Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Побудова локальних мереж з використанням обладнання Juniper Networks

(тема)

Виконав:

студент *2* курсу, групи *ІМІм-22-2*

Парінцев Д.О.
(прізвище, ініціали)

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва спеціальності)

Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва освітньої програми)

Керівник *доц. Омельченко А.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування.

Студент  / Парінцев Д.О. /
(підпис) (прізвище та ініціали)

Керівник  / Омельченко А.В. /
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)

Факультет *Інфокомунікацій*
Кафедра *Інформаційно-мережної інженерії*
Освітній рівень *другий (магістерський)*
Спеціальність *172 Телекомунікації та радіотехніка*
Тип програми *освітня*
Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІМІ
_____ *проф. Безрук В.М.*
"*18*" *03* 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту *Парінцеву Дмитру Олексійовичу*
(прізвище,ім`я,по батькові)

1. Тема роботи *Побудова локальних мереж з використанням обладнання Juniper Networks*

затверджена наказом університету від «*18*» *03* *2024 р. №232* Ст .

2. Термін подання студентом роботи до екзаменаційної комісії *10.06. 2024 р.*

3. Вихідні дані до роботи *Об'єкт дослідження – структури локальних мереж, побудованих з використанням обладнання Juniper Networks . Виконати аналіз особливостей побудови мереж на основі обладнання Juniper Проаналізувати методи побудови захищених інформаційних мереж. Розробити структуру захищеної мережі з використанням платформи EVE-NG*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Аналіз методів побудови мереж на основі обладнання Juniper
2. Аналіз методів побудови захищених інформаційних мереж
3. Побудова захищеної мережі з використанням платформи EVE-NG
Висновки

5. Перелік графічного матеріалу із зазначенням креслень, схем, плакатів, комп´ютерних ілюстрацій (включається до завдання за рішенням випускової кафедри)

Слайди презентації (назва, мета і актуальність кваліфікаційної роботи, технології Juniper для побудови захищениех мереж, протоколи Juniper, схема розробленої мережі,основні результати роботи, налаштування протоколу IPsec висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ*	*19.03.24*	*Виконано*
2	*Підбір літератури за темою роботи*	*20.03-27.03*	*Виконано*
3	*Виконання розділу 1*	*28.03-10.04*	*Виконано*
4	*Виконання розділу 2*	*11.04-20.04*	*Виконано*
5	*Виконання розділу 3*	*21.04-10.05*	*Виконано*
6	*Оформлення пояснювальної записки*	*11.05-29.05*	*Виконано*
7	*Оформлення презентаційного матеріалу, підготовка до захисту у ЕК*	*30.05-10.06.24*	*Виконано*

Дата видачі завдання *18.03.2024 р.*

Студент _____ *(Парінцев Д.О.)*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *(доц. Омельченко А.В.)*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка 66 с., 21 рис., 31 джерел, 2 додатків.

Об’єкт роботи – корпоративна мережа підприємства

Мета роботи – розробка безпечної та стійкої локальної мережі на основі пристроїв Juniper.

Проаналізовано методи побудови мереж на основі обладнання Juniper. Розглянуто різні конфігурації мережі, такі як шина та кільце, і вибрано кільцеву топологію як спосіб забезпечення надійних з’єднань, на які можна завжди покладатися.

Виконано аналіз методів побудови захищених інформаційних мереж. Проведено дослідження фільтрів брандмауера, які дозволяють регулювати та контролювати мережевий трафік відповідно до певних правил. Розглянуто функції протоколу IPsec VPN, який забезпечує безпечний зв’язок у віддалених мережах завдяки використанню шифрування та стандартів автентифікації.

Розроблено структуру мережі компанії XYZ Corporation. Топологія мережі розроблена у формі кільця. У ній для забезпечення відмовостійкості мережі передбачено використання протоколів LACP, BGP і RSTP. Для інформаційного захисту мережі використовкються протокол IPsec VPN і фільтри брандмауера. Використання DNS і DHCP сприяє підтримці мережі. Для імітації роботи роутерів і ПК Juniper використана віртуальна лабораторія EVE-NG.

ВІРТУАЛЬНА ЛАБОРАТОРІЯ, ІНФОРМАЦІЙНІ ЗАГРОЗИ, МЕРЕЖА, МАРШРУТИЗАТОРИ JUNIPER, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ТОПОЛОГІЯ.

ABSTRACT

Explanatory note 66 p., 21 fig., 31 sources, 2 attach.

The object of work is the enterprise's corporate network

The purpose of the work is the development of a secure and stable local network based on Juniper devices.

The methods of building networks based on Juniper equipment are analyzed. Different network configurations such as bus and ring were considered and the ring topology was chosen as a way to provide secure connections that can always be relied upon.

An analysis of the methods of building protected information networks was performed. Research has been conducted on firewall filters that allow you to regulate and control network traffic according to certain rules. The functions of the IPsec VPN protocol, which ensures secure communication in remote networks through the use of encryption and authentication standards, are considered.

The network structure of XYZ Corporation was developed. The topology of the network is developed in the form of a ring. It provides for the use of LACP, BGP, and RSTP protocols to ensure network fault tolerance. The IPsec VPN protocol and firewall filters are used for network information protection. Using DNS and DHCP helps maintain the network. The EVE-NG virtual laboratory was used to simulate the work of Juniper routers and PCs.

VIRTUAL LAB, INFORMATION THREATS, NETWORK, JUNIPER ROUTERS, SOFTWARE, TOPOLOGY.

ЗМІСТ

С

ПЕРЕЛІК СКОРОЧЕНЬ

ШПЗ	Шкідливе програмне забезпечення.
DDoS	Distributed Denial of Service.
Juniper	Juniper Advanced Threat Prevention
MPLS	Multiprotocol Label Switching
BGP	BGP Border Gateway Protocol
OSPF	Open Shortest Path First
VPLS	Virtual Private LAN Service
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
DEC	Digital Equipment Corporation
IEEE	Institute of Electrical and Electronics
VLAN	Virtual Local Area Network
LAG	Link Aggregation Group
LACP	Link Aggregation Control Protocol
AS	Autonomous system
DNS	Domain Name System
IP-адреса	Internet Protocol address
MAC	Media Access Control
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DHCP	Dynamic Host Configuration Protocol
IPsec VPN	IP Security Virtual Private Network
ESP	Encapsulating Security Payload
AH	Authentication Header
RADIUS	Remote Authentication Dial-In User Service
LDAP	Lightweight Directory Access Protocol
VPN	Virtual Private Network
NAC	Network Access Control

ВСТУП

Компанія Juniper є передовим виробником мережного обладнання для побудови захищених мереж. Побудування мережі на основі Juniper у поєднанні з правильною методикою побудови дозволяє надати надійний захист від кіберзагроз. Основні переваги побудови мережі на базі обладнання Juniper [1]:

1. Безпека: Juniper поєднав брандмауери, системи виявлення та запобігання вторгненням, шифрування даних та інші пристрої для запобігання різним кібератакам. Це гарантує, що дані в мережі залишаються конфіденційними, цілісними та доступними.

2. Відмовостійкість: Обладнання Juniper відоме своїм високим рівнем надійності, який зазвичай призводить до альтернативних мережевих шляхів, що забезпечує безперебійне функціонування мережі незалежно від того, чи виходить з ладу основне обладнання чи втрачається зв’язок, що ще більше обмежує шанси ініціювати передачу по мережі.

3. Масштабованість: Обладнання Juniper забезпечує гнучкість для масштабування мережі відповідно до потреб організації. Завдяки різноманітним модулям і конфігураціям ви зможете побудувати найкращу мережеву архітектуру, яка задовольнить потреби бізнесу.

4. Керованість: Juniper пропонує розширені можливості для роботи з мережевою інфраструктурою та спостереження за нею. Це дозволяє інженерам ефективно керувати мережею, знаходити й усувати можливі проблеми, а також аналізувати трафік для підвищення продуктивності мережі.

5. Сумісність: Стандартні протоколи та відкриті інтерфейси, які використовуються в обладнанні Juniper, не лише забезпечують гнучкість, необхідну для з’єднання з іншими мережевими системами, які у вас уже є, але й дозволяють скористатися сторонніми програмами, якщо вам потрібні додаткові функції.

Побудова надійної та захищеної мережі на основі обладнання Juniper потребує кількох способів забезпечення високої доступності та безпеки.

Надійність мережі буде підвищено за допомогою протоколів LACP, BGP і RSTP. Щоб захистити мережу, пропонується налаштувати конфігурації для IPsec VPN і фільтрів брандмауера. DNS і DHCP також будуть використовуватися для підтримки мережі. Така мережа матиме кільцеву архітектуру.

Застосування спеціальних механізмів та протоколів дозволяє захистити мережу та всі пристрої від фішингу, грубої сили, спаму, встановлення шкідливого програмного забезпечення та стягнення персональних даних.

У даній роботі проаналізовано процес налаштування безпечної мережі за допомогою засобів Juniper. Розглянуто різні конфігурації мережі, такі як початок, шина та кільце, і вибрано кільцеву топологію як спосіб забезпечення безпечних з'єднань, на які можна завжди покладатися. З використанням платформи EVE-NG побудовано захищену інформаційну мережу та здійснено процес її налаштування.

У практичній частині роботи буде розроблено мережу компанії XYZ Corporation, яка є середньою за розмірами IT-компанією, що займається розробкою програмного забезпечення та наданням IT-консалтингових послуг. Основні вимоги компанії до мережевої інфраструктури включають високу безпеку, надійність та масштабованість. Мережа для XYZ Corporation буде розроблена з урахуванням високих вимог до безпеки, відмовостійкості та підтримки мережевих служб. Використання сучасного мережевого обладнання Juniper та протоколів LACP, BGP, RSTP, IPsec VPN і фільтрів брандмауера забезпечить надійну та безпечну роботу мережі, що відповідає потребам компанії

1 АНАЛІЗ МЕТОДІВ ПОБУДОВИ МЕРЕЖ НА ОСНОВІ ОБЛАДНАННЯ JUNIPER

1.1 Маршрутизатори Juniper

Компанія Juniper має надійне обладнання, яке добре зарекомендувало себе на світовому ринку. Розглянемо лише один вид їх обладнання - маршрутизатори Juniper. Роутерами від Juniper користуються такі гіганти [1], як: Verizon; British Telecom; Alibaba Cloud; Amazon Web Services; Microsoft Azure; Apple; Google; Facebook; Twitter; LinkedIn; Spotify; Netflix; Electronic Arts (EA).

Ці компанії надають перевагу Juniper з огляду на широкий спектр переваг, які пропонують їх маршрутизатори [2]:

1. Висока продуктивність. Маршрутизатори Juniper характеризуються високою продуктивністю, що дозволяє обробляти величезні обсяги трафіку та підтримувати численні служби одночасно без будь-якого зниження ефективності.
2. Безпека. Маршрутизатори Juniper захищають мережі від таких загроз безпеці, як DDoS-атаки, зловмисне програмне забезпечення та віруси, використовуючи надійні вбудовані заходи безпеки. Рішення Juniper, такі як ATP і Connected Security, можна покластися на ефективний захист даних.
3. Масштабованість. Можливість масштабування зробила маршрутизатори Juniper дуже корисними для великих мереж, отже, найбільш бажаними. Вони мають велику кількість інтерфейсів, які можна легко змінити відповідно до мінливих потреб мережевого трафіку.
4. Гнучкість. Маршрутизатори Juniper підтримують широкий спектр мережевих технологій, включаючи MPLS, BGP, OSPF і VPLS, що робить їх універсальним вибором для різноманітних мережевих середовищ, від корпоративних мереж до постачальників послуг і центрів обробки даних.

5. Управління. Інтерфейс для управління Junos Space в Інтернеті зрозумілий і спрощує конфігурацію та керування мережею, роблячи їх простішими. Це, в свою чергу, робить його більш ефективним і менш складним.

Топології, в яких можна використовувати маршрутизатори Juniper [3]:

1. Топологія точка-точка застосовується, коли є необхідність встановлення прямих з'єднань «точка-точка», наприклад, між двома будівлями, маршрутизатори Juniper дуже допомагають.

2. Зірка. У топології "зірка" кожен мережевий пристрій підключений до центрального концентратора, що зазвичай використовується в малих і середніх мережах.

3. Змішана топологія. Змішана топологія — це різновид конфігурації мережі, за якої кожен пристрій підключається до будь-якого іншого пристрою в системі. Така топологія може підтримуватися маршрутизаторами Juniper.

4. Кільце. Кільцевій топологія передбачає що кожен пристрій з'єднується з двома іншими, щоб утворити кільце, яке часто використовується в волоконно-оптичних мережах.

5. Гібридна топологія. Маршрутизатори Juniper підходять для гібридних топологій, що змішують кілька різних топологій, як-от комірчасту і зіркоподібний.

Топологія шини з економічної точки зору потребує менше кабелів порівняно з іншими топологіями. Пристрої легко додати до мережі шини цього пристрою, підключивши їх лише до основної шини, а не змінюючи чи модифікуючи всю інфраструктуру. Топологія шини має можливість запропонувати більшу пропускну здатність передачі даних, коли використовуються високошвидкісні шини разом із передавачами з високою пропускною здатністю.

Мінуси топології "Шина":

1. У топології шини лише один пристрій може надсилати дані одночасно. Через це мережі з великою кількістю пристроїв працюють повільно.

