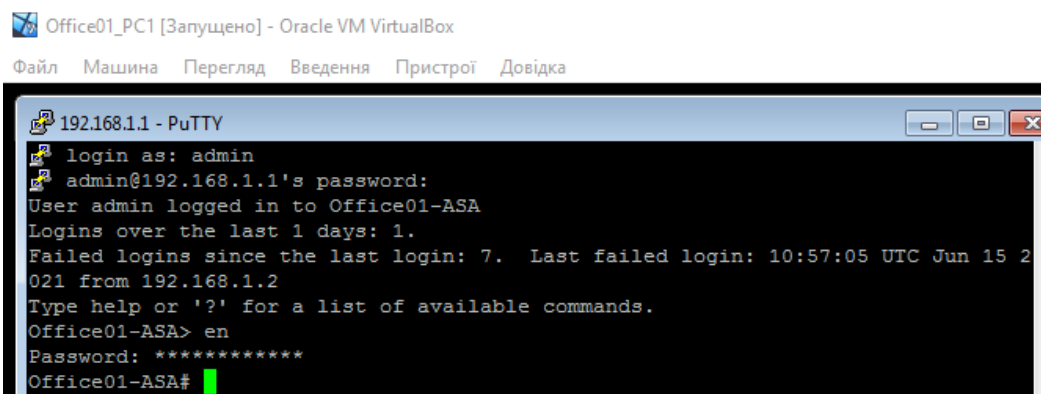


Рисунок 3.22 – Успішне підключення до міжмережного екрану Office01_ASA з робочої станції Office01_PC1 центральної мережі OFFICE01 по протоколу SSH

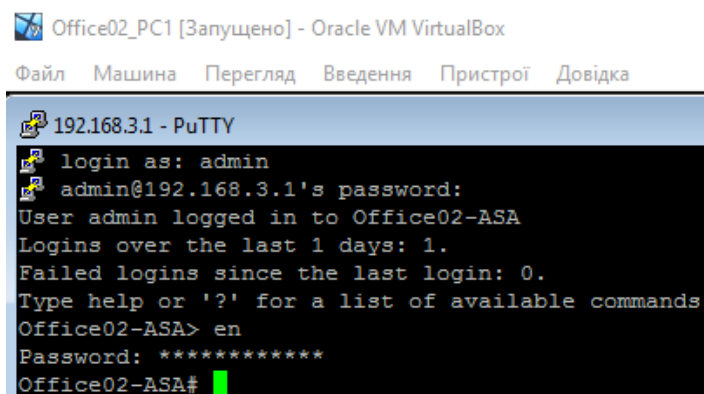


Рисунок 3.23 – Успішне підключення до міжмережного екрану Office02_ASA з робочої станції Office02_PC1 мережі філії OFFICE02 по протоколу SSH

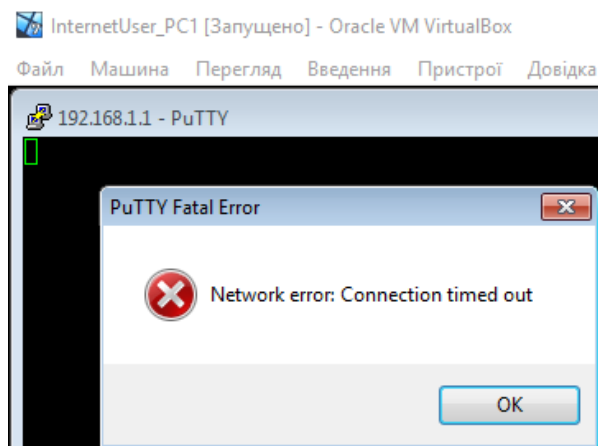


Рисунок 3.24 – Невдала спроба підключитися до міжмережного екрану Office01_ASA з віддаленого хоста в глобальній мережі

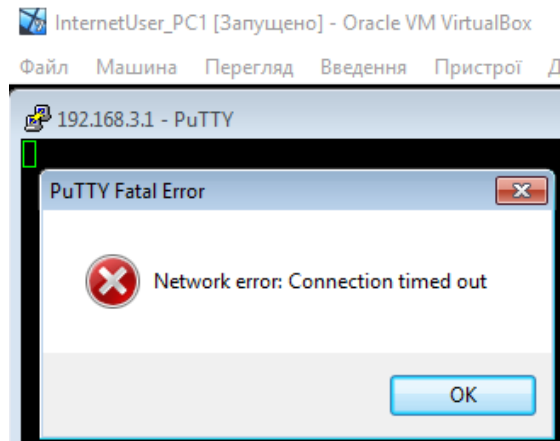


Рисунок 3.25 – Невдала спроба підключитися до міжмережного екрану Office02_ASA з віддаленого хоста в глобальній мережі

Парольний доступ до міжмережних екранів через протокол віддаленого доступу SSH тільки з локальних мереж офісів налаштовано коректно.

Після тестування всіх функцій корпоративної комп'ютерної мережі та її підсистеми захисту на базі рішень Cisco ASA можна зробити висновок, що все налагоджено коректно. Всі задачі, які були поставлені на дану кваліфікаційну роботу успішно досягнуто.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

ВИСНОВКИ

У даній кваліфікаційній роботі було досягнуто поставлені задачі через дослідження, проектування та розробку проекту підсистеми захисту корпоративної комп'ютерної мережі на базі рішень Cisco ASA.

Було вивчено та проаналізовано основні підходи до побудови корпоративної мережі за допомогою різних мережевих пристроїв та з використанням мережевих технологій, які забезпечують зв'язок в мережі та надійний захист. Проаналізовано особливості побудови корпоративних мереж за допомогою технологій та технологічних рішень від компанії Cisco. Після аналізу особливостей побудови корпоративної мережі за допомогою пристроїв компанії Cisco було обрано для побудови основи підсистеми захисту рішення Cisco ASA.

Cisco ASA наразі є потужним сучасним пристроєм для захисту різних мереж від різних мережевих атак, ціллю яких є викрадення, спотворення, руйнування інформації, або виведення з ладу всієї чи частини корпоративної мережі. Даний пристрій забезпечує не тільки захист, а й виконує функції комутатора та маршрутизатора, що є великою перевагою в економії та зменшення витрат на обслуговування певної кількості мережних пристроїв, що підтримують роботу мережі.

Для більш точного розуміння роботи міжмережного екрану було проаналізовано основні та додаткові функції даного пристрою для забезпечення захисту, зв'язку та обслуговування локальних мереж. Однією з основних функцій міжмережного екрану Cisco ASA є розбиття локальних мереж на зони та рівні безпеки, за допомогою яких можна виділити основні локальні мережі, яким потрібен найвищий захист та локальні мережі з меншим захистом. За замовчуванням локальна мережа з найвищим рівнем безпеки може звертатися до всіх інших локальних мереж, а мережа з меншим рівнем безпеки не може мати доступ до локальної мережі з вищим.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Після вивчення та аналізу особливостей побудови підсистеми захисту корпоративної комп'ютерної мережі на базі рішень Cisco ASA було створено постановку технічного завдання для розуміння всіх поставлених задач на дану кваліфікаційну роботу.

У другому розділі було проведено проектування корпоративної комп'ютерної мережі, враховуючи всі теоретичні аспекти та особливості побудови, які були проаналізовані у першому розділі. Дане проектування було розділено на такі етапи:

- розробка загального проекту корпоративної мережі;
- розробка проекту фізичної та логічної топологій мережі;
- розробка політик підсистеми захисту міжзональної взаємодії корпоративної мережі;
- аналіз та розробка структури Windows-мережі.

