МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чернігівський національний технологічний університет
Навчально-науковий інститут технологій
Кафедра програмної інженерії

Технології розробки та супроводження програмного забезпечення систем

МЕТОДИЧНІ ВКАЗІВКИ
до лабораторного практикуму та самостійної роботи
для студентів напрямів підготовки
6.050103 – "Програмна інженерія"

ЗАТВЕРДЖЕНО
на засіданні кафедри
програмної інженерії
протокол № 10 від 21.12.2015

Чернігів ЧНТУ 2016

Технології розробки та супроводження програмного забезпечення систем. Методичні вказівки до лабораторного практикуму та самостійної роботи з дисципліни «Технології розробки та супроводження програмного забезпечення систем» для студентів напрямів підготовки 6.050103 – “Програмна інженерія”. /Укл.: Литвинов В.В., Нехай В.В. – Чернігів: ЧНТУ, 2016. – 48 с.

Укладачі: Литвинов Віталій Васильович, д-р. техн. наук, професор;
Нехай Валентин Валентинович, асистент.

Відповідальний за випуск: В.В. Литвинов, зав. кафедрою програмної інженерії, д-р. техн. наук, проф.

Рецензент: І. С. Скітер к.ф.-м.н., доцент кафедри програмної інженерії Чернігівського національного технологічного університету

ЗМІСТ

Вступ

В даний час комп'ютерні мережі є ключовою складовою сучасних інформаційно - телекомунікаційних систем.

Серед усіх завдань з побудови комп'ютерних мереж найважливішою є забезпечення їх захищеності від загроз конфіденційності, цілісності та доступності. При цьому підсистема захисту повинна бути повноцінною частиною комп'ютерної мережі, що забезпечує її безпеку, як одна з властивостей. При такому підході до побудови архітектури комп'ютерних мереж говорять про захищені комп'ютерні мережі.

Даний лабораторний практикум представляє набір лабораторних робіт з основ побудови та інструментальному аналізу захищених комп'ютерних мереж. Метою лабораторного практикуму є розвиток науково-освітнього забезпечення в галузі безпеки інформаційно-телекомунікаційних технологій. Завданням лабораторного практикуму є отримання знань і навичок за наступними напрямками:

– архітектура і методи побудови, захищених телекомунікаційних та комп'ютерних мереж;

– планування та проектування підсистем захисту інформаційних технологій;

– налагоджування засобів захисту мережевої інфраструктури;

– методи і засоби аналізу захищеності мережевих інформаційних інфраструктури.

Лабораторні роботи, орієнтовані на побудову інфраструктури захищених комп'ютерних мереж і налагодження механізмів їх коректного функціонування та захисту.

Опис кожної лабораторної роботи включає: назву, мету, короткі теоретичні відомості, постановку задачі, послідовність дій виконавця, а також питання і завдання для самостійних досліджень.

Для забезпечення умов виконання лабораторних робіт з побудови захищених комп`ютерних мереж рекомендується використовувати наступне основне програмне забезпечення:

– програмний емулятор мереж «Cisco Packet Tracer»;

– ОС сімейства Microsoft Windows;

Програмне забезпечення «Cisco Packet Tracer» дозволяє емулювати всі основні процеси функціонування реальних комп'ютерних мереж і надає в розпорядження навчанню віртуальну комп'ютерну мережу, в якій і проводяться всі налаштування мережевої інфраструктури, вивчаються мережеві технології і аналізуються деякі з можливих мережевих атак.

При необхідності «Cisco Packet Tracer» може бути замінений на симулятор GNS3 в рамках проведення додаткових факультативних занять або демонстрацій. Це дозволить найбільш глибоко і детально вивчити можливості сучасних мережевих технологій, протоколів і маршрутизаторів.

За лабораторну роботу студент може отримати до 100 балів, з урахуванням своєчасності та якості виконання всіх складових роботи. Складовими є: звіт, проект і відповіді на контрольні питання. Оцінки, отримані за лабораторні роботи, враховуються при виставленні підсумкової оцінки. Для отримання допуску до іспиту всі роботи повинні бути виконані і кожна з них оцінена не менше ніж в 60 балів.

Лабораторна робота № 1.

Захист інфраструктури комутації

Мета роботи:

Метою лабораторної роботи є навчання методам і засобам захисту інфраструктури комутації при використанні технології віртуальних ЛОМ (VLAN), їх налаштування та маршрутизації.