2. Надійність. Коли основна шина не працює належним чином або вийшла з ладу; це означає, що мережа також перестане працювати. Інша причина полягає в тому, що ця форма топології вважається менш надійною, ніж інші, через її схильність до збоїв.

3. Складність у виявленні проблем. Якщо виникають проблеми з передачею даних, локалізація і виявлення несправностей може бути складною, оскільки всі пристрої підключені до однієї шини.

Топологія "Шина" може бути використана в наступних ситуаціях:

1. Малий масштаб: Невеликі мережі з обмеженою кількістю пристроїв і достатньою пропускною здатністю для задоволення потреб мережі ідеально підходять для топології «шина».

Прості застосування: Якщо системі не потрібні складні мережеві структури чи багато пристроїв, а лише базовий обмін даними між тими, хто знаходиться на одній смузі, то топологія шини може бути більш зручною, отже, практичною та економічною для використання. З метою навчання та оцінки часто використовується шинна топологія. Цю мережу легко втілити в життя, щоб учні могли отримати певне уявлення про те, як вона виглядає на найнижчому рівні демонстрації принципів мережі, оскільки вона досить проста порівняно з іншими.

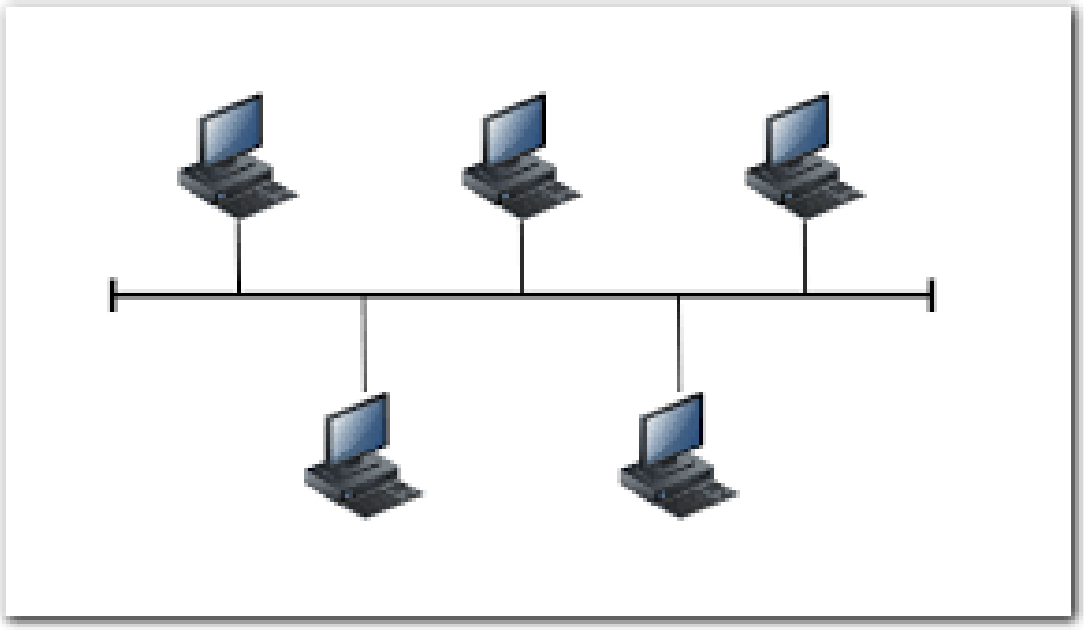


Рисунок 1.1 - Приклад топології «Шина»

Топологія «Зірка» є популярною конфігурацією для створення комп'ютерних мереж. У цьому налаштуванні кожен пристрій підключено окремо до центрального комутатора або концентратора.

Переваги топології "Зірка" [6]:

1. Висока надійність: Центральний комутатор підключає кожен пристрій окремо, так що якщо один пристрій виходить з ладу, це не вплине на всю мережу.
2. Простота управління: Що стосується керування мережею, все досить просто. Це тому, що кожен окремий пристрій підключено до основного комутатора, таким чином дозволяючи додавати, видаляти або навіть переміщувати будь-який пристрій.
3. Зручність діагностики проблем: Коли ви підключаєте пристрої один за одним до центрального комутатора, проблема розпізнавання мереж набагато легша, ніж раніше, і будь-яке несправне джерело можна легко розпізнати.

Недоліки топології "Зірка":

1. Залежність від центрального комутатора: Уся мережа може перестати функціонувати, якщо центральний концентратор або головний комутатор вийдуть з ладу. Ця установка може мати збої в центральних вузлах.

2. Збільшені витрати на кабелі: Витрати на кабель зростають через те, що кожен окремий пристрій має пряме з’єднання з головним вимикачем, що потребує більше кабелів. Загальна вартість кабельної системи може зрости.

Сфери застосування топології "Зірка":

1. Офісні мережі: Мережі в офісі зазвичай встановлюються таким чином, оскільки вони дуже надійні та прості в обслуговуванні. Будь-який комп’ютер або гаджет можна легко під’єднати до центрального комутатора.

2. Мережі з інтенсивним потоком даних: Коли є величезний потік інформації, ці мережі стають у нагоді. Це правда, що існують мережі, які вимагають високої швидкості обміну даними, тому використання «зірки» є великою перевагою.

3. Надійні мережі: З огляду на надійність, топологія "Зірка" є надійною мережею. Це пояснюється тим, що його структура дає змогу запобігти враженню всієї мережі проблемою з одним пристроєм через ізольовані з’єднання.

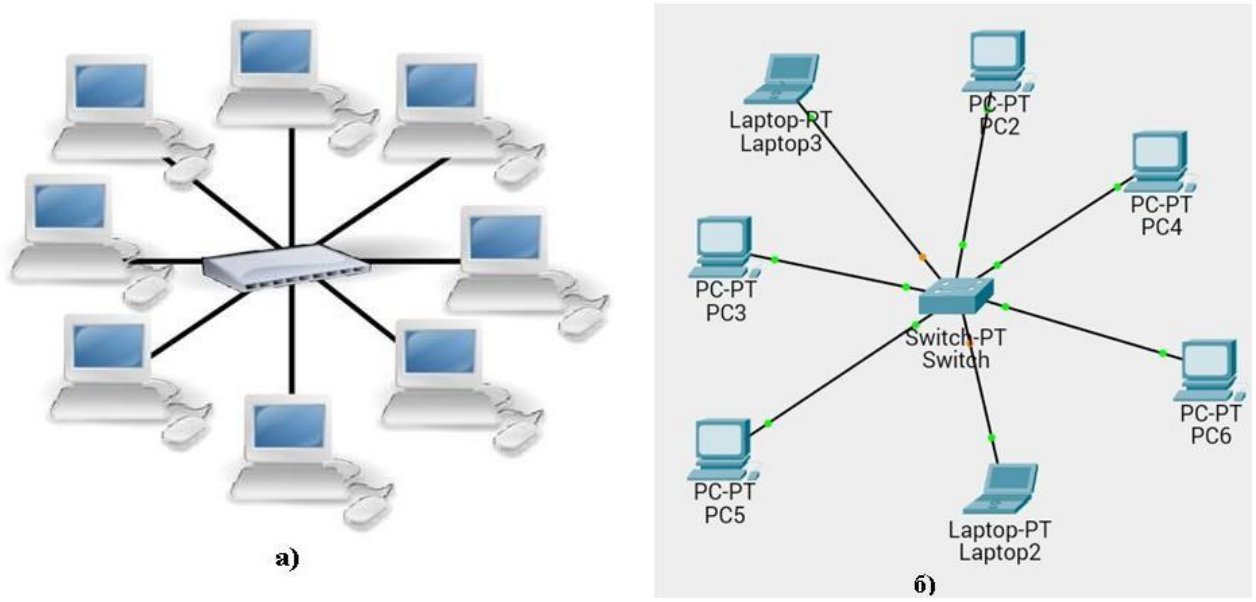


Рисунок 1.2 - Топологія «Зірка» (а) та топологія «Зірка» у віртуальному середовищі Cisco Packet Tracer (б)

Отже, варто зазначити, що конфігурація «Зірка» залишається одним із найпопулярніших варіантів під час налаштування різних мереж завдяки своїй надійності, простоті в управлінні та усуненні несправностей . Зокрема, цей дизайн в основному використовується для офісних мереж або інших місць, де потрібна висока продуктивність і надійність мережі.

Топологія "Кільце" є однією з основних конфігурацій для комп'ютерних мереж. У цій топології кожен пристрій підключений до двох сусідніх, утворюючи замкнене кільце.

Переваги топології «Кільце» [7]:

1. Висока пропускна здатність: Швидкість передачі даних збільшується, оскільки кільцева структура замкнута. Це означає, що кожен пристрій може передавати великий обсяг інформації, не зупиняючи інші пристрої.

2. Простота налаштування: Встановлення цього обладнання не становить великої праці, оскільки кожен пристрій підключається до двох інших пристроїв.

3. Ефективне управління: Управління інформаційним потоком плюс визначення користувачів мережевих ресурсів може здійснюватися з однієї точки

в такій топології.

Недоліки топології "Кільце":

1. Вразливість до збоїв: Щоразу, коли пристрій у кільцевій топології виходить з ладу або від’єднується, це може призвести до збоїв у всій мережі, призводячи до зупинки роботи. Крім того, відновлення втраченого з’єднання може виявитися складним.

2. Затримки у передачі даних: Затримки передачі даних у кільцевій топології залежать від рухомого маркера для керування в мережі. Щоразу, коли кількість підключених пристроїв збільшується, багато чого може призвести до затримок.

3. Складність розширення: Додавання нових пристроїв до кільцевої топології може бути складним через налаштування з'єднань з двома сусідніми пристроями.

Сфери застосування топології "Кільце":

1. Мережі з високими вимогами до пропускної здатності: Топологія "Кільце" підходить для мереж, де потрібна висока швидкість передачі даних, як-от відео або великі обсяги даних.

2. Критично важливі мережі: Для забезпечення надійності топологія "Кільце" може бути використана з резервними шляхами. Якщо один шлях виходить з ладу, дані можуть бути перенаправлені через альтернативний маршрут.

3. Гібридні мережі: Топологія "Кільце" може бути частиною гібридних мереж, поєднуючи різні топології для досягнення певних цілей.

Отже, конфігурація «Кільце» підходить для мереж, які вимагають високої пропускної здатності даних, а також надійності, а також застосовна в гібридних мережах, які можуть потребувати різних конфігурацій для різних цілей.

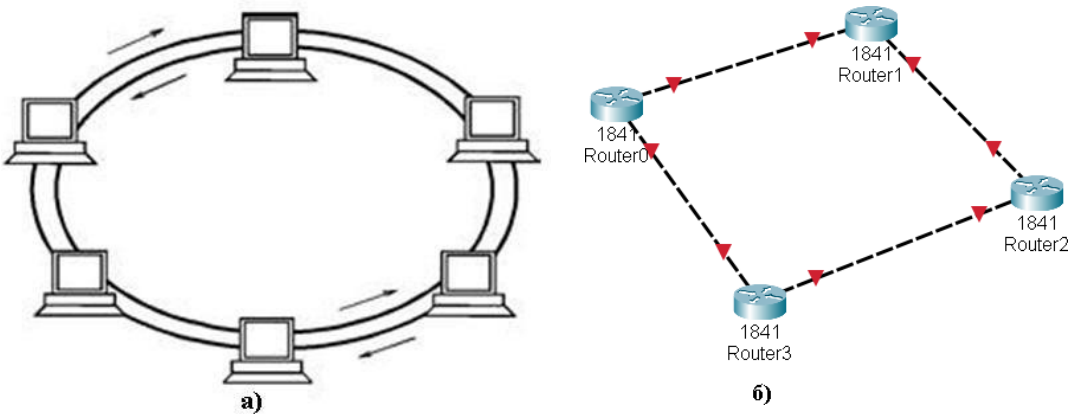


Рисунок 1.3 - Приклад топології «Кільце» (а) та топологія «Зірка» у середовищі Cisco Packet Tracer (б)

1.3 Вибір протокола кільцювання

Протокол STP і RSTP служать для запобігання виникненню петель і управління структурою кільцевих мереж, тим самим підвищуючи стабільність і надійність мережевих з'єднань. Нижче наведено більш детальний огляд цих протоколів, їх відмінності та переваги».

У 1985 році DEC винайшов протокол Spanning Tree Protocol (STP), який пізніше був прийнятий як IEEE 802.1D. Алгоритм, який використовується STP, дозволяє виявляти та видаляти надлишкові зв’язки в зациклених мережах. Ця техніка допомагає збалансувати мережевий трафік, але призводить до повільного формування деревоподібної структури, сповільненої реакції на зміни в мережі.

RSTP (протокол Rapid Spanning Tree Protocol), також відомий як IEEE 802.1w, насправді є вдосконаленою версією STP, яка була винайдена для зменшення кількості збоїв у мережі. Що робить RSTP кращим за STP, так це те, що системі потрібно дуже короткий час, щоб повернутися до нормальної роботи відразу після поломки, що гарантує, що високонадійні мережі залишаються функціональними весь час [9].

Основні елементи RSTP:

1. Bridge ID: Ідентифікатор моста, що використовується для визначення

кореневого моста в мережі.