На даних етапах загалом було розроблено повний план побудови корпоративної комп'ютерної мережі та підсистеми захисту на базі рішень Cisco ASA та забезпечення взаємодії центральної мережі з мережами філій за допомогою зв'язку VPN.

При розробці політик підсистеми захисту міжзональної взаємодії потрібно було враховувати особливості розташування основних серверів в зонах безпеки для безпечного доступу робочих станцій та інших серверів до них. Загалом політики міжзонального обміну були розроблені за допомогою розширених списків ACL. Під час написання даних списків потрібно передбачити те, що, наприклад, при дозволі проходження трафіку локальної мережі А до іншої мережі Б, весь інший трафік, який буде проходити з локальної мережі А взагалі до інших мереж буде автоматично заборонено, тому потрібно було уважно застосовувати дані списки ACL та по можливості застосовувати їх на вихідний трафік на інтерфейс локальної мережі, до якої потрібен доступ за правилами проходження трафіку.

При проектуванні було ще й враховано функціонування Windows-мережі, так як вона забезпечує додатковий захист та контроль над роботою

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

всіх робочих станцій та серверів, які під'єднані до даної мережі, що є невід'ємною частиною в роботі всієї корпоративної комп'ютерної мережі.

У третьому розділі, проаналізувавши проектування та розробку корпоративної комп'ютерної мережі та підсистеми захисту на базі рішень Cisco ASA з другого розділу, було налагоджено мережеві пристрої та сервери.

Налагодження корпоративної комп'ютерної мережі проводилося в програмному симуляторі GNS3, де всі сценарії налагодження можна легко застосовувати й на реальному обладнанні.

Перед самим налагодженням потрібно було обрати обладнання, яке б найкраще підходило для підтримки функціонування корпоративної комп'ютерної мережі. Було проведено порівняння міжмережних екранів Cisco ASA, після чого стало зрозуміло, яку модель краще використовувати. Під час вибору мережевого обладнання потрібно враховувати можливість масштабованості мережі, характеристику самого обладнання, щоб воно не було занадто потужним (економія ресурсів організації) та занадто слабким для підтримки функціонування мережі організації.

Після вибору обладнання було проведено налагодження корпоративної комп'ютерної мережі. Під час даного процесу було важливим поділити його на налагодження основних функцій корпоративної комп'ютерної мережі та додаткових для кращого розуміння пріоритету налагодження й розуміння основної суті роботи корпоративної мережі для кращого її обслуговування, тощо.

Налагодження в основному було проведено на міжмережних екранах Cisco ASA, так як насамперед метою кваліфікаційної роботи є підсистема захисту на базі рішень Cisco ASA. Однак, було проведено ще й налагодження структури Windows-мережі, так як потрібно показати особливості проходження трафіку на міжмережних екранах Cisco ASA при розроблених політиках міжзональної взаємодії.

Після всього налагодження корпоративної комп'ютерної мережі було проведено її тестування на наявність помилок в налаштуванні та коректність виконання всіх поставлених задач на дану кваліфікаційну роботу.

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Andrew Osipov. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services 3rd Edition. Cisco Press, 2014 – 1248 с.
2. Don R. Crawley. Cisco ASA for Accidental Administrators: An Illustrated Step-by-Step ASA Learning and Configuration Guide. Crawley International, Inc, 2015 – 258 с.
3. Базовая настройка NAT на ASA: Веб-сервер в DMZ в ASA. [Электронный ресурс]. Режим доступа:
https://www.cisco.com/c/ru_ru/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-DMZ-00.html
4. Інструкція конфігурації Cisco ASA. [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/ru_ru/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
5. Конфигурация Twice NAT на ASA 9.x. [Электронный ресурс]. Режим доступа: <http://www.ccienetlab.com/security/17-konfiguraciya-twice-nat-na-asa-9x.html>
6. Корпоративні мережі. [Електронний ресурс]. Режим доступу: <https://newtravelers.ru/uk/poleznoe/korporativnye-seti-klassifikaciya-korporativnyh-setei-yavlyaetsya-li-korporativnaya-set-lokalnoi.html>
7. Маршрутизаторы [Электронный ресурс]. Режим доступа: https://www.cisco.com/c/ru_ru/products/routers/index.html
8. Навчальний курс CCNA Security 2.0 [Електронний ресурс] – Режим доступу: www.netacad.com.
9. Структура корпоративной сети. [Электронный ресурс] – Режим доступа: <https://wiki.merionet.ru/seti/61/struktura-korporativnoj-seti/>
10. Четыре лучших практики по настройке DMZ. [Электронный ресурс] – Режим доступа: <https://networkguru.ru/nastroika-dmz-demilitarizovannaya-zona/>

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

11. Що таке NAT? Для чого використовую даний стандарт? [Електронний ресурс] – Режим доступу: <https://hyperhost.ua/info/uk/shcho-take-nat-dlya-chogo-vikoristovuyu-daniy-standart>
12. Introduction to Deep Packet Inspection (DPI). [Електронний ресурс]. Режим доступу: <https://www.routexp.com/2018/09/introduction-to-deep-packet-inspection.html>
13. Cisco ASA Site-to-Site IKEv1 IPsec VPN. [Електронний ресурс]. Режим доступу: <https://networklessons.com/cisco/asa-firewall/cisco-asa-site-site-ikev1-ipsec-vpn>
14. Cisco ASA Site-to-Site IKEv1 IPsec VPN Dynamic Peer. [Електронний ресурс]. Режим доступу: <https://networklessons.com/cisco/asa-firewall/cisco-asa-site-to-site-ipsec-ikev1-vpn-dynamic-peer>
15. Cisco ASA. [Електронний ресурс]. Режим доступу: http://xgu.ru/wiki/Cisco_ASA
16. Cisco ASA/NAT — Configuration. [Електронний ресурс]. Режим доступу: <https://linkas.ru/services/cisco-asa-static-nat/>
17. Cisco ASA Series General Operations CLI Configuration Guide, 9.5. [Електронний ресурс]. Режим доступу: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-general-config/interface-zones.html>
18. Cisco ASA Security Levels. [Електронний ресурс]. Режим доступу: <https://networklessons.com/cisco/asa-firewall/cisco-asa-security-levels>
19. Cisco ASA Series CLI Configuration Guide, 9.0. Chapter: Configuring OSPF. [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/route_ospf.html
20. IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY. [Електронний ресурс]. Режим доступу:

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html

21. VPN: ещё раз просто о сложном. [Электронный ресурс]. Режим доступа: <https://habr.com/ru/post/534250/>

22. VPN Topologies Guide. [Электронный ресурс]. Режим доступа: <http://www.internet-computer-security.com/VPN-Guide/VPN-Topologies.html>

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

ДОДАТКИ

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Основний сегмент топології корпоративної комп'ютерної мережі