1.1.Короткі теоретичні відомості

Віртуальна ЛОМ або VLAN - широкомовний домен другого рівня. Порти комутаторів, що належать одній VLAN, можуть обмінюватися кадрами між собою, але не можуть обмінюватися кадрами з портами інших VLAN.

Для централізованого управління VLAN на комутаторах може бути використаний протокол VTP.

Для передачі кадрів декількох VLAN між комутаторами використовуються магістральні з'єднання, або транш.

Порти комутаторів, що утворюють магістральний канал, називаються магістральними, або транкові портами. На магістральних портах (на відміну від портів доступу) проводиться ідентифікація та інкапсуляція кадрів VLAN за допомогою протоколів ISL або IEEE 802.1Q.

Для динамічного створення магістрального каналу між комутаторами може використовуватися протокол DTP. Порти комутатора, що передають кадри тільки однієї VLAN, називаються портами доступу (access port). Як правило, за замовчуванням всі порти комутаторів є портами доступу і знаходяться в

VLAN з номером 1, званої власної або стандартної VLAN (native VLAN). Для власних VLAN не застосовуються ніякі протоколи інкапсуляції.

Розрізняють статичні і динамічні VLAN. У статичних VLAN призначення порту здійснюється адміністратором на етапі налаштування комутатора. У динамічних VLAN призначення порту здійснюється по деякому протоколу і, як правило, на основі MAC-адреси вузла мережі. В даний час в основному використовуються статичні VLAN.

Комп'ютери, що знаходяться в різних VLAN можуть обмінюватися даними тільки через маршрутизатор (або будь-яке інше пристрій рівня L3), що має інтерфейси в цих VLAN. Такі VLAN називаються маршрутизованими, інакше - ізольованими.

В даний час рекомендується використовувати наступні принципи при створенні і настройці захищених комутованих ЛОМ:

1. Не використовувати для розповсюдження інформації про використовувані VLAN в ЛОМ протокол VTP (включати режим transparent).

2. В якості протоколу інкапсуляції використовувати протокол IEEE 802.1Q.

3. Заборонити передавати кадри власної VLAN магістральними каналами. В якості native VLAN використовувати спеціально для цього виділену VLAN, яка не використовується ні для яких інших цілей.

4. Не використовувати стандартну VLAN 1 в ЛОМ ні для яких цілей, особливо для управління мережевим обладнанням.

5. На магістральних портах використовувати тільки необхідні VLAN - VLAN, яким належать порти комутаторів на іншій стороні. Всі інші VLAN забороняти.

6. Не використовувати однакові VLAN на різних комутаторах. Найкращий варіант проектування - один комутатор, одна VLAN, одна IP-підмережа.

7. Усі невикористовувані порти комутатора переводити в режим shutdown і призначати їх у спеціально створену для цього не маршрутизовану і ізольовану VLAN.

8. На портах доступу відключати використання протоколу DTP. Для мінімізації часу відновлення функціонування системи при підключенні каналу на магістральних портах встановлювати протокол DTP в режимах On / On і Nonegotiate (відключати погодження).

1.2.Постановка задачі

ЛОМ філії банку побудована на базі двох комутаторів рівня доступу філії Cisco Catalyst 2960 (SW4-2, SW4-3), комутатора рівня ядра-розподілу філії Cisco Catalyst +3560 (SW4-1) і маршрутизатора доступу Cisco 2811 (R4).

Потрібно створити VLAN з номерами для робочих станцій, принтерів і серверів банку відповідно до схеми, представленої на рис. 1, налаштувати маршрутизацію між цими VLAN при їх підключенні до маршрутизатора R4 по магістральному каналу, а також виконати налаштування у відповідності з наведеними вище рекомендаціями.