2. Port ID: Ідентифікатор порта, який визначає, який порт буде використовуватися для передачі даних.

3. Cost: Вартість передачі даних через порт.

4. State: Стан порту, що вказує, чи може порт передавати дані в мережі.

Переваги RSTP над STP:

1. Швидкість: RSTP може відновити мережу в рази швидше, ніж STP.

2. Ефективність: RSTP використовує менше ресурсів мережі, що підвищує її ефективність.

3. Масштабованість: RSTP дозволяє легше масштабувати мережу, додаючи нові пристрої.

4. Надійність: RSTP забезпечує високу надійність мережі, запобігаючи утворенню петель.

5. Підтримка VLAN: RSTP може працювати з віртуальними локальними мережами, що підвищує гнучкість мережі.

6. Підтримка різних типів портів: RSTP підтримує різні типи портів, що дозволяє більш гнучке налаштування мережі.

7. Виключення портів: Можливість виключення портів з мережі при необхідності для зменшення трафіку.

8. Захист мережі: RSTP забезпечує захист від шкідливих атак та зловмисних дій.

Налаштування RSTP на пристроях Juniper:

1. Вмикання RSTP: Активуйте RSTP на кожному мережевому пристрої Juniper і налаштуйте параметри протоколу, такі як пріоритет кореневого моста та час переходу.

2. Налаштування портів: Конфігуруйте параметри протоколу на кожному порту, вказуючи тип порту (наприклад, access або trunk) та стан порту.

3. Перевірка налаштувань: Після налаштування перевірте правильність конфігурації за допомогою команд перевірки стану мережі, таких як `show spanning-tree`.

4. Відлагодження: Якщо виникають проблеми, діагностуйте і вирішуйте їх за допомогою діагностичних повідомлень від пристроїв.

5. Документація налаштувань: Після завершення налаштування створіть документацію, щоб мати можливість швидко відновити мережу в разі збоїв або відновлення.

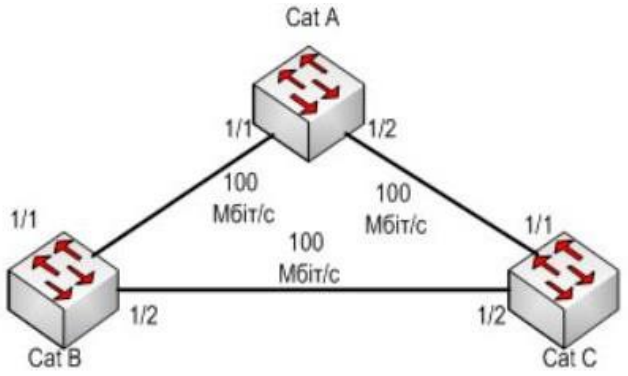


Рисунок 1.4 - Приклад використання RSTP

У порівнянні зі старішою версією STP нижчої якості, RSTP революціонізував мережеве керування, оскільки він швидший і ефективніший, тому ідеально підходить для сучасних мереж, які є дуже надійними та працюють добре[8].

На рис. 1.5 показано, як протокол RSTP забезпечує надійність і безперервність мережевих з'єднань у разі відмови одного з комутаторів. На малюнку наведені три комутатори: CatA, CatB і CatC. З'єднання між ними виглядають наступним чином:

- Інтерфейси 1/2-1/2 між CatB та CatC знаходяться в режимі DOWN.
- Інтерфейси 1/1-1/1 між CatB та CatA знаходяться в режимі FRW.
- Інтерфейси 1/2-1/1 між CatA та CatC також знаходяться в режимі FRW.

Якщо комутатор CatA виходить з ладу, вся мережа не припиняє роботу. В такому випадку інтерфейси 1/2-1/2 між CatB та CatC переходять в режим FRW

(Forwarding). Це забезпечує безперервність передачі даних між комутаторами CatB та CatC.

RSTP — це складний протокол, призначений для підтримки ефективної передачі даних у мережах з деревовидною структурою, які завжди є надійними. Основні переваги RSTP включають:

1. Швидке відновлення: У разі збою, RSTP здатний швидко відновити мережу, мінімізуючи час простою.

2. Масштабованість: Протокол дозволяє легко масштабувати мережу, додаючи нові пристрої.

3. Гнучкість: RSTP підтримує різні типи портів і топологій, що робить мережу більш гнучкою.

4. Ефективність: Використання RSTP дозволяє оптимізувати використання мережевих ресурсів.

5. Надійність: Протокол забезпечує високу надійність, запобігаючи утворенню петель і збоїв у мережі.

Опишемо як працює RSTP у разі відмови.

Проблеми з автоматичною зміною топології мережі за допомогою rstp. Таким чином, коли перемикач CatA не працює, rstp швидко встановлює інтерфейси 1/2-1/2 між CatB і CatC, щоб створити новий спосіб передачі інформації, що гарантує постійну роботу мережі.

Швидке усунення поломок і скорочення часу простою значно підвищують надійність і ефективність мережевих систем. Це пояснює важливість RSTP для побудови сучасних надійних з’єднань.

1.4 Протокол агрегації LACP

Для забезпечення надійності мережі використовуються різні протоколи, серед яких більш ефективним виявився LACP (Link Aggregation Control Protocol). Протягом певного періоду часу комітет IEEE 802.3ad запровадив цей механізм для покращення попередньої версії LAG (Link Aggregation Group) .

Протокол LAG раніше використовувався для об’єднання двох фізичних з’єднань, щоб збільшити пропускну здатність і підвищити надійність мережі, але він не міг налаштовуватися залежно від того, наскільки останнє було завантажено. Існує вдосконалення LACP, яке дає змогу динамічно змінювати фізичні з’єднання в логічному з’єднанні. Ця зміна дозволяє мережі підходити до різних робочих середовищ і пропонувати чудову якість і завадостійкість.

За стандартами 802.1AX і 802.3ad IEEE слідує LACP. Правила протоколу пояснюють, як встановлюється віртуальний канал, кількість фізичних каналів, з яких він складається, може змінюватися залежно від навантаження на мережу, а також способи обміну інформацією між станціями (ПК, принтер), щоб їх діяльність не зникала. бути порушеною, коли ресурси, необхідні мережі, використовуються належним чином.

Для забезпечення надійності мережі необхідно ввести в дію протокол LACP. Якщо фізичне, але не логічне з’єднання не вдається, протокол LACP відреагує перенесенням даних на інше фізичне з’єднання залежно від доступних ресурсів конфігурації мережі. Це робиться для запобігання збоїв у мережі та підтримки постійного потоку інформації [11].

Обладнання Juniper добре працює зі стандартами IEEE 802.1AX і 802.3ad, і його можна встановити для створення логічного зв’язку через протокол LACP. Крім того, можна налаштувати різні параметри LACP, включаючи критерії вибору порту та часовий інтервал. Це забезпечує якісну передачу даних, а також стабільну роботу за будь-яких вимог користувача.

Згідно з опитуванням мережевої компанії Cisco, проведеним у 2021 році, протокол LACP є найпоширенішим для агрегації каналів зв'язку:

- 70% мереж центрів обробки даних використовують LACP.

- 47% корпоративних кампусів також використовують LACP.

- 59% організацій планують розгорнути або розширити використання LACP протягом наступних 12 місяців[13].

1. Автоматична конфігурація: за допомогою LACP пристрої можуть знаходити та створювати групи агрегації каналів без необхідності ручного втручання.

2. Розподіл трафіку в реальному часі: у LAG трафік розподіляється між декількома посиланнями за допомогою методів, включаючи MAC-адресу джерела/одержувача, IP-адресу або номер порту TCP/UDP, щоб забезпечити динамічне балансування навантаження.

3. Резервування і обхід відмов: Резервування та завадостійкість забезпечуються шляхом виявлення збою каналу та перемикання його трафіку на інші активні канали в межах LAG, таким чином запобігаючи його дублюванню та резервному копіюванню.

4. Сумісність на основі стандартів: LACP є загальновизнаним промисловим стандартом, який забезпечує плавний зв’язок між пристроями, виготовленими різними компаніями.

Протокол LACP — це універсальний, масштабований і надійний підхід до об’єднання каналів зв’язку між пристроями в мережі. У сучасних сучасних мережах, які вимагають здатності витримувати зміни в трафіковому навантаженні, залишаючись достатньо надійними, щоб усе це працювало, це незамінна частина. Це має вирішальне значення для збереження з’єднання з мережею, навіть якщо деякі фізичні з’єднання виходять з ладу, завдяки цій функції LACP здатності об’єднувати декілька з’єднань Ethernet в одне логічне з’єднання.

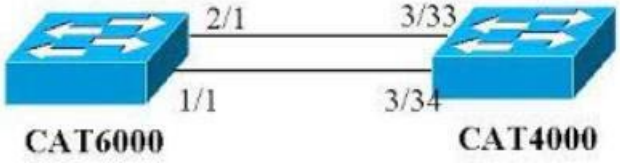


Рисунок 1.5 - Приклад використання протоколу LACP [15]

Неможливо переоцінити функцію протоколу керування агрегацією каналів (LACP) у підвищенні завадостійкості мережі, оскільки він не лише оптимізує використання ресурсів, але й збільшує пропускну здатність. У цьому уривку ми заглибимося в практичний приклад, який демонструє переваги використання LACP у практичній установці.

На рис. 1.5 наведений приклад мережі з використанням протоколу LACP. Якщо фізичний канал 2/1 - 3/33 вийде з ладу, мережа все ще буде функціонувати завдяки іншому фізичному каналу 1/1 - 3/34. Таким чином, LACP забезпечує неперервність передачі даних навіть у випадку відмови окремого фізичного з'єднання[14].

1. Підвищення надійності: LACP дозволяє створювати логічні з'єднання з надлишковістю, що забезпечує автоматичне переключення на інші активні канали у разі відмови.

2. Збільшення пропускної здатності: Об'єднання декількох фізичних з'єднань у логічний канал дозволяє збільшити пропускну здатність мережі.

3. Ефективне використання ресурсів: LACP дозволяє динамічно розподіляти трафік між різними фізичними з'єднаннями в залежності від навантаження.

4. Сумісність і стандартизація: LACP є стандартним протоколом, що підтримується більшістю мережевих пристроїв і операційних систем, що забезпечує його широку сумісність та застосування.

LACP особливо важливий у великих мережах, таких як:

- центри обробки даних;
- хмарні мережі;
- мережі провайдерів;
- телекомунікаційні мережі.

Використовуючи LACP у високопродуктивних надійних середовищах, можна оптимізувати роботу мережі та підтримувати безперервну передачу даних.

1.5 Динамічна маршрутизація

Однією з основних причин, чому комп'ютерні мережі потребують антивірусної програми, є контроль найкращого маршруту для обміну даними. Такі ролі в цьому домені мають протоколи BGP і OSPF.

Протокол OSPF (Open Shortest Path First) служить внутрішнім протоколом маршрутизації в рамках єдиної самоврядної системи. Він використовує алгоритм Дейкстри, щоб визначити найкращі маршрути до певного пункту призначення. Для OSPF слід зазначити, що він має розподілену базу даних маршрутизації, яка дозволяє швидко змінювати маршрут, коли змінюється конфігурація мережі [17].

BGP BGP (Border Gateway Protocol) — це протокол маршрутизації, який допомагає маршрутизувати мережі між незалежними системами, які називаються автономними системами . У всесвітній мережі Інтернет, де різні провайдери мережі спілкуються один з одним, це широко використовуваний протокол. Основними перевагами BGP є його всесвітня застосовність, гнучкість у контролі маршрутизації, гарантія безпеки та підтримка різних показників) [18].

Протокол BGP має наступні основні переваги:

1. Він спеціально розроблений для глобальних мереж Інтернету, які можна легко розширити до великих мереж із великою кількістю маршрутів.

2. BGP пропонує покращену гнучкість у контролі маршрутів завдяки врахуванню різних політик і умов у автономних системах.

3. Надає заходи безпеки, щоб гарантувати безпечний обмін маршрутами, включаючи автентифікацію та шифрування.

4. Має гнучкість у підтримці політики: підтримка BGP для кількох показників, за допомогою яких визначаються великі потреби в дорозі та встановлюються жорсткі політики маршрутизації.

5. Забезпечує підтримку внутрішніх і зовнішніх шляхів: це робиться завдяки дозволу BGP підключатися до різних типів мереж через зовнішні та внутрішні протоколи маршрутизації.

Розглядаючи мережеве середовище, як OSPF, так і BGP є важливими для

забезпечення ефективності, масштабованості та безпеки.

Динамічна маршрутизація передбачає автоматизацію вибору найкращого шляху передачі даних у комп’ютерних мережах. Замість того, щоб вибирати маршрути вручну, мережеві пристрої використовують протоколи динамічної маршрутизації, які дозволяють їм обмінюватися інформацією про стан мережі та знаходити шлях, який найкраще працюватиме для передачі даних.

Основні протоколи динамічної маршрутизації включають OSPF (Open Shortest Path First) і BGP (Border Gateway Protocol) [19].

1. OSPF: Використовує алгоритм Дейкстри для пошуку найефективніших маршрутів до пункту призначення, оскільки працює в одній автономній системі. OSPF вибирає найкращий шлях на основі таких факторів, як пропускна здатність лінії. Коли відбуваються зміни в мережі, OSPF надає розподілену базу даних маршрутизації та забезпечує швидке оновлення маршрутів.