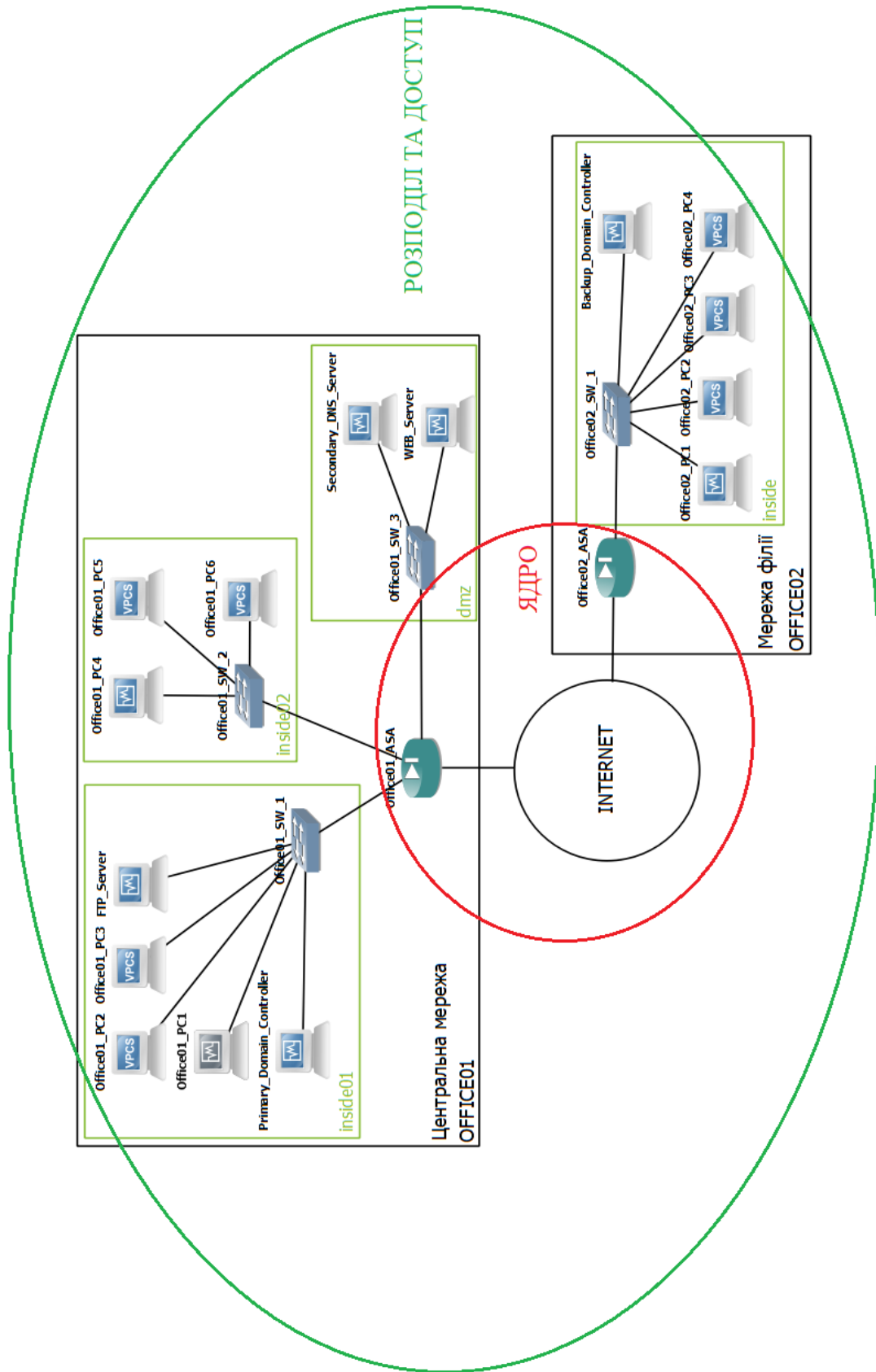


Рисунок А.1 – Частина загальної топології корпоративної комп'ютерної мережі

		Чевкота А.С.		
		Російський Ю.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

Схеми підключень та таблиці IP-адресації пристроїв мережі

Таблиця Б.1

Підключення пристроїв мережі OFFICE01

Пристрій	Інтерфейс	Підключення до пристрою/Мережі	Підключення до інтерфейсу
Міжмережний екран Office01_ASA	Gig0/0	Комутатор Office01_SW_1	Gig0/1
	Gig0/1	Комутатор Office01_SW_2	Gig0/1
	Gig0/2	Комутатор Office01_SW_3	Gig0/1
	Gig0/3	Internet	Gig
Комутатор Office01_SW_1	Gig0/1	Міжмережний екран Office01_ASA	Gig0/0
	Gig0/2	Сервер FTP_Server	Gig0
	Gig0/1	Сервер Primary_Domain_Controller	Fa0
	Gig0/2	Робоча станція Office01_PC1	Fa0
	... Gig0/4	... Робоча станція Office01_PC3	... Fa0
Комутатор Office01_SW_2	Gig0/1	Міжмережний екран Office01_ASA	Gig0/1
	Gig0/1	Робоча станція Office01_PC4	Fa0
	... Gig0/3	... Робоча станція Office01_PC6	... Fa0
Комутатор Office01_SW_3	Gig0/1	Міжмережний екран Office01_ASA	Gig0/2
	Gig0/2	Сервер Secondary_DNS_Server	Gig0
	Gig0/3	Сервер WEB_Server	Gig0

Схема адресації пристроїв мережі OFFICE01

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Підмережа inside01	-	192.168.1.0	255.255.255.0	/24
Підмережа inside02	-	192.168.2.0	255.255.255.0	/24
Підмережа DMZ	-	192.168.10.0	255.255.255.0	/24
Мережа outside	-	100.1.1.0	255.255.255.224	/27
Міжмережний екран Office01_ASA	Gig0/3	100.1.1.1	255.255.255.224	/27
	Gig0/0	192.168.1.1	255.255.255.0	/24
	Gig0/1	192.168.2.1	255.255.255.0	/24
	Gig0/2	192.168.10.1	255.255.255.0	/24
Сервер Primary_Domain_Controller	Fa0	192.168.1.254	255.255.255.0	/24
Сервер FTP_Server	Gig0	192.168.1.253	255.255.255.0	/24
Сервер Secondary_DNS_Server	Gig0	192.168.10.2 (static 100.1.1.3)	255.255.255.0	/24
Сервер WEB_Server	Gig0	192.168.10.3 (static 100.1.1.4)	255.255.255.0	/24
Робоча станція Office01_PC1	DHCP			
... Робоча станція Office01_PC6				

Порівняння мережевого обладнання від компанії Cisco

Таблиця В.1

Порівняння характеристик різних моделей Cisco ASA

Характеристика	Cisco ASA 5506-X	Cisco ASA 5525-X	Cisco ASA 5555-X
Пропускна здатність міжмережного екрану	300 Мбіт/с	1 Гбіт/с	2 Гбіт/с
Пропускна здатність з контролем стану підключень при використанні кількох протоколів	300 Мбіт/с	1 Гбіт/с	2 Гбіт/с
Пропускна здатність (AVC)	250 Мбіт/с	1100 Мбіт/с	1750 Мбіт/с
Пропускна здатність мереж VPN з 3DES/AES	100 Мбіт/с	300 Мбіт/с	700 Мбіт/с
Максимальна кількість нових підключень в секунду	5000	20000	50000
Максимальна кількість одночасних сеансів	20000 - 50000	500000	1000000
Кількість IPSec VPN-тунелів між вузлами	10 - 50	300	700
Кількість віртуальних інтерфейсів (VLAN)	5 - 30	200	500
Кількість користувачів вузлів	Не обмежено	Не обмежено	Не обмежено
Тип жорсткого диску	mSata	SSD	SSD
Пам'ять жорсткого диску	50 Гбайт	120 Гбайт	120 Гбайт
Кількість та тип портів	8 портів, 1 Гбіт/с	8 портів, 10/100/1000 Мбіт/с	8 портів, 10/100/1000 Мбіт/с