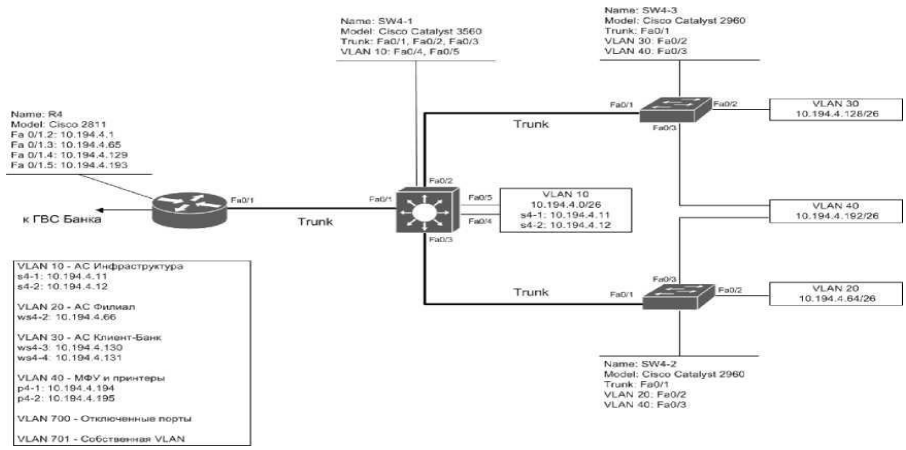

Рисунок 1 – Схема з’єднання обладнання ЛОМ

1.3.Послідовність дій

Крок 1. На комутаторі рівня доступу філії SW4-3 відключити протокол VTP, створити необхідні VLAN, налаштувати магістральний порт і порти доступу комутатора:

```
vtp mode transparent
vlan 30
name AS_Client_Bank
vlan 40
name Service
vlan 700
name unused ports
vlan 701
name native
```

Крок 2. Налаштувати використовувані магістральні порти і порти доступу комутатора SW4-3:

```
interface fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 701
interface fastEthernet 0/2
switchport mode access
switchport nonegotiate
switchport access vlan 30
```

Крок 3. Налаштувати невикористовувані порти комутатора SW4-3, використовуючи можливість вказівки діапазону портів:

```
interface range fastEthernet 0/4-24
switchport mode access
switchport nonegotiate
switchport access vlan 700
shutdown
```

Крок 4. Виконати аналогічні налаштування з урахуванням необхідних VLAN, на комутаторі SW4-2.

Крок 5. На комутаторі рівня ядра-розподілу філії SW4-1 налаштувати магістральні порти для з'єднання з маршрутизатором і комутаторами доступу за схемою магістрального підключення. Виконати налаштування безпеки згідно з наведеними вище рекомендаціями:

```
ip routing
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 701
switchport trunk allowed vlan 10,20,30,40
```

Крок 6. На маршрутизаторі філії R4 створити необхідні VLAN, налаштувати sub-інтерфейси на порту Fa0 / 1 і включити інкапсуляцію по протоколу IEEE 802.1Q:

```
interface fa0/1
no shutdown
no ip address
interface fa0/1.2
encapsulation dot1q 10
ip address 10.194.4.1 255.255.255.192
interface fa0/1.3
encapsulation dot1q 20
ip address 10.194.4.65 255.255.255.192
interface fa0/1.4
encapsulation dot1q 30
ip address 10.194.4.129 255.255.255.192 interface fa0/1.5
```

```
encapsulation dot1q 40
ip address 10.194.4.193 255.255.255.192
```

Крок 7. Перевірити доступність серверів АС з робочих станцій, досліджувати формат кадрів, що передаються по магістральному каналу між комутатором ядра-розподілу і маршрутизатором. Переконатися в неможливості взаємодії з серверами АС з VLAN 700.

Крок 8. Переконатися, що кадри native VLAN НЕ інкапсулюються протоколом IEEE 802.1q при їх передачі по магістральному каналу.

1.4.Запитання і завдання

1. Пояснити рекомендації по налаштуванню механізмів захисту віртуальних ЛОМ.
2. Реалізувати в ЛОМ атаку типу «VLAN hopping» при налаштуванні різних власних VLAN на транкових портах, що з'єднують комутатори.
3. Налаштувати розповсюдження бази даних VLAN через протокол VTP відповідно до рекомендованими параметрами.
4. Налаштувати термінування і маршрутизацію VLAN на комутаторі рівня ядра-розподілу ЛОМ.

1.5.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

1.6.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 2.

Захист ЛОМ від петель на канальному рівні

Мета роботи:

Метою лабораторної роботи є вивчення методів і засобів побудови, захисту та оптимізації відмовостійких ЛОМ на основі протоколу STP.