2. BGP: це протокол маршрутизації для обміну інформацією про маршрутизацію між окремими системами. BGP використовується в мережах глобальної мережі Інтернет для з'єднання кількох мережевих провайдерів один з одним. Певні критерії, такі як пропускна здатність, географічне розташування, протоколи маршрутизації тощо, використовуються цим протоколом маршрутизації для вибору найкращого шляху для надсилання пакетів даних від однієї AS до іншої.

BGP має ряд переваг, таких як глобальне охоплення, гнучке керування політикою маршрутизації, покращені функції безпеки та підтримка багатьох параметрів. Завдяки здатності швидко зростати до сотень тисяч мережевих префіксів, BGP дозволяє мережевим адміністраторам бути більш гнучкими у прийнятті рішень щодо маршрутизації, використовуючи автономні системи для параметрів політики та обмежень. Крім того, він поставляється з різними засобами захисту, які можна використовувати для забезпечення безпеки.

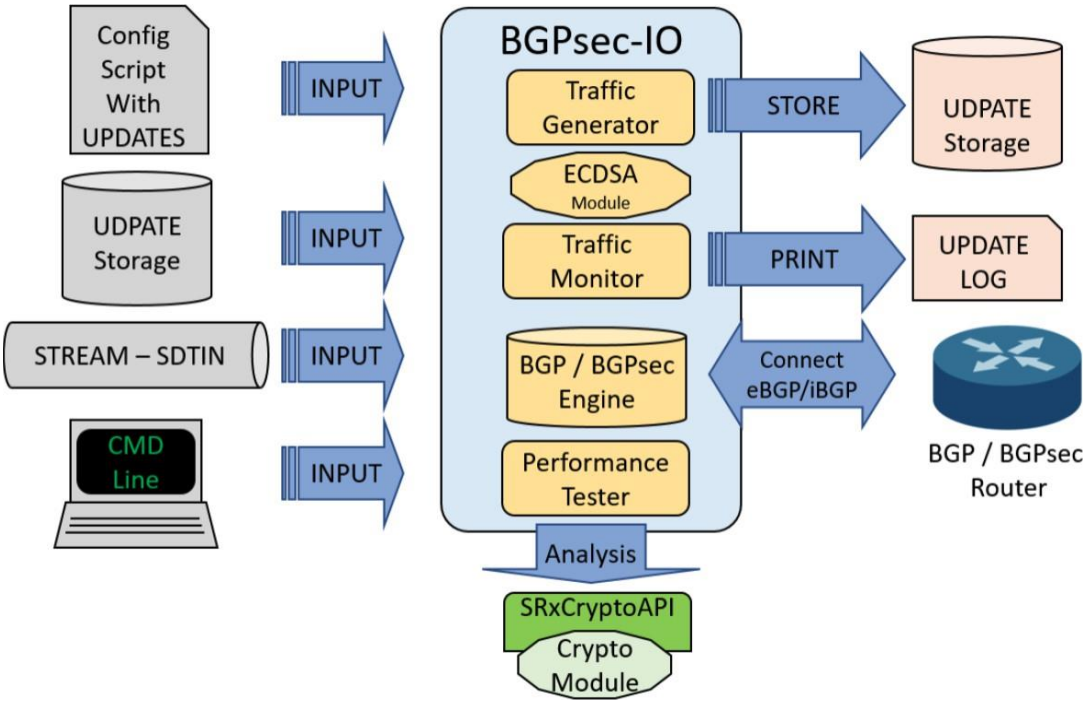


Рисунок 1.6 - Приклад роботи протоколу BGP [19]

Топографічна мережа, відома як «Кільце», була визначена як найбільш придатна для надійної мережі через її важливість у забезпеченні найкращої продуктивності та надійності. Це важливо, оскільки він може відігравати ключову роль у складних мережах у поєднанні з мережами гібридного типу.

Вибір таких завадостійких протоколів, як LACP, RSTP і BGP, відповідає цілям проекту, що свідчить про те, що ці конкретні протоколи можуть краще впоратися з потребами завадостійкості мережі.

1.6 Управління і прогнозування трафіку в інформаційних мережах з використанням обладнання Juniper Networks

Використання сучасного обладнання є запорукою стабільної та ефективної роботи мережі [29]. Одним з провідних виробників у цій галузі є компанія Juniper Networks, відома своїми передовими технологіями та широким асортиментом продукції. Обладнання Juniper Networks дозволяє організаціям досягти високої продуктивності та безпеки мережі. Juniper Networks пропонує рішення для різних

потреб, включаючи маршрутизацію, комутацію, безпеку та управління мережею. Серед найважливіших напрямків - розробка і впровадження передових технологій, таких як програмно-визначені мережі (SDN) і мережі на основі намірів (IBN), які дозволяють автоматизувати і оптимізувати роботу мереж. Оптимізація локальних мереж з обладнанням Juniper стає серйозним викликом для мережевих інженерів з такими технологіями, як QoS (Quality of Service), VLAN (Virtual Local Area Networks), LAG (Link Aggregation) і багатьма іншими. Juniper Networks постійно працює над вдосконаленням своїх продуктів і розробкою нових рішень для задоволення зростаючих мережевих потреб сучасних організацій. Окрім надання стабільного та надійного обладнання, компанія також впроваджує інтелектуальні системи управління мережею, які відіграють важливу роль в індустрії. При управлінні мережами слід враховувати явище фрактальності (самоподібності) трафіку. При цьому значний інтерес для таких областей, як контроль перевантажень, контроль втрат та розподіл смуги пропускання має задача прогнозування мережевого трафіку [20].

Самоподібність трафіку в комп`ютерних мережах була вперше описана в класичних роботах [30, 31]. Такий трафік характеризується значною нерівномірністю, що приводить до погіршення його обслуговування.

Інтуїтивно самоподібність означає, що властивості об`єкту зберігаються незалежно від масштабування часу або простору. У комп’ютерних мережах нас цікавить статистична самоподібність, тобто поведінка кореляційної функції на різних часових масштабах. Ступінь нерівномірності фрактального трафіку зазвичай характеризується параметром Херста. Більшість досліджень зосереджено на прогнозуванні трафіку за допомогою таких методів, як ARIMA; різні версії ARIMA [22].

Метою дослідження, виконаного в [29], була оцінка ефективності алгоритму прогнозування трафіку в локальних мережах. Дослідження включало порівняльний аналіз декількох алгоритмів прогнозування, прогнозування на основі моделей ARIMA, просте експоненціальне згладжування та подвійне експоненціальне згладжування. Для оцінки алгоритмів використовувалася

середньоквадратична помилка прогнозу. Результати проведеного дослідження підтвердили, що просте експоненціальне згладжування дає найкращі прогнози для заданого трафіку. Перехід до подвійного згладжування не покращив точність прогнозу, що можна пояснити відсутністю чіткого тренду у трафіку, що розглядається. Використання авторегресійних моделей 1-го та 2-го порядку суттєво відстає за точністю прогнозу від простого експоненціального згладжування, яке є найбільш придатним для процесів ARIMA [20].

Таким чином, застосування простого експоненціального згладжування є одним із кращих підходів для управління інформаційним трафіком в інформаційних мережах з використанням обладнання Juniper Networks.

2 АНАЛІЗ МЕТОДІВ ПОБУДОВИ ЗАХИЩЕНИХ МЕРЕЖІ

2.1 Види інформаційних загроз

Розглянемо основні види інформаційних загроз [15].

Ефективна розширена система виявлення мережевого шахрайства, яка використовує різні технології, ефективно справляється зі складністю таких атак. Крім того, він також забезпечує безпечне шифрування передачі даних в основному за допомогою IPSec VPN.

Спуфінг — поширена техніка, яка використовується в Інтернет-комунікації, і її можна досить добре використовувати .

Атаки Brute-force спрямовані на злам паролів або ключів шифрування з використанням усіх можливих перестановок. Вони розпізнаються та забороняються фільтрами брандмауера, але IPsec VPN допомагає запобігти несанкціонованому доступу.

Витік персональних даних: Розголошення особистих даних може призвести до великих фінансових втрат і шкоди репутації. щоб захистити конфіденційну інформацію, у тому числі важливо використовувати шифрування трафіку, наприклад IPsec VPN, а також налаштувати фільтри брандмауера для контролю доступу.

Спам, який є небажаними повідомленнями, що містять шкідливі посилання або вкладення, може значно негативно вплинути на роботу в мережі. однак надано фільтри брандмауера, які блокують їх у точках входу, таким чином зупиняючи цей трафік до користувача.

Встановлення шкідливого програмного забезпечення (зловмисне програмне забезпечення): шкідливе програмне забезпечення здатне завдати значної шкоди мережевій інфраструктурі та даним. Фільтри брандмауера можуть уникати шкідливих інтернет-з’єднань із шкідливим програмним забезпеченням, тоді як IPsec VPN забезпечує конфіденційність даних.

Витік даних може призвести до значних фінансових і репутаційних втрат. Для захисту конфіденційної інформації використовується шифрування трафіку за допомогою IPSec VPN і контроль доступу через фільтри брандмауера.

Загрози, які долає мережа:

- фішинг;
- атаки brute force;
- спам;
- встановлення шкідливого ПЗ;
- витік персональних даних.

Таким чином, досліджувані методології захисту мереж включають: оцінку протоколу; IPsec VPN; фільтри брандмауера та інші способи посилення безпеки за допомогою серверів DNS або DHCP. Цей огляд відображає розуміння того, наскільки важливі різні методи для підтримки безпеки інфраструктури комп’ютерної мережі.

IPsec VPN використовуються для створення безпечних приватних віртуальних мереж, щоб конфіденційні дані передавалися безпечно, забезпечуючи їх цілісність і автентичність джерела. Фільтри брандмауера дозволяють контролювати доступ до мережі та захищати її від різних небезпек і нападів. Цей гнучкий механізм дозволяє налаштувати параметри безпеки для кожного інтерфейсу, порту чи навіть протоколу.

Для DNS-сервера та DHCP-сервера важливо застосовувати додаткові заходи безпеки. DNS-сервер — це сервер, який перетворює доменні імена в IP-адреси та запобігає можливому зловмисному трафіку. І навпаки, DHCP-сервер слугує для автоматизації мережевих конфігурацій для підключених гаджетів, таким чином забезпечуючи правильне налаштування та ідентифікацію пристрою.

Забезпечення безпеки мережевої інфраструктури значною мірою залежить від заходів безпеки та протоколів. Реалізація цілісної стратегії, наприклад, використання IPsec VPN; Фільтри брандмауера; DNS сервер; Сервер DHCP відіграє важливу роль у створенні надійної захищеної мережі, яка забезпечує

конфіденційність даних, захист від несанкціонованого проникнення серед інших ризиків.

Служби DNS забезпечують основу, на якій налаштовано Інтернет для перетворення доменних імен на IP-адреси для полегшення мережевого зв’язку; система почалася з народженням Інтернету в 1960-х роках, отже, реагуючи на нагальність розробки методів комп’ютерної ідентифікації, які були б ефективними та зручними. Спочатку листування велося за допомогою табличних даних, але це стало проблематичним через їх обсяг з огляду на зростання мереж. DNS[20] служить основою Інтернету, полегшуючи перетворення доменних імен на IP-адреси, що допомагає в мережевому спілкуванні. Воно виникло з появою Інтернету в 1960-х роках, оскільки виникла потреба у відповідному режимі ідентифікації комп’ютера. Спочатку листування велося через таблиці, але це було недостатньо через зростання складності мережі.

Стандарт протоколу DNS був сформульований у 1983 році, що призвело до створення ієрархічної серверної системи, яка замінила попередні таблиці відповідності. Подальший розвиток DNS спричинив за собою нові версії протоколу, різні розширення, такі як впровадження нових типів записів; включення покращень безпеки.

Система доменних імен (DNS) працює як децентралізована мережа серверів, організованих в ієрархічний спосіб за допомогою доменних імен. Таке розташування забезпечує рівномірне завантаження сервера та його резервування. DNS постійно розвивається у відповідь на зростаючі потреби та досягнення Інтернету.

DNS підвищує ефективність спілкування в мережі, роблячи доменні імена розпізнаваними пристроями, уможливлюючи розподіл навантаження та роблячи мережу більш безпечною. Реалізації цього сприяє використання таких елементів DNS, як DNS-сервери, DNS-перетворювачі та DNS SEC, що зрештою призводить до більш ефективного захищеного мережевого зв’язку.

2.3 DHCP сервер

Розроблений у 1980-х роках протокол динамічної конфігурації хоста (DHCP) є частиною пакету TCP/IP, який спрощує процес призначення IP-адрес і таких налаштувань мережевим пристроям. Ця концепція виникла в RFC 951 у 1985 році. Рання версія DHCP під назвою DHCPv1 з'явилася в 1993 році та мала основні функції. Згодом у 1997 році з'явилася інша версія під назвою DHCPv2, яка представила більш розширені функції, такі як динамічне перепризначення IP-адреси та підтримка мобільних мереж. У той час ці розробки призвели до створення DHCPv6 у 1999 році, який був сумісний з Інтернет-протоколом версії 6 (IPv6).

Техніка постійно змінюється для включення різноманітних розширень, таких як динамічні оновлення DNS та ідентифікація клієнта, щоб вона могла постійно задовольняти потреби сучасних мереж. Тут варто згадати DHCPv6, який спеціально призначений для IPv6 і для призначення IPv6-адрес цим мережам.