Продовження таблиці В.1

Максимальна кількість користувацьких сеансів з віддаленим VPN-підключенням Cisco AnyConnect IKEv1	5 - 30	200	500
Оперативна пам'ять	4 Гбайт	8 Гбайт	16 Гбайт
Флеш-пам'ять	8 Гбайт	8 Гбайт	8 Гбайт
Виділений порт керування	Так (спільне користування з сервісами FirePower), 10/100/1000 Мбіт/с	Так, 1 Гбіт/с	Так, 1 Гбіт/с

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Демонстрація основних етапів налаштування серверів Windows-мережі

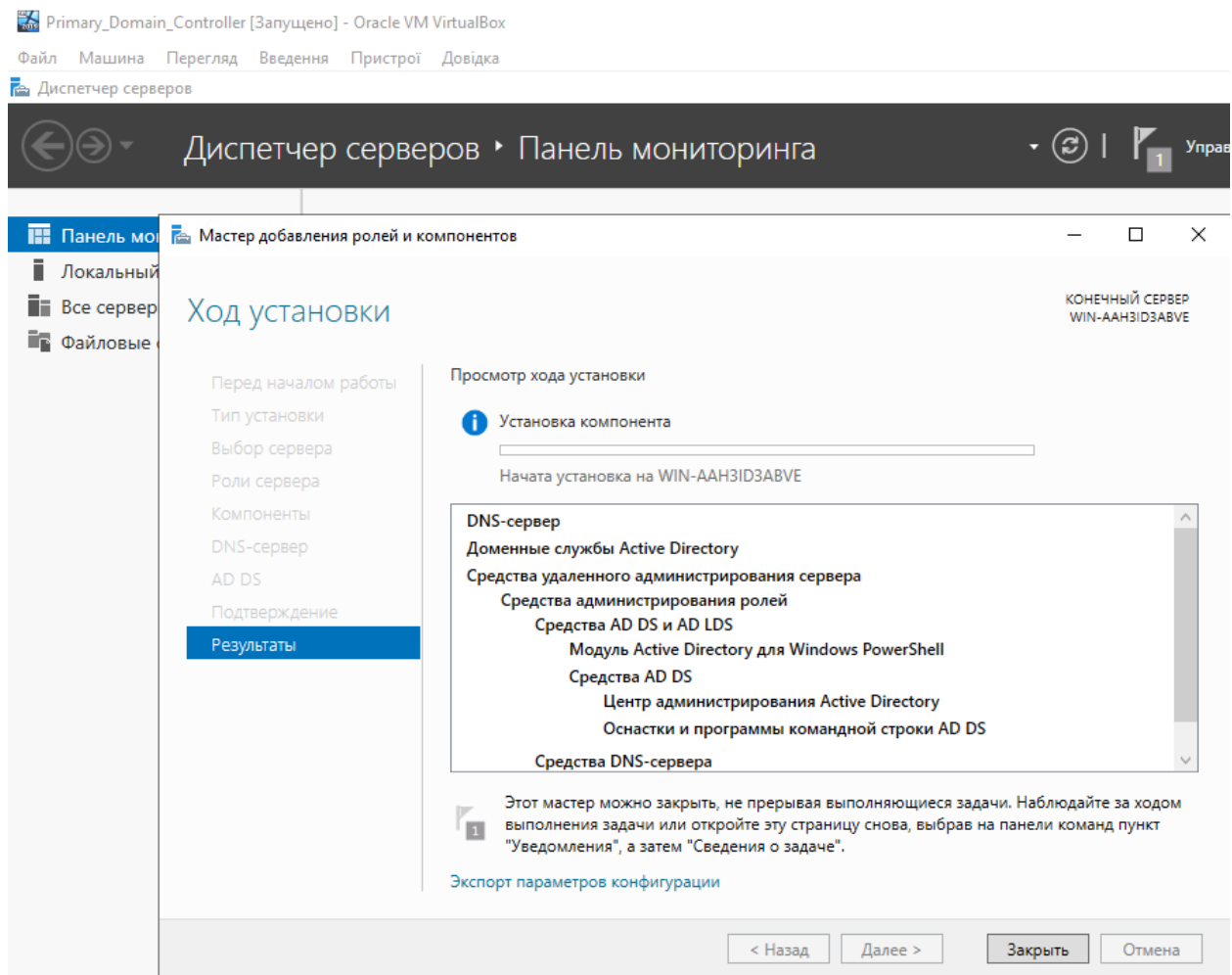


Рисунок Г.1 – Встановлення DNS-сервера та доменних служб Active Directory на сервері Primary_Domain_Controller центральної мережі OFFICE01

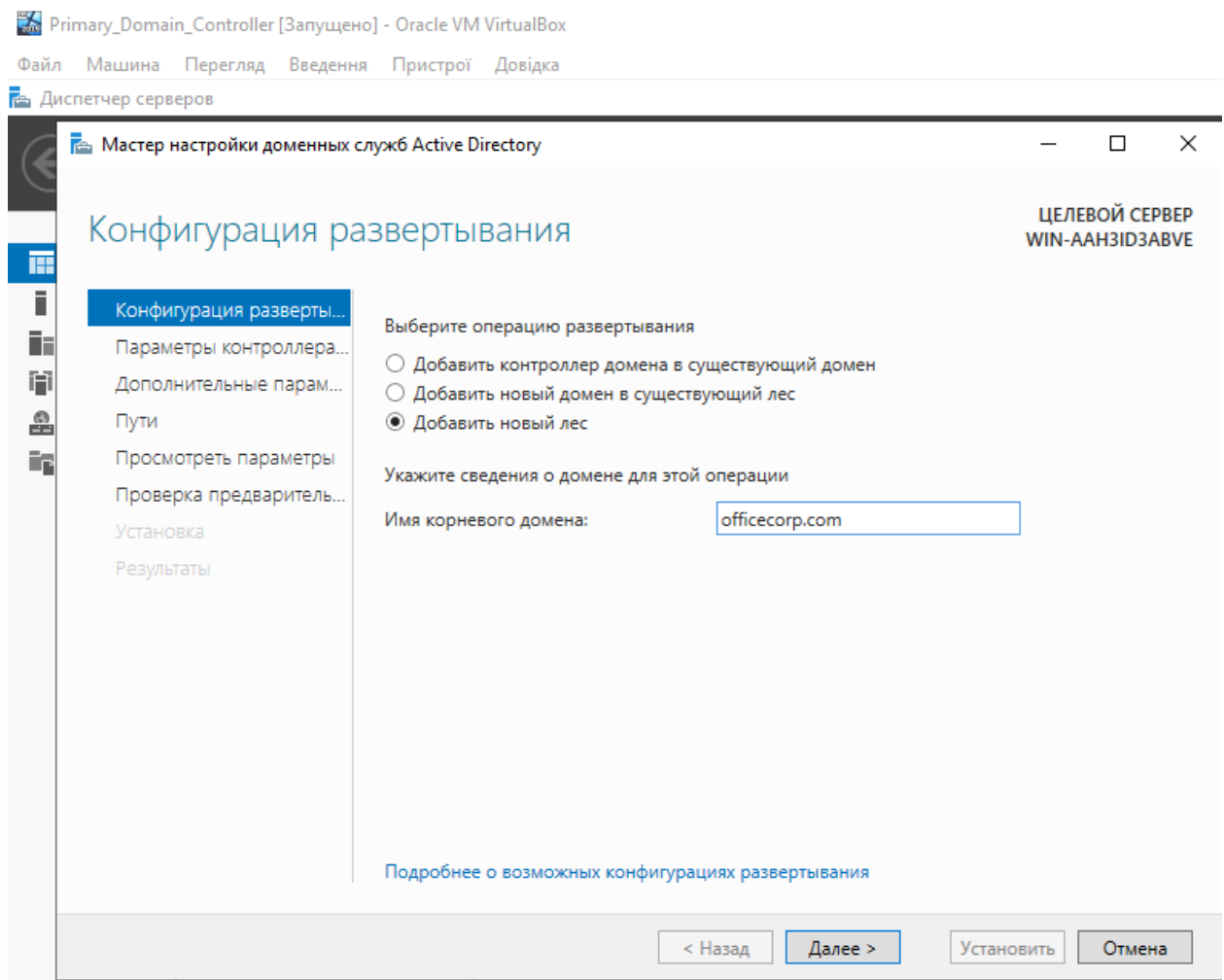


Рисунок Г.2 – Підвищення ролі сервера Primary_Domain_Controller до головного контролера домена officecorp.com