2.1.Короткі теоретичні відомості

Протоколи та механізми оптимізації та захисту сімейства STP призначені для запобігання петель (циклів) в мережах з множинними маршрутами на канальному рівні ЛОМ. За рахунок обміну службовими BPDU-кадрами комутатори, на яких запущений протокол STP, будують топологію, в якій між будь-якими двома комутаторами існує тільки один активний в даний момент маршрут на канальному рівні.

В даний час сімейство протоколів STP включає протоколи та механізми IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1t, а також розширення Cisco Spanning Tree Toolkit.

Одним з основних елементів протоколу STP є кореневий комутатор. Некоректний вибір кореневого комутатора, викликаний помилками конфігурування обладнання або атаками порушників, може призвести до порушення штатного функціонування мережевої інфраструктури або перенаправлення і перехопленню інформаційних потоків на канальному рівні.

В даний час використовуються наступні принципи при проектуванні, настройці і оптимізації протоколів сімейства STP.

1. Використовувати протоколи сімейства STP з метою побудови відмовостійких ЛОМ тільки при необхідності. По можливості для забезпечення відмовостійкості та високої доступності ЛОМ використовувати механізми і протоколи маршрутизації мережевого рівня.

2. Застосування протоколу STP є обов'язковим у разі передачі даних в одній і тій же віртуальної ЛОМ, організованою на різних комутаторах, а також для захисту від дій користувачів на портах доступу комутаторів ЛОМ і помилок обслуговуючого персоналу.

3. У сімействі протоколів STP рекомендується використовувати протокол Rapid-PVST +.

4. Адміністративно визначати і призначати кореневі комутатори. Використовувати додаткові механізми та засоби захисту протоколу STP (Root Guard, Loop Guard,

UplinkFast, UDLD) для запобігання отримання ролі кореневого комутатора іншими комутаторами.

5. На портах доступу комутаторів ЛОМ виконувати налаштування щодо запобігання можливості появи або фільтрації BPDU-пакетів протоколу STP (механізми BPDU Guard і BPDU Filter відповідно), а також виконувати налаштування для швидкого включення і захисту кореневого комутатора (механізми PortFast і Root Guard відповідно).

2.2.Постановка задачі

На комутаторах ЛОМ філії банку виконати налаштування протоколу STP і механізмів його захисту. Побудована ЛОМ повинна забезпечувати стан доступності при відмові:

- одного з комутаторів SW7-1 або SW7-2;
- активного комутованого порту маршрутизатора R7;
- однієї з ліній зв'язку каналу EtherChannel;
- активного порту лінії зв'язку між комутатором рівня доступу і комутатором рівня ядра-розподілу.