Наявність DHCP в мережі робить значну різницю у декількох аспектах[22]:

1. Автоматичне налаштування: Коли налаштування виконується автоматично за допомогою DHCP, це усуває ручне призначення IP-адрес і налаштувань мережі, таким чином спрощує процес додавання нових пристроїв у мережі зі зменшенням шансів помилок.

2. Ефективне використання IP-адрес: За оптимальних умов DHCP гарантує, що IP-адреси добре розподіляються, щоб не було статичних конфігурацій, які спричиняють інші проблеми через конфлікти, навіть якщо він прагне максимального використання.

3. Централізоване керування: DHCP дозволяє централізоване керування налаштуваннями мережі, гарантуючи, що всі пристрої в мережі мають однакові налаштування.

4. Зручність для користувачів: Через DHCP мережеве з'єднання стає простішим, оскільки не потрібно втручання людини, коли пристрої підключено.

Сучасні комп’ютерні мережі стають більш ефективними завдяки таким функціям, як DHCP, які спрощують керування мережею, що, у свою чергу, підвищує зручність для користувачів.

2.4 Firewall Filters

Необхідність захисту безпеки мереж, а також роботи з виникаючими ризиками тісно пов’язана з еволюцією та вдосконаленням фільтрів брандмауера [23]. З 1980-х років фільтри брандмауера стали важливим компонентом для захисту мереж від несанкціонованих вторгнень і зломів.

Фільтри брандмауера були в основному розроблені для перевірки мережевого трафіку, щоб запобігти будь-якому несанкціонованому проникненню, а також захистити від знайомих небезпек. Однак із ускладненням мереж і появою нових загроз безпеці з’являються фільтри брандмауера.

Сьогодні потужні фільтри брандмауера [24] мають багато функцій, вони можуть працювати на різних рівнях мережевої купи (наприклад, на рівні IP, TCP/UDP або на рівні програми). Вони можуть підтримувати різні критерії фільтрації - деякі з них дозволяють трафік, а інші блокують його за допомогою інших політик.

Останні досягнення в галузі фільтрів брандмауера пов’язані з розробками технологій машинного навчання та штучного інтелекту. Це покращило їх здатність виявляти нові загрози та ефективно боротися з ними.

Основними перевагами використання Firewall Filters в мережах з використанням обладнання Juniper є:

1. Безпека: запобігайте неавторизованому доступу та захищайтеся від відомих загроз і атак.

2. Керування трафіком: точно регулюйте потік мережевого трафіку, щоб уможливити створення правил доступу, а також розділення трафіку.

3. Універсальність: можливість реалізації фільтрації трафіку на різних рівнях мережевого стеку, що забезпечує гнучкість реалізації політики безпеки.

4. Логування та аналіз: Ви можете реєструвати події та аналізувати мережеву активність з метою виявлення потенційних загроз.

Використання Firewall Filters в мережах Juniper сприяє ефективному управлінню мережевим трафіком, захищаючи його від будь-якої форми незахищеності, пов’язаної з мережевим трафіком.

2.5 Побудова IPsec VPN

Технологія IPsec VPN була представлена в 1990-х роках для захисту даних, що передаються через ненадійні мережі, такі як Інтернет. Саме після стандартизації цих протоколів у 1995 році VPN-з’єднання почали надійно використовуватися для захисту даних у мережах [25].

З кожним днем IPsec VPN продовжує вдосконалюватися, щоб задовольнити зростаючу складність налаштувань мережі та нові вимоги безпеки. Його розширені функції включають підтримку різних алгоритмів шифрування та автентифікації, більш розширені можливості адміністрування та автентифікації, а також сумісність з мобільними пристроями.

Принцип побудови IPsec Tunnel показано на рис. 2.1.

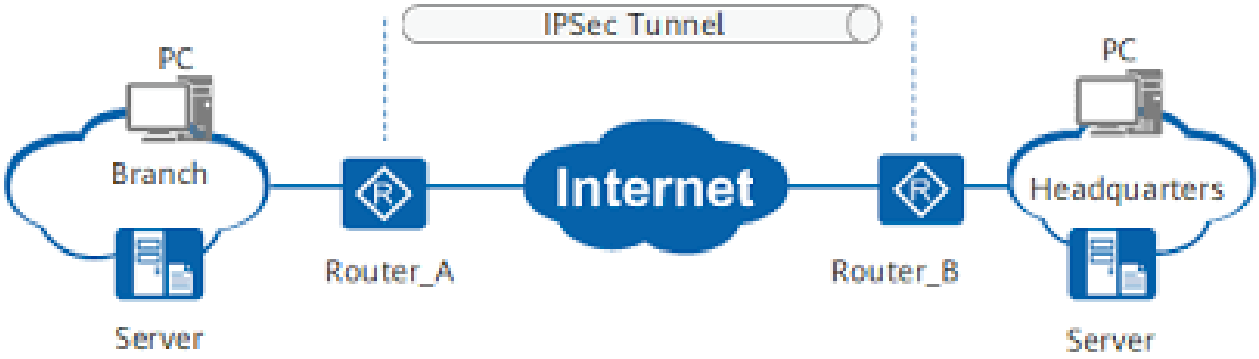


Рисунок 2.1 - Приклад побудови IPsec Tunnel

Ключовою технологією, яка використовується для створення безпечних з’єднань для мереж і користувачів у віддалених місцях у мережах обладнання Juniper, є IPsec VPN, яка працює на критичних рівнях. Ці рішення мають низку

атрибутів, що становлять IPsec VPN від Juniper, таких як надійна продуктивність, можливість масштабування на додаток до можливості налаштування за допомогою вибраних параметрів, наприклад автентифікації, алгоритмів шифрування. Основні переваги використання IPsec VPN на обладнанні Juniper включають автентифікацію та шифрування, настроювані параметри конфігурації, можливість розширення та надійність звуку. Ці атрибути роблять їх надійним і ефективним засобом захисту інформації в сучасних мережах [26].

3 ПОБУДОВА ЗАХИЩЕНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ПЛАТФОРМИ EVE-NG

3.1 Віртуальна лабораторія EVE-NG

Віртуальна лабораторія EVE-NG є платформою, що імітує точні мережеві структури, придатні для різних цілей, включаючи тестування навчання та дослідження. Вона використовує дружнє середовище для створення віртуальних мереж для імітації сценаріїв живої мережі без потреби у фізичних пристроях [27].

Основні переваги EVE-NG порівняно з іншими віртуальними лабораторіями [28]:

1. Гнучкість та масштабованість - Платформа EVE-NG використовується для створення складних мереж з використанням багатьох віртуальних пристроїв. Відповідно до ваших потреб ви можете об’єднати та керувати різним мережевим обладнанням, таким як маршрутизатори, комутатори та брандмауери

2. Підтримка різних платформ - На платформі EVE-NG користувач може емалювати пристрої від різних виробників, таких як Cisco, Palo Alto, Juniper Networks, Fortinet та інші, щоб зрозуміти, як вони працюють, і налаштувати їх.

3. Легкість використання - EVE-NG розроблено з думкою про користувача, тому створення віртуальних мереж, підключення пристроїв і їх налаштування є легким заняттям завдяки простому підходу перетягування.

4. Підтримка додаткових функцій - розширені функції, які надає EBE-NG, включають моніторинг мережі, аналіз трафіку, запис і відтворення сеансу, візуалізацію трафіку серед інших функцій, які допомагають у вивченні та аналізі мережевих проблем.

5. Спільнота та ресурси - Платформа EVE-NG має активну та дружелюбну спільноту користувачів, яка надає величезну кількість корисних ресурсів, таких як топології мереж, файли конфігурації, навчальні матеріали та посібники, що робить її центром для користувачів, щоб обмінюватися знаннями та досвідом.

Розробка EVE-NG почалася в 2014 році, в результаті чого була випущена

перша версія. З тих пір EVE-NG зазнала ряду вдосконалення і прогресу, представивши нові функції, підвищивши продуктивність і зберігаючи сумісність з віртуальними пристроями різних типів. Вирішальний внесок, який спільнота користувачів EVE-NG робить щодо зворотного зв'язку для покращень, є життєво важливим для розвитку платформи. Це зростання в основному завдяки її здатності імітувати складні мережеві параметри - простіше кажучи, все, починаючи від підключення до невеликої віддаленої мережі. Ваші домашні пристрої з серверами десь у хмарах, для великомасштабного ефекту глобальної мережі або міської мережі, не встаючи зі стільця, крім того, він надає зручний віртуальний робочий простір, призначений насамперед для тестування та тренувань [27].