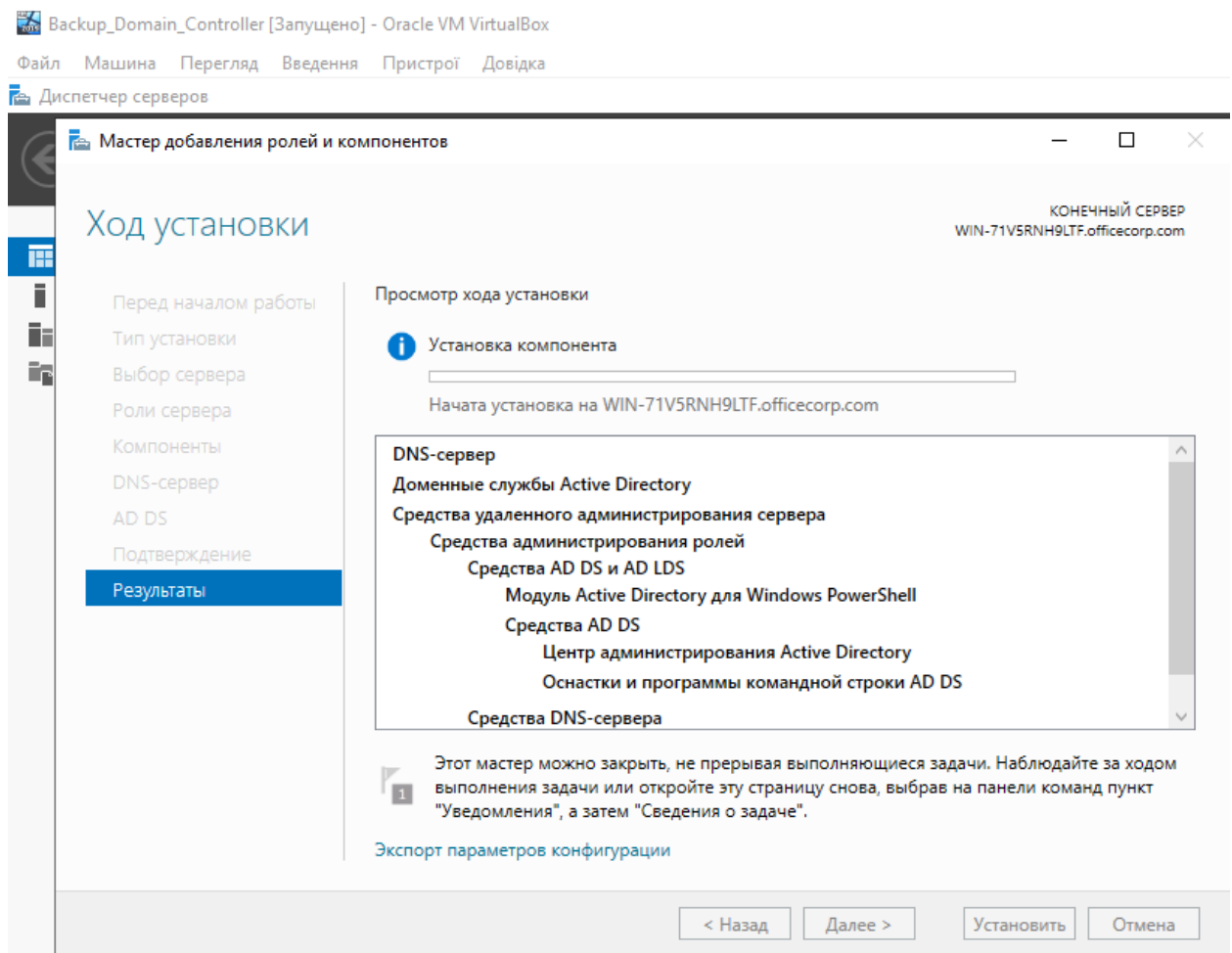


Рисунок Г.3 – Встановлення DNS-сервера та доменних служб Active Directory на сервері Backup_Domain_Controller мережі філії OFFICE02