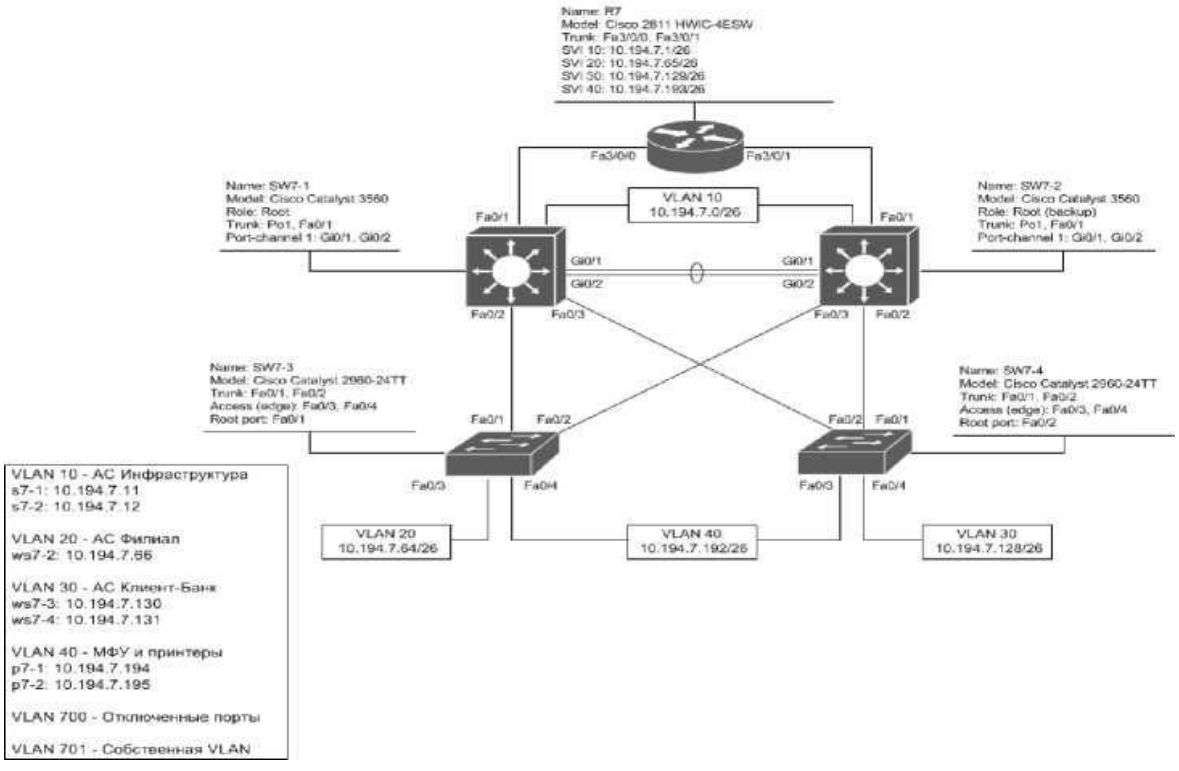

Рисунок 2 – Схема з’єднання комутаторів відказостійкої ЛОМ

2.3.Послідовність дій

Крок 1. Побудувати схему логічного з'єднання комутаторів ЛОМ і знайти можливі цикли на канальному рівні (див. Рис. 2). Визначити оптимальне положення кореневого комутатора відповідно до маршрутами інформаційних потоків.

Крок 2. До маршрутизатора R7 в слот № 3 підключити модуль HWIC-4ESW, що забезпечує наявність додаткових чотирьох комутованих Ethernet-портів. Створити на комутуючих модулі маршрутизатора віртуальні ЛОМ і для кожної з них налаштувати інтерфейс SVI, що забезпечує маршрутизацію віртуальних ЛОМ:

```
vlan database
vlan 10 name Servers
vlan 20 name AS_Filial
vlan 30 name AS_Client_Bank
vlan 40 name Service
interface vlan10
ip address 10.194.7.1 255.255.255.192
interface vlan20
ip address 10.194.7.65 255.255.255.192
 interface vlan30
ip address 10.194.7.129 255.255.255.192
interface vlan40
ip address 10.194.7.193 255.255.255.192 i
nterface fastEthernet 3/0/0
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701
interface fastEthernet 3/0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701
```

Крок 3. На комутуючу модулі маршрутизатора R7 настро-іть протокол Rapid-PVST для необхідних VLAN:

```
spanning-tree mode rapid-pvst
```

Крок 4. Між комутаторами SW7-1 і SW7-2 налаштувати агрегування двох каналів передачі даних за технологією Etherchannel:

```
interface GigabitEthernet0/1
channel-protocol lacp
channel-group 1 mode on
interface GigabitEthernet0/2
channel-protocol lacp
channel-group 1 mode on
interface port-channel 1
no shutdown
switchport mode trunk
switchport trunk native vlan 701
switchport trunk allowed vlan 10,20,30,40
```

Крок 5. На комутаторі SW7-1 налаштувати протокол Rapid-PVST для необхідних віртуальних ЛОМ і задати найвищий пріоритет комутатора, забезпечивши йому роль кореневого моста в зазначених VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root primary
```

Крок 6. На комутаторі SW7-2 налаштувати протокол Rapid-PVST для необхідних VLAN і задати найвищий пріоритет комутатора, забезпечивши йому роль кореневого моста в зазначених VLAN в разі виходу з ладу комутатора SW7-1:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root secondary
```

Крок 7. На комутаторах SW7-1 і SW7-2 налаштувати механізм Root Guard:

```
interface range fa0/2-3
spanning-tree guard root
```

Крок 8. На комутаторах SW7-3 і SW7-4 налаштувати протокол Rapid-PVST для необхідних VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 20,30,40,701
```

Крок 9. На портах доступу комутаторів SW7-3 і SW7-4 налаштувати протокол STP в режимі portfast, включити механізми захисту BPDU Guard:

```
interface range fa0/3-4
switchport mode access
```

```
spanning-tree bpduguard enable
spanning-tree portfast
```

Крок 10. Переконатися в коректності настройки