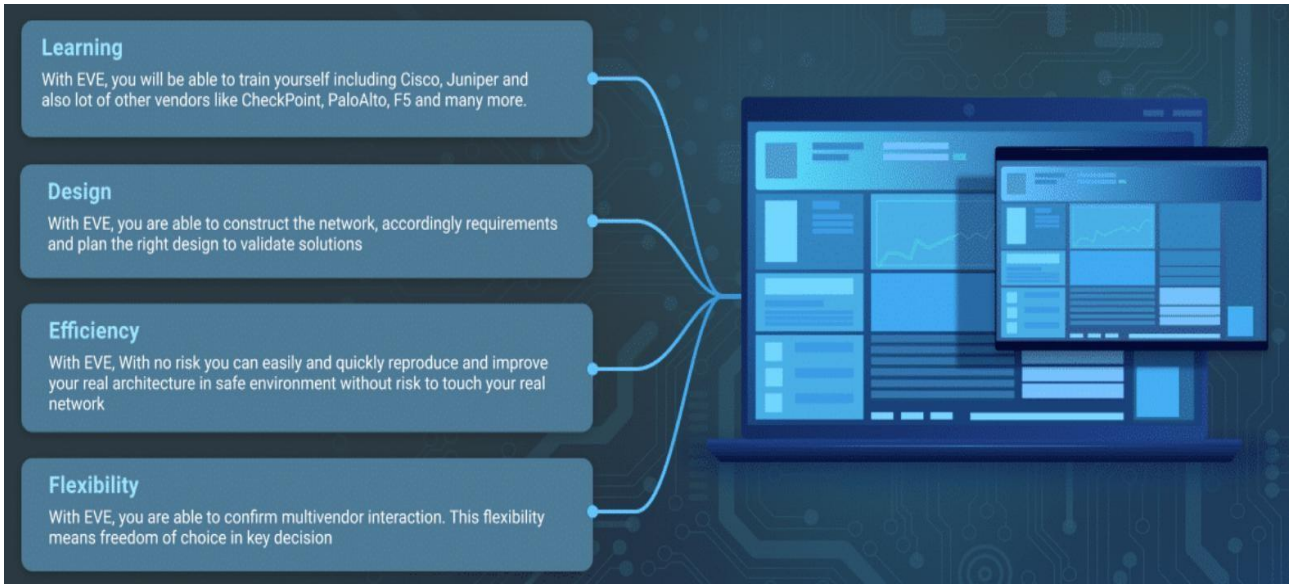


Рисунок 3.1 - Переваги EVE-NG над іншими віртуальними лабораторіями

3.2 Побудова макету мережі

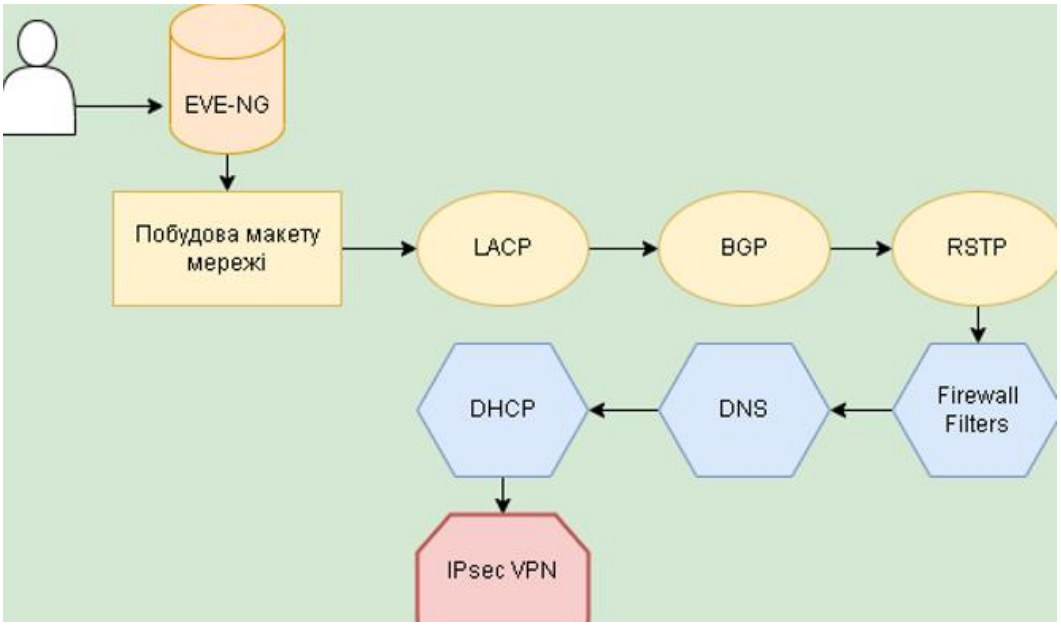


Рисунок 3.2 - Методика побудови захищеної мережі

Функціонал лабораторії EVE-NG

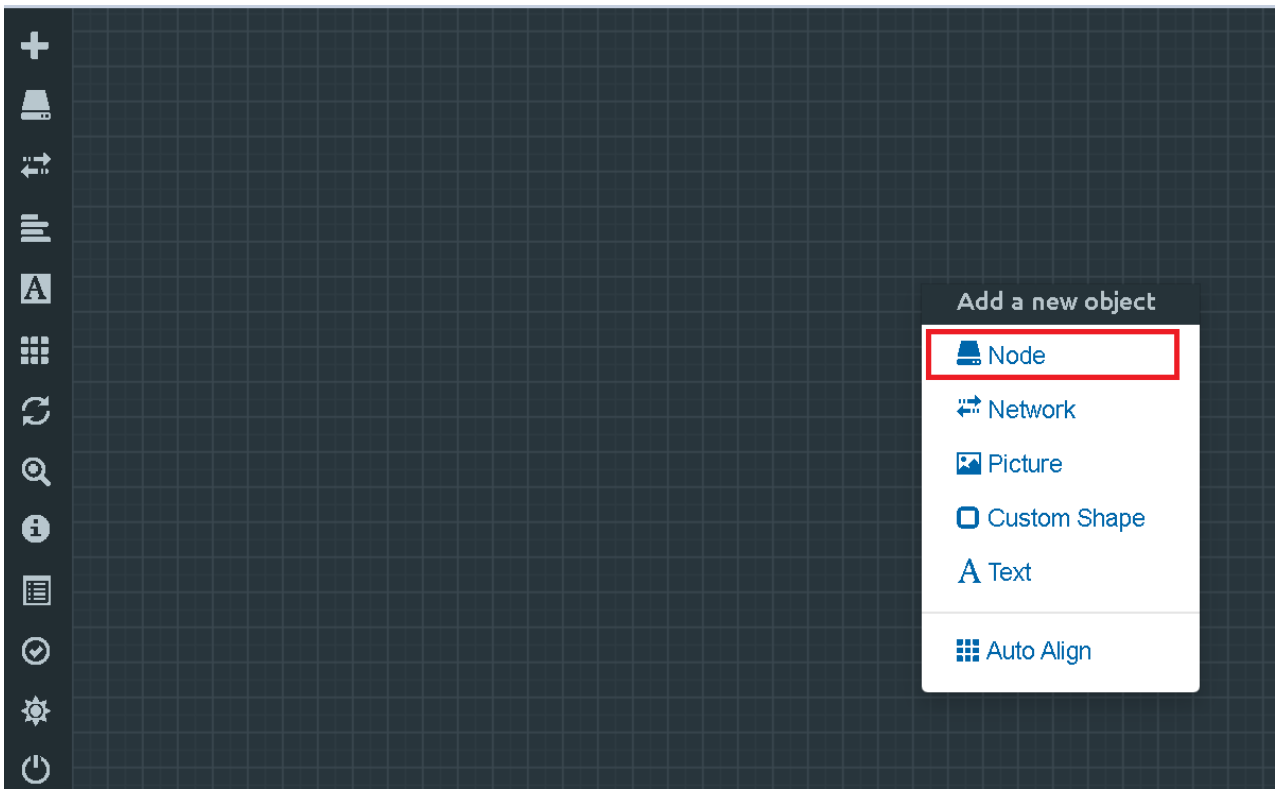


Рисунок 3.3 - Вибір Node

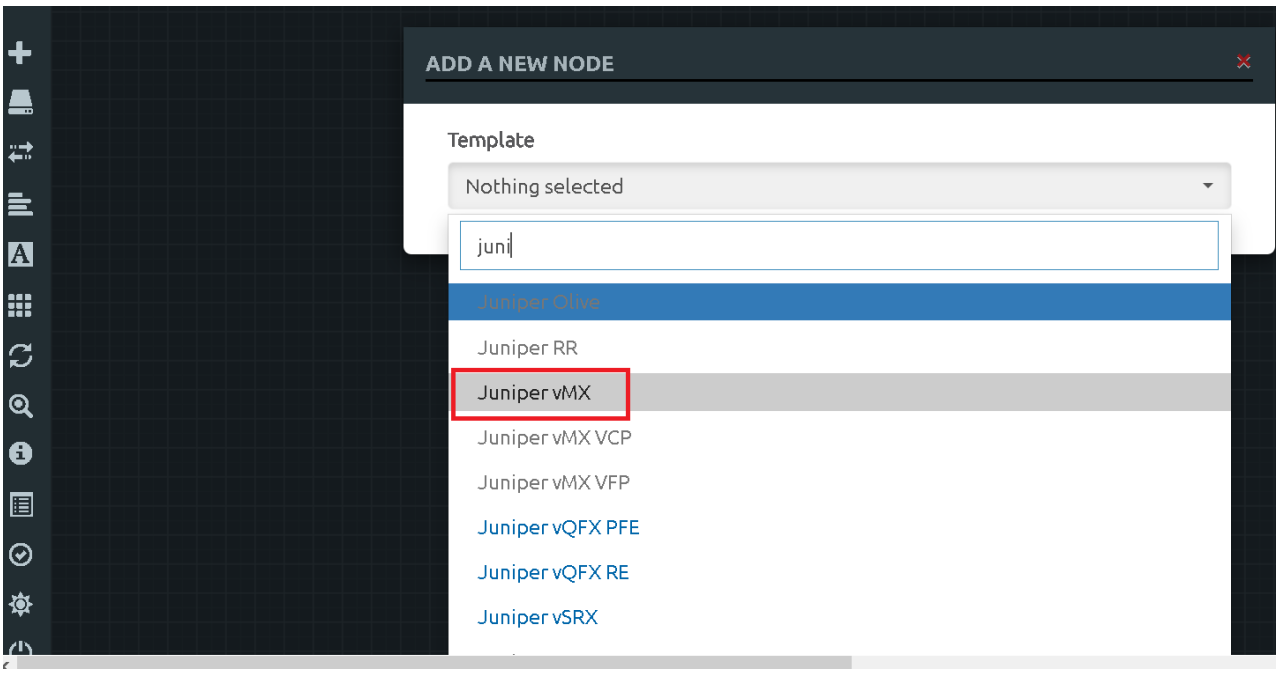


Рисунок 3.4 - Вибір потрібної моделі Juniper

3.3 Базові параметри

Наведемо основні параметрами для розробки мережі:

- кількість девайсів які потрібно створити 5;
- кількість портів - 22;
- версія образу системи - 6.0.2.0;
- кількість роутерів juniper vmx - 10;
- об’єм оперативної пам’яті - 16 ГБ.

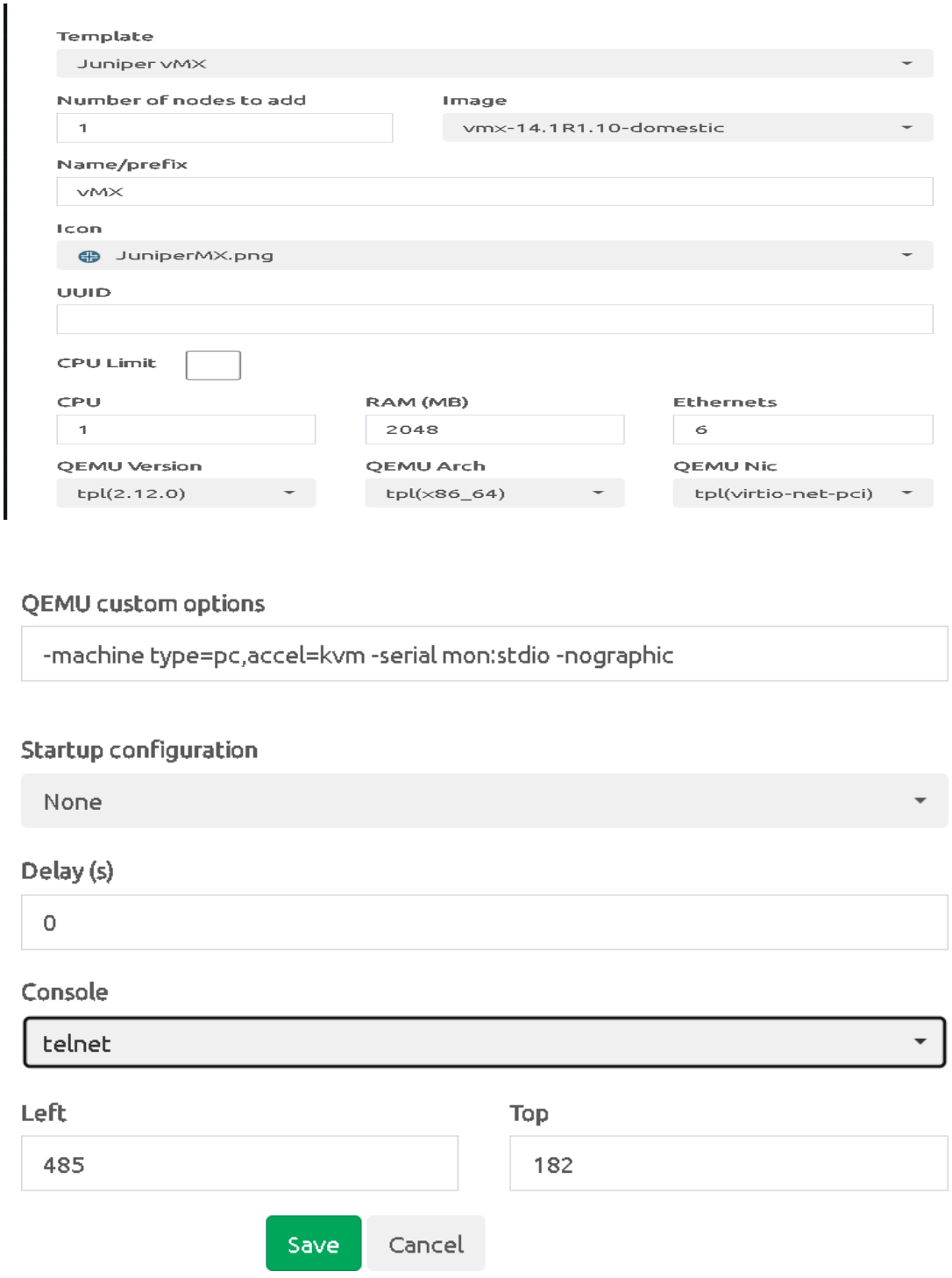


Рисунок 3.5 - Вибір параметрів маршрутизатора, друга частина

3.4 Умовні позначення на схемі

Будемо використовувати наступні позначення для основних елементів структури мережі, що наведено нижче.

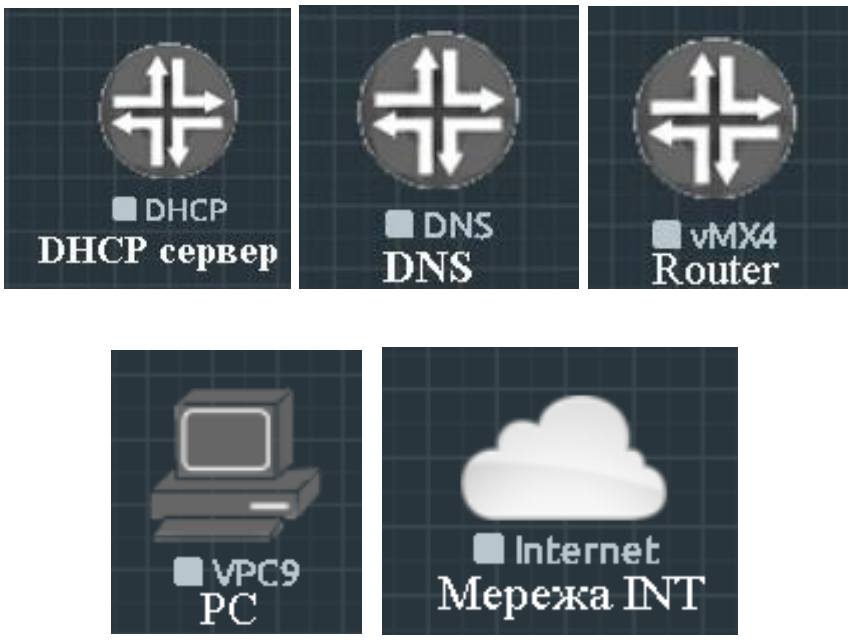


Рисунок 3.6 - Умовні позначення

3.5 Кінцева схема мережі

Кінцеву схему мережі наведемо на рис. 3.7.