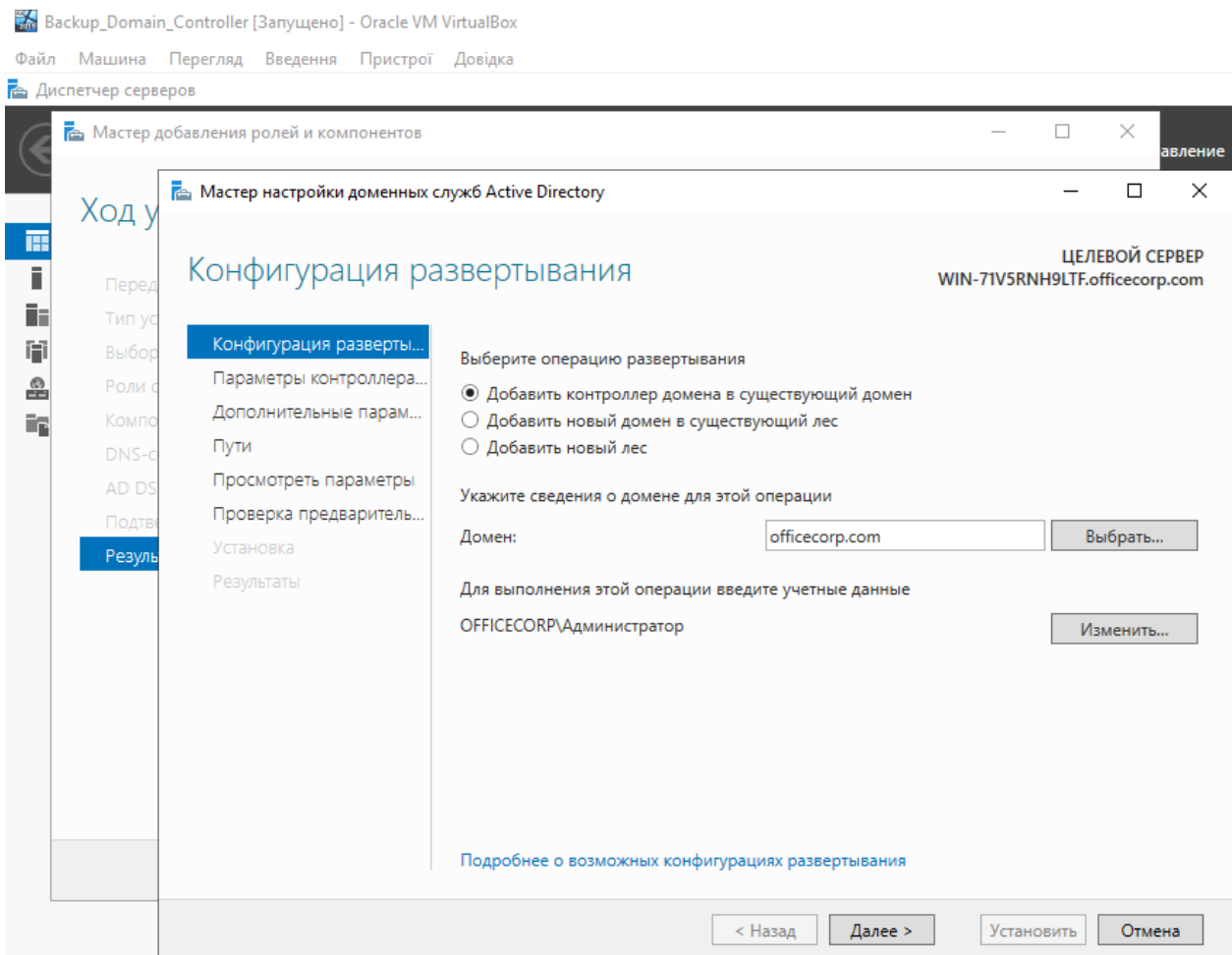


Рисунок Г.4 – Підвищення ролі сервера Backup_Domain_Controller до додаткового контролера домена officecorp.com

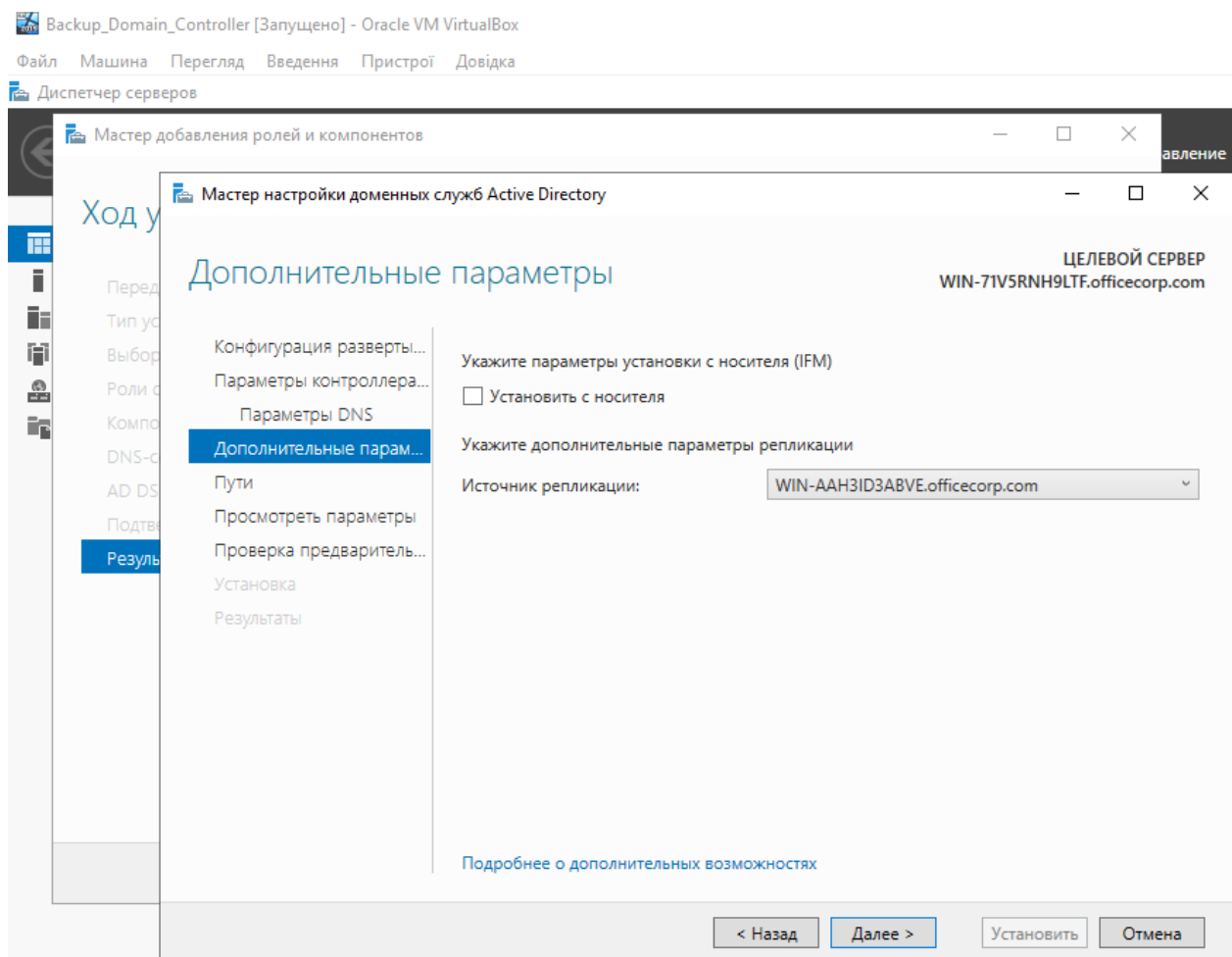


Рисунок Г.5 – Вказання джерела реплікації для додаткового контролера домена Backup_Domain_Controller

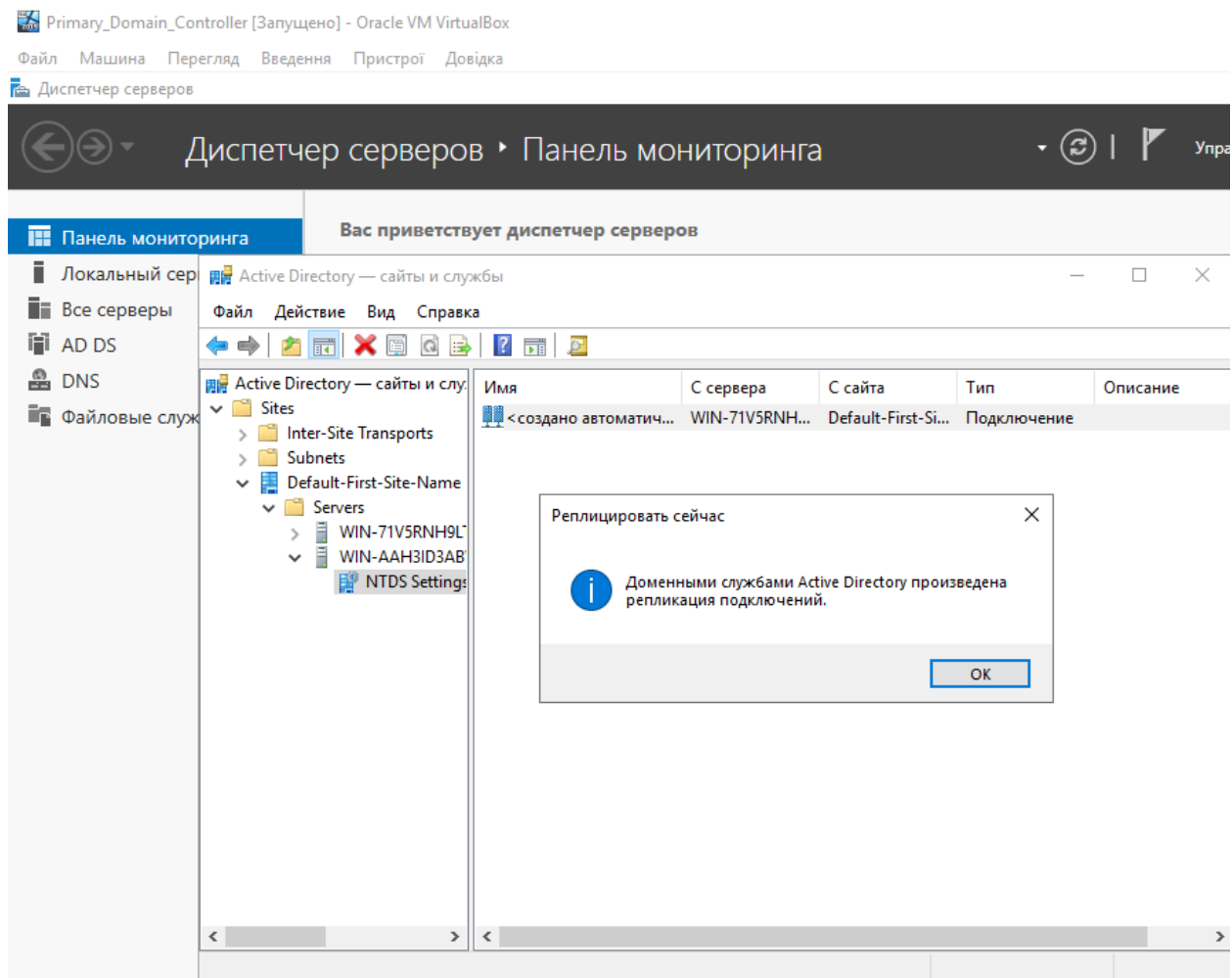


Рисунок Г.6 – Реплікація підключень з додаткового контролера домену Backup_Domain_Controller до головного контролера домену Primary_Domain_Controller

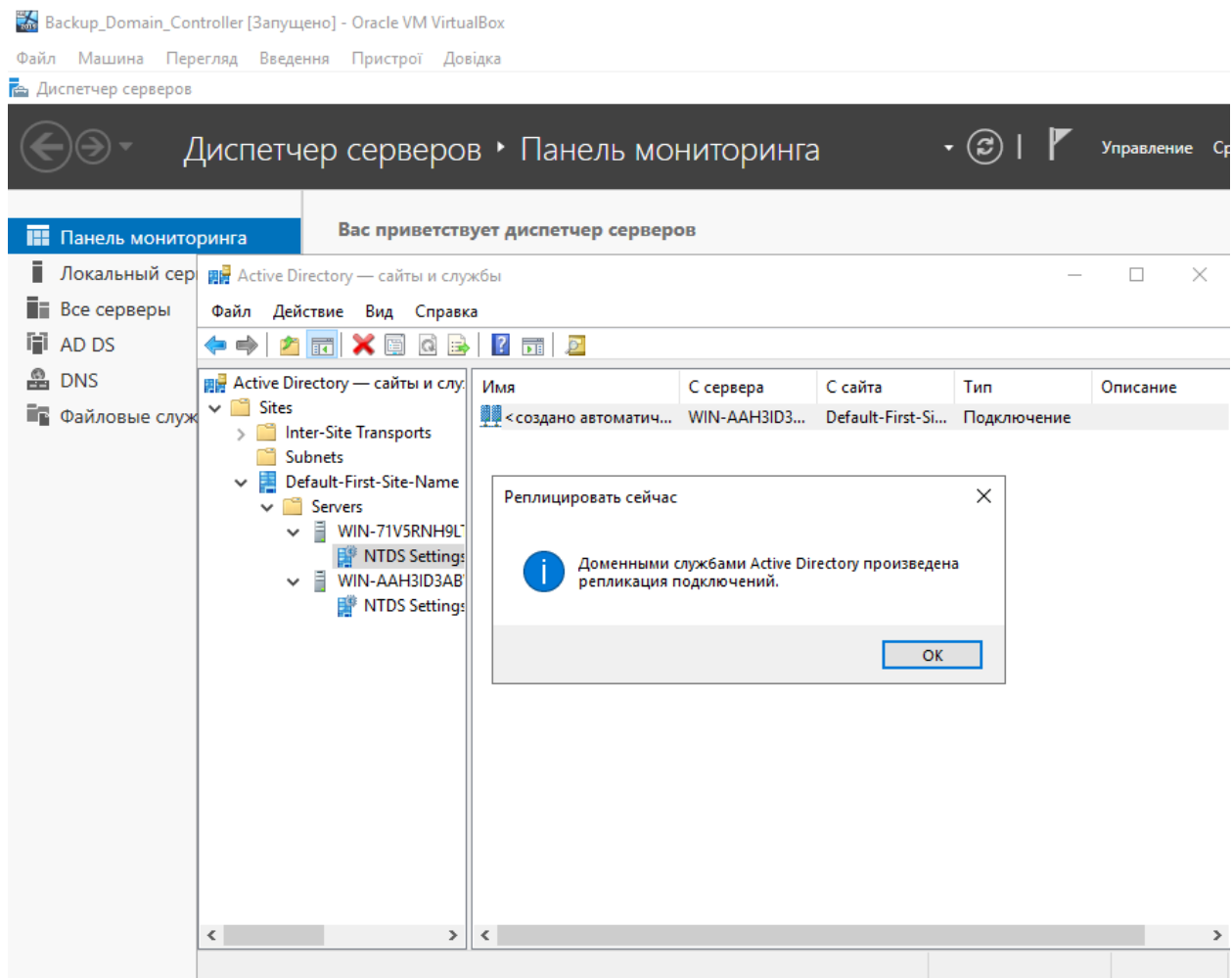


Рисунок Г.7 – Реплікація підключень з головного контролера домену Primary_Domain_Controller до додаткового контролера домену Backup_Domain_Controller

Вивід конфігураційних файлів міжмережних екранів Cisco ASA

Міжмережний екран Office01_ASA **Міжмережний екран Office02_ASA**

```

: Serial Number: 9AXJ2K9GA84
: Hardware:   ASAv, 2048 MB RAM, CPU
Pentium II 2807 MHz
:
ASA Version 9.8(1)
!
hostname Office01-ASA
enable password
$sha512$5000$P70uyb0XcrCHhnZKDANw==$Zx
L/XbMPbFHp4w/JRxsyhw== pbkdf2
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 inside01
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside02
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif dmz
 security-level 85
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/3
 nameif outside
 security-level 0
 ip address 100.1.1.1 255.255.255.224
 ospf message-digest-key 1 md5 *****
 ospf authentication message-digest
!
...
...
!
interface Management0/0
 shutdown

```

```

: Serial Number: 9A56KEGP5HG
: Hardware:   ASAv, 2048 MB RAM, CPU
Pentium II 2807 MHz
:
ASA Version 9.8(1)
!
hostname Office02-ASA
enable password
$sha512$5000$HWb8HTfr3R1rXrMsBYtPbw==$IR
1MaTz3rzyFELD+aspFNg== pbkdf2
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
 ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 100.6.1.1 255.255.255.224
 ospf message-digest-key 1 md5 *****
 ospf authentication message-digest
!
...
...
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network INSIDE-NET
 subnet 192.168.3.0 255.255.255.0
object network LAN1
 subnet 192.168.1.0 255.255.255.0