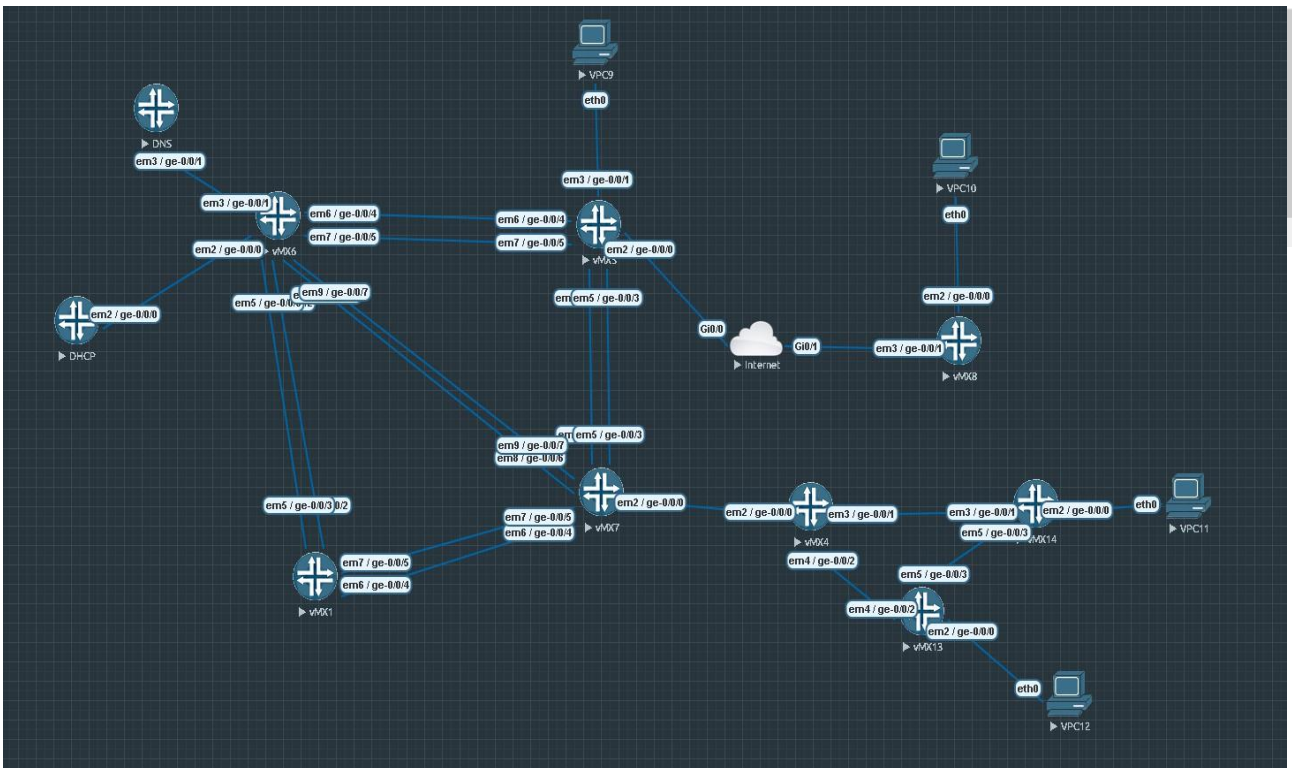


Рисунок 3.7 – Кінцева схема мережі

3.6 Налаштування LACP

Опишемо процес налаштування.

При цьому будемо мати на увазі, що автентифікацію слід налаштувати перед початком конфігурації LACP і оновлювати паролі щоразу, коли вони змінюються, оскільки будь-який інший спосіб не працюватиме в цій системі .

```
[edit]
root# set system root-authentication plain-text-password
New password:
Retype new password:

[edit]
root#
```

Потім налаштуємо Hostname:

Далі проведемо подібні налаштування на кожному з роутерів.

Потім налаштуємо максимальну кількість агрегованих каналів:

```
[edit]
root@Router1# set chassis aggregated-devices ethernet device-count 6

[edit]
root@Router1#
```

Для цього для агрегованих каналів Ethernet призначимо віртуальні інтерфеси та налаштовуємо їх наступним чином:

```
[edit]
root@Router1# set interfaces ge-0/0/4 gigether-options 802.3ad ae1

[edit]
root@Router1# set interfaces ge-0/0/5 gigether-options 802.3ad ae1

[edit]
root@Router1# set interfaces ge-0/0/2 gigether-options 802.3ad ae0

[edit]
root@Router1# set interfaces ge-0/0/3 gigether-options 802.3ad ae0

[edit]
root@Router1# set interfaces ge-0/0/6 gigether-options 802.3ad ae2

[edit]
root@Router1# set interfaces ge-0/0/7 gigether-options 802.3ad ae2
```

Задаємо IP адреси:

```
[edit]
root@Router1# set interfaces ae0 unit 0 family inet address 10.10.10.1/24

[edit]
root@Router1# set interfaces ae1 unit 0 family inet address 11.11.11.1/24

[edit]
root@Router1# set interfaces ae2 unit 0 family inet address 12.12.12.1/24
```

Потім активуємо канали LACP:

```
[edit]
root@Router1# set interfaces ae0 aggregated-ether-options lacp active

[edit]
root@Router1# set interfaces ae1 aggregated-ether-options lacp active

[edit]
root@Router1# set interfaces ae2 aggregated-ether-options lacp active
```

Подібним чином налаштуємо усі інші інтерфейси мережних пристроїв (див. рис. 3.8).

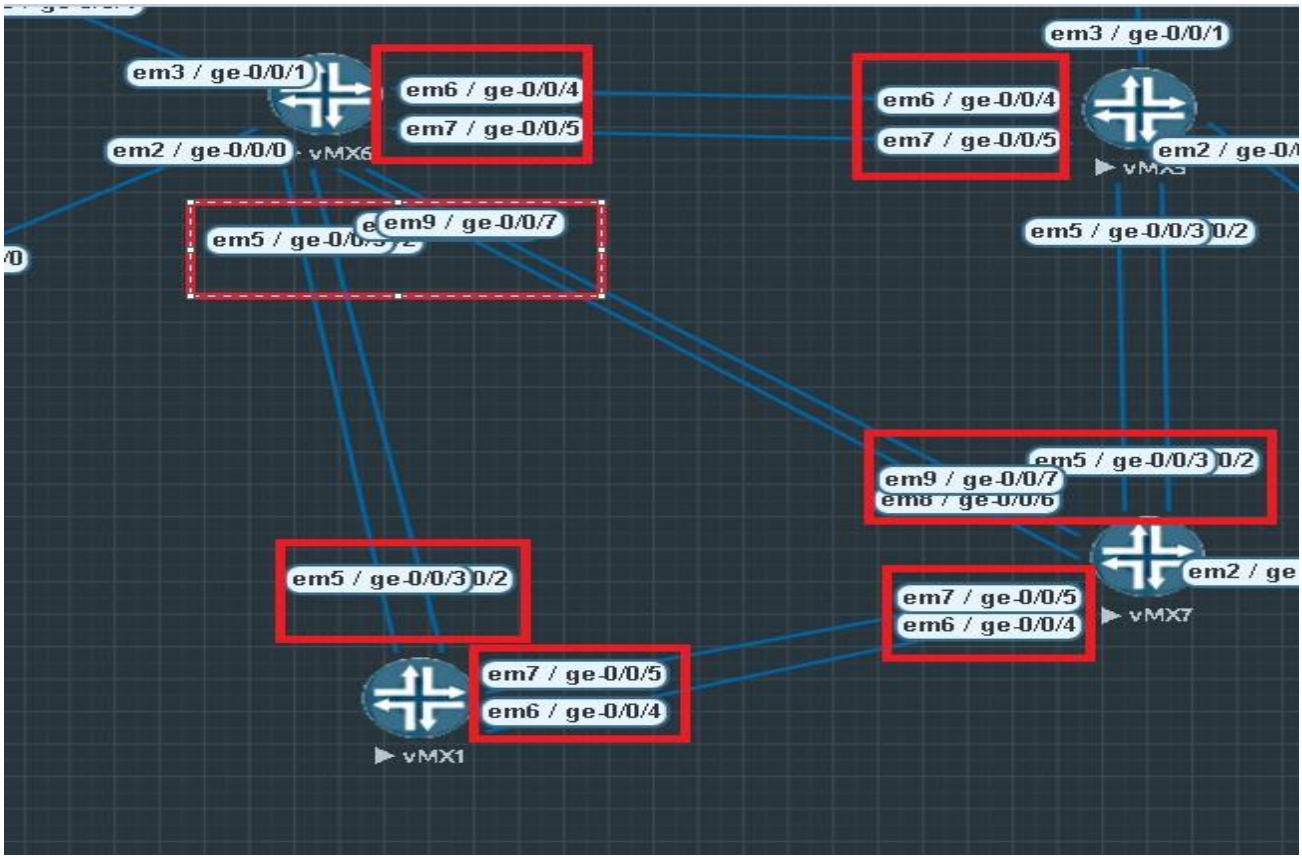


Рисунок 3.8 – Налаштування інтерфейсів мережі

Перевіримо коректність виконаних налаштувань:

```
root@Router1> show lacp interfaces
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/2      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/2    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
      ge-0/0/3      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/3    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/2                Current   Fast periodic Collecting distributing
      ge-0/0/3                Current   Fast periodic Collecting distributing

Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/4      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/4    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
      ge-0/0/5      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/5    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/4                Current   Fast periodic Collecting distributing
      ge-0/0/5                Current   Fast periodic Collecting distributing

Aggregated interface: ae2
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/6      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/6    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
      ge-0/0/7      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/7    Partner    No    No   Yes  Yes  Yes   Yes     Fast   Passive
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/6                Current   Fast periodic Collecting distributing
      ge-0/0/7                Current   Fast periodic Collecting distributing

root@Router1>
```

```
[edit]
root@Router1#  ...cy-statement announce-term from protocol direct

[edit]
root@Router1#  ...cy-statement announce-term then accept

[edit]
root@Router1#  ...e-policy term announce-term from protocol direct

[edit]
root@Router1#  ...e-policy term announce-term then accept

[edit]
root@Router1#  ... internal neighbor 10.10.10.2 family inet unicast

[edit]
root@Router1#  ... internal neighbor 10.10.10.2 export announce-policy

[edit]
root@Router1#  ...p group internal neighbor 11.11.11.2 family inet unicast

[edit]
root@Router1#  ...roup internal neighbor 11.11.11.2 export announce-policy

[edit]
root@Router1#  ...p group internal neighbor 12.12.12.2 family inet unicast

[edit]
root@Router1#  ...roup internal neighbor 12.12.12.2 export announce-policy
```

3.7 Налаштування BGP

Створимо автономну систему та групу BGP:

```
[edit]
root@Router1# set protocols bgp peer-as 65001

[edit]
root@Router1# set protocols bgp group internal type internal
```

Встановлюємо локальні IP адреси для BGP:

```
[edit]
root@Router1# set protocols bgp group internal local-address 10.10.10.1

[edit]
root@Router1# set protocols bgp group internal local-address 11.11.11.1

[edit]
root@Router1# set protocols bgp group internal local-address 12.12.12.1
```

Добавляємо сусідні вузли у створену групу:

```
[edit]
root@Router1# set protocols bgp group internal family inet unicast

[edit]
root@Router1# ... internal neighbor 10.10.10.2 peer-as 65002

[edit]
root@Router1# ...ols bgp group internal neighbor 11.11.11.2 peer-as 65003

[edit]
root@Router1# ...ls bgp group internal neighbor 12.12.12.2 peer-as 65004
```

Далі додаємо маршрути в політики маршрутизації та здійснюємо перегляд виконаних налаштувань.

Аналогічні налаштування виконуємо на кожному із роутерів.

```
[edit protocols bgp]
root@Router1# show
peer-as 65001;
group internal {
    type internal;
    local-address 12.12.12.1;
    family inet {
        unicast;
    }
    neighbor 10.10.10.2 {
        family inet {
            unicast;
        }
        export announce-policy;
        peer-as 65002;
    }
    neighbor 11.11.11.2 {
        family inet {
            unicast;
        }
        export announce-policy;
        peer-as 65003;
    }
    neighbor 12.12.12.2 {
        family inet {
            unicast;
        }
        export announce-policy;
        peer-as 65004;
    }
}
```

3.8 Налаштування RSTP

Переходимо в режим налаштувань RSTP та встановлюємо, що ми також можемо співпрацювати з STP:

```
[edit]
root# edit protocols rstp

[edit protocols rstp]
root# set force-version stp
```

Встановлює MAC-адрес призначення BPDU:

```
[edit protocols rstp]
root# set bpdu-destination-mac-address provider-bridge-group
```

Переходимо в інтерфейси ge-0/0/1 та ge-0/0/2. Налаштовуємо їх пріоритетність та режим роботи:

```
[edit protocols rstp]
root# edit interface ge-0/0/1

[edit protocols rstp interface ge-0/0/1]
root# set priority 0

[edit protocols rstp interface ge-0/0/1]
root# set mode point-to-point

[edit protocols rstp interface ge-0/0/1]
root# quit

[edit protocols rstp]
root# edit interface ge-0/0/2

[edit protocols rstp interface ge-0/0/2]
root# set priority 16

[edit protocols rstp interface ge-0/0/2]
root# set mode point-to-point

[edit protocols rstp interface ge-0/0/2]
root# quit
```

Налаштовуємо пріоритет самого мосту, максимальний очікуваний час прибуття блоків BPDU та інтервал часу, через який кореневий міст передає конфігураційні BPDU:

```
[edit protocols rstp]
root# set bridge-priority 8k

[edit protocols rstp]
root# set max-age 6

[edit protocols rstp]
root# set hello-time 6
```

Перегляд налаштувань:

```
[edit protocols rstp]
root# show
bpdu-destination-mac-address provider-bridge-group;
bridge-priority 8k;
max-age 6;
hello-time 6;
interface ge-0/0/1 {
    priority 0;
    mode point-to-point;
    edge;
}
interface ge-0/0/2 {
    priority 16;
    mode point-to-point;
    edge;
}
force-version stp;
```

3.9 Налаштування Firewall Filters

Створюємо Firewall Filter який буде дозволяти трафіку з source-address та destination-address проходити по порту і все це буде відбуватися на агрегованому інтерфейсі:

```
root# ...m allow-http from source-address 10.10.10.0/24

[edit]
root# ...m allow-http from destination-address 0.0.0.0/0

[edit]
root# ...t filter filter1 term allow-http from destination-port http

[edit]
root# set firewall family inet filter filter1 term allow-http then accept

[edit]
root# set interfaces ae0 unit 0 family inet filter input filter1
```

Налаштування Firewall Filter для блокування певного діапазону IP-адрес:

Налаштування Firewall Filter для дозволу SSH трафіку:

```
[edit]
root# ...nge term block-range from source-address 100.100.100.0/24

[edit]
root# ...t filter block-ip-range term block-range then discard
```

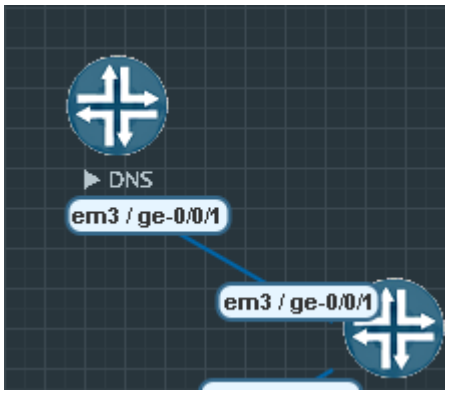
```
[edit]
root# set interfaces ae1 unit 0 family inet filter input allow-ssh
```

```
[edit]
root# ...erm allow-ssh-traffic from source-address 11.11.11.0/24

[edit]
root# ...erm allow-ssh-traffic from destination-port ssh

[edit]
root# ...t filter allow-ssh term allow-ssh-traffic then accept
```

Налаштування терміналу для Firewall Filter:

3.10 Налаштування DNS та DHCP

Налаштуємо інтерфейс конекту:




```
[edit]
root# set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.2/24
```

Визначимо DNS-сервери, які будуть використовуватись маршрутизатором для резольвації імен:

```
[edit]
root# set system name-server 8.8.8.8
```

Встановимо маршрут за замовчуванням для DNS-запитів через наш внутрішній інтерфейс IP-адресу:

```
[edit]
root# set routing-options static route 0.0.0.0/0 next-hop 192.168.1.2
```

3.11 Налаштування IPsec VPN

Змоделюємо налаштування протоколу IPsec VPN з врахуванням того, що для побудови IPsec потрібне середовище Internet,.

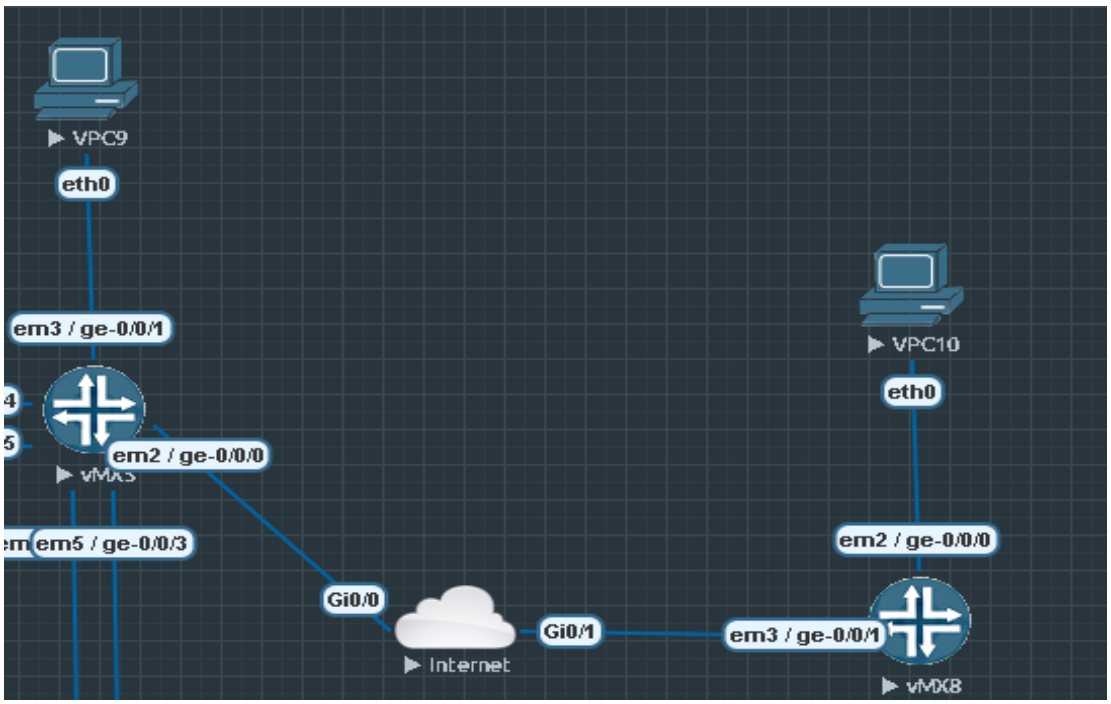


Рисунок 3.9 – Налаштування протоколу IPsec

Наведемо результати налаштування для Router 5.

Налаштуємо набір параметрів, які використовуються при налаштуванні тунелю IPsec між двома вузлами:

```
set security ipsec proposal Router5 protocol esp
set security ipsec proposal Router5 authentication-algorithm hmac-sha1-96
set security ipsec proposal Router5 encryption-algorithm aes-256-cbc
set security ipsec proposal Router5 lifetime-seconds 3600
```

Виконаємо налаштування параметрів для безпечного обміну ключами:

```
set security ike proposal Router5 auth-method pre-shared-keys
set security ike proposal Router5 dh-group group2
set security ike proposal Router5 auth-algorithm sha1
set security ike proposal Router5 enc-algorithm aes-256-cbc
set security ike proposal Router5 lifetime-seconds 28800
```

Проведемо налаштування політики IPsec:

```
set security ipsec policy policy1 proposals Router5
set security ipsec policy policy1 pfs-keys group2
set security ipsec policy policy1 protocol esp
```

Здійснимо налаштування VPN IPsec:

```
set security ipsec vpn VPN1 ike gateway gateway1
set security ipsec vpn VPN1 ike policy ipsec-policy-1
set security ipsec vpn VPN1 establish-tunnels immediately
set security ipsec vpn VPN1 bind-interface ge-0/0/0
```

Налаштуємо інтерфейс для тунелю IPsec:

```
set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.1/30
```

Виконаємо налаштування маршрутів:

```
set routing-options static route 1.1.1.1/30 next-hop ge-0/0/0
```

Проведемо налаштування для Router8:

```
set security ipsec proposal Router8 protocol esp
set security ipsec proposal Router8 authentication-algorithm hmac-sha1-96
set security ipsec proposal Router8 encryption-algorithm aes-256-cbc
set security ipsec proposal Router8 lifetime-seconds 3600
```

Налаштуємо параметри для безпечного обміну ключами:

```
set security ike proposal Router8 auth-method pre-shared-keys
set security ike proposal Router8 dh-group group2
set security ike proposal Router8 auth-algorithm sha1
set security ike proposal Router8 enc-algorithm aes-256-cbc
set security ike proposal Router8 lifetime-seconds 28800
```

Проведемо налаштування політики IPsec:

```
set security ipsec policy policy2 proposals Router8
set security ipsec policy policy2 pfs-keys group2
set security ipsec policy policy2 protocol esp
```

Виконаємо налаштування VPN IPsec:

```
set security ipsec vpn VPN2 ike gateway gateway2
set security ipsec vpn VPN2 ike policy ipsec-policy-2
set security ipsec vpn VPN2 establish-tunnels immediately
set security ipsec vpn VPN2 bind-interface ge-0/0/1
```

Налаштуємо інтерфейс для тунелю IPsec:

```
set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.2/30
```

І виконаємо налаштування маршрутів:

```
set routing-options static route 1.1.1.1/30 next-hop ge-0/0/1
```

Таким чином, було виконано оптимізацію конфігурації і тепер можемо здійснювати встановлення безпечного IPsec VPN з’єднання. Використання віртуальної лабораторії EVE-NG допомогло нам налаштувати захищену мережу з різними елементами, а також різними процесами. Налаштування елементів DNS, DHCP, LACP, RSTP, BGP, IPsec VPN і фільтри брандмауера позволило краще зрозуміти, як різні технології працюють у мережевому середовищі та як вони пов’язані між собою.

Очевидно, що створення неприступної мережі разом із налаштуванням DNS, DHCP, LACP, RSTP, BGP, IPsec VPN і фільтрів брандмауера є ключовими аспектами побудови надійної та безпечної інфраструктури. Ці технології виконують особливі функції в забезпеченні ефективного зв'язку, максимальної надійності та надійної безпеки в мережевому середовищі.

ВИСНОВКИ

У даній роботі проаналізовано процес налаштування безпечної мережі за допомогою засобів Juniper. Розглянуто різні конфігурації мережі, такі як шина та кільце, і вибрано кільцеву топологію як спосіб забезпечення безпечних з'єднань, на які можна завжди покладатися. Крім того, наявність такої топології вимагає впровадження додаткових заходів безпеки та керування, які враховувалися під час проектування та розгортання мережі.

Були проаналізовані різноманітні протоколи керування побічними реакціями, такі як LACP, RSTP і BGP. Використовуючи LACP, можна підвищити надійність, а також пропускну здатність за допомогою компіляції фізичних з'єднань на мережевих пристроях. Мережевий RSTP дозволяє швидко відновлювати зв'язки у разі перебоїв у мережі, тоді як статичні чи динамічні маршрутизатори можуть використовуватися для обміну пакетами в різних вузлах Beast. Наступні протоколи були ретельно перевірені та успішно інтегровані в систему.

Провели дослідження фільтрів брандмауера, які дозволяють регулювати та контролювати мережевий трафік відповідно до певних правил. З міркувань безпеки можна покращити функціональність мережі за допомогою IPsec VPN разом із іншими інструментами, такими як сервери DNS або DHCP. Протокол IPsec VPN забезпечує безпечний зв'язок у віддалених мережах завдяки використанню шифрування та стандартів автентифікації, тоді як DNS або DHCP допомагають керувати IP-адресами, а також надавати інші служби в мережі.

Розроблена мережа має кільцеву топологію та використовує IPsec VPN разом із фільтрами LACP, BGP, RSTP, DNS, DHCP і брандмауера.

Результати роботи свідчать, що обладнання Juniper добре підходить для створення безпечних мереж, які забезпечують стійку та надійну інфраструктуру з винятковою надійністю та продуктивністю. Саме завдяки оцінці протоколів LACP, RSTP і BGP, а також фільтрів брандмауера, мережевих конфігурацій і IPsec VPN надаються необхідні ресурси для створення такої мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.juniper.net/
2. http://readonline.com.ua/items/25235-osoblivosti-marshrutizatoriv-juniper- networks/
3. https://www.juniper.net/documentation/en_US/junos/topics/concept/junos - network-building-technologies-overview.html
4. https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh.
5. https://uk.warbletoncouncil.org/topologia-de-bus-12
6. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. – СПб.: Питер, 2003. – 864 с.
7. БерлинА.Н. Телекоммуникационные сети и устройства: Учебное пособие / А.Н. Берлин — М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. — 319 с
8. https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/2.4.4.html
9. http://conferenc.its.kpi.ua/2023/paper/view/27800
10. https://etutorials.org/Networking/Lan+switching+fundamentals/Chapter+10.+I mplementing+and+Tuning+Spanning+Tree/Introducing+Rapid+Spanning+Tree+Protocol/
11. https://routers.in.ua/lacp/
12. https://www.ibm.com/docs/ru/aix/7.2?topic=protocol-etherchannel-ieee-8023ad-link-aggregation-teaming
13. https://askanydifference.com/ru/difference-between-cisco-lag-and-lacp-with- table/
14. https://www.wik.ukua.nina.az
15. 2023 email security trends [Електронний ресурс] // Barracuda. – 2023. – Режим доступу до ресурсу: https://www.barracuda.com/reports/email-security-trends-report-2023.
16. https://uk.wikipedia.org/wiki/OSPF

17. https://highload.today/bgp/

18. https://studfile.net/preview/10030620/page:32/

19. https://www.nist.gov/services-resources/software/bgp-secure-routing-extension-bgp-srx-software-suite

20. https://www.ukraine.com.ua/blog/vse-o-domenah/chto-takoe-dns-server.html.

21. https://support.microsoft.com/ukua/topic/dns-d7476f12-818e-1db7-aa7b-7066fb5e382a.

22. https://techukraine.net

23. https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/firewall-filter-stateless-overview.html

24. https://networkdirection.net/study-notes/introduction-to-juniper/firewall-filters/

25. https://help.keenetic.com/hc/ru/articles/360000422620-IPSec-VPN-

26. https://www.juniper.net/documentation/us/en/software/junos/vpnipsec/topics/to pic-map/security-ipsec-vpn-overview.html

27. https://www.eve-ng.net

28. https://www.eve-ng.net/documentation

29. Парінцев Д.О. “Прогнозування трафіку у локальних мережах, побудованих з використанням обладнання JUNIPER” / 28-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2024.

30. Beran J., Sherman R., Taqqu M.S. Willinger W., Long-Range Dependence in Variable-Bit Rate Video Traffic. IEEE Transactions on Communications. Vol. 43. № 2,3,4. 1995.

31. Leland W.E., Taqqu M.S., Willinger W., Wilson D.V. On the self-similar nature of ethernet traffic // IEEE/ACM Transactions of Networking, 2(1), 1994. P. 1-15.