```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

```

no nameif
no security-level
no ip address
!
ftp mode passive
same-security-traffic permit inter-
interface
object network INSIDE01-NET
 subnet 192.168.1.0 255.255.255.0
object network INSIDE02-NET
 subnet 192.168.2.0 255.255.255.0
object network DMZ-NET
 subnet 192.168.10.0 255.255.255.0
object network DNS_SERVER-EXTERNAL-IP
 host 192.168.10.2
object network WEB_SERVER-EXTERNAL-IP
 host 192.168.10.3
object network LAN2
 subnet 192.168.3.0 255.255.255.0
access-list ALLOW_TRAFFIC_INSIDE
extended permit ip any host 192.168.10.2
access-list ALLOW_TRAFFIC_INSIDE
extended permit tcp any host
192.168.10.3 eq www
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any unreachable
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any time-
exceeded
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any source-
quench
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any echo-reply
access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONL
Y extended permit ip 192.168.2.0
255.255.255.0 host 192.168.1.253
access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONL
Y extended permit ip 192.168.2.0
255.255.255.0 host 192.168.1.254
access-list
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONL
Y extended permit ip host 192.168.10.2
host 192.168.1.254
access-list
ALLOW_DNS_SERVER_TRAFFIC_TO_PDC extended
permit ip host 192.168.10.2 host
192.168.1.254
access-list LAN1_LAN2 extended permit ip
192.168.1.0 255.255.255.0 192.168.3.0
255.255.255.0
pager lines 23
mtu inside01 1500
mtu inside02 1500
mtu dmz 1500
mtu outside 1500
no failover

access-list LAN2_LAN1 extended permit ip
192.168.3.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any echo-reply
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any source-
quench
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any unreachable
access-list ALLOW_TRAFFIC_INSIDE
extended permit icmp any any time-
exceeded
pager lines 23
mtu inside 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
arp rate-limit 8192
nat (inside,outside) source static
INSIDE-NET INSIDE-NET destination static
LAN1 LAN1
!
object network INSIDE-NET
 nat (inside,outside) dynamic interface
access-group ALLOW_TRAFFIC_INSIDE in
interface outside
router ospf 1
 network 100.6.1.0 255.255.255.224 area
0
 network 192.168.3.0 255.255.255.0 area
1
 log-adj-changes
!
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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact

```

		Чевката А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (inside01,outside) source static
INSIDE01-NET INSIDE01-NET destination
static LAN2 LAN2
!
object network INSIDE01-NET
  nat (inside01,outside) dynamic
interface
object network INSIDE02-NET
  nat (inside02,outside) dynamic
interface
object network DMZ-NET
  nat (dmz,outside) dynamic interface
object network DNS_SERVER-EXTERNAL-IP
  nat (dmz,outside) static 100.1.1.3
object network WEB_SERVER-EXTERNAL-IP
  nat (dmz,outside) static 100.1.1.4
access-group
ALLOW_TRAFFIC_TO_INSIDE01_TO_SERVERS_ONLY out interface inside01
access-group
ALLOW_DNS_SERVER_TRAFFIC_TO_PDC in
interface dmz
access-group ALLOW_TRAFFIC_INSIDE in
interface outside
router ospf 1
  network 100.1.1.0 255.255.255.224 area 0
  network 192.168.1.0 255.255.255.0 area 1
  network 192.168.2.0 255.255.255.0 area 1
  network 192.168.10.0 255.255.255.0 area 1
log-adj-changes
!
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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL

```

```

crypto ipsec ikev1 transform-set
TRANS_SET esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-
aging infinite
crypto map CRYP_MAP 10 match address
LAN2_LAN1
crypto map CRYP_MAP 10 set peer
100.1.1.1
crypto map CRYP_MAP 10 set ikev1
transform-set TRANS_SET
crypto map CRYP_MAP 10 set security-
association lifetime seconds 7200
crypto map CRYP_MAP interface outside
crypto ca trustpoint
_SmartCallHome_ServerCA
  no validation-usage
  crl configure
crypto ca trustpool policy
  auto-import
crypto ca certificate chain
_SmartCallHome_ServerCA
  certificate ca
18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018
dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081
ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967
6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374
204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269
5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520
6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320
5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574
686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336
30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506
0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656
65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331
28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175
74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269
5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274
69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609
2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35
9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8
31895d22 e82aaaa6 42b38ff8 b955b7b1

```

		Чевката А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set
TRANS_SET esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-
aging infinite
crypto map CRYPT_MAP 10 match address
LAN1_LAN2
crypto map CRYPT_MAP 10 set peer
100.6.1.1
crypto map CRYPT_MAP 10 set ikev1
transform-set TRANS_SET
crypto map CRYPT_MAP 10 set security-
association lifetime seconds 7200
crypto map CRYPT_MAP interface outside
crypto ca trustpoint
_SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain
_SmartCallHome_ServerCA
certificate ca
18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018
dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081
ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967
6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374
204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269
5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520
6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320
5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574
686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336
30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506
0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656
65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331
28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175
74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269
5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274
69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609
2a864886 f70d0101 01050003 82010f00

```

```

b74bb3fe 8f7e0757 ecef43db 66621561
cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233
49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf
1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c
eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe
ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0
6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381
b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04
04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516
09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d
8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572
69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f
d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105
05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a
584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc
defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
quit
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 7200
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.3.0 255.255.255.0 inside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 192.168.3.254
!
```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

3082010a 02820101 00af2408 08297a35
9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8
31895d22 e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561
cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9febf5 a191c233
49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf
1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c
eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe
ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd b7e4fc5 95ae0e9d d4d143c0
6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381
b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04
04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516
09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d
8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572
69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f
d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105
05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a
584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc
defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
quit
crypto isakmp identity address
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 7200
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside01
ssh timeout 5

```

```

dhcpd address 192.168.3.2-192.168.3.253
inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-
intercept
dynamic-access-policy-record
DfltAccessPolicy
username admin password
$sha512$5000$9D2e0ILc9aFK/7Qf6+Cso==$0a
8dTMqeSr9uQdeRhRZpFw== pbkdf2 privilege
15
tunnel-group 100.1.1.1 type ipsec-l2l
tunnel-group 100.1.1.1 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map traceroute
match any
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
no tcp-inspection
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
inspect icmp error
class traceroute
set connection decrement-ttl
policy-map type inspect dns
migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!

```

		Чевката А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Російський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 192.168.1.254
!
dhcpd address 192.168.1.2-192.168.1.200
inside01
dhcpd enable inside01
!
dhcpd address 192.168.2.2-192.168.2.254
inside02
dhcpd enable inside02
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-
intercept
dynamic-access-policy-record
DfltAccessPolicy
username admin password
$sha512$5000$I2Z6ykSpZYN90smHdwb/Kg==$zg
zpRJo+LEfutL6W1Xi88g== pbkdf2 privilege
15
tunnel-group 100.6.1.1 type ipsec-l2l
tunnel-group 100.6.1.1 ipsec-attributes
ikev1 pre-shared-key *****
!
class-map traceroute
match any
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
no tcp-inspection
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
inspect icmp error
class traceroute

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/services/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/services/DDCEService
destination transport-method http
Cryptochecksum:8f2466b3a2bde86d797245e8c07dcad4
: end

```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Россійський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

set connection decrement-ttl
policy-map type inspect dns
migrated_dns_map_2
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
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/services/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/services/DDCEService
  destination transport-method http
Cryptochecksum:3664868d04bf79768900b6ce9f94f64f
: end

```

		Чевкота А.С.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Росієський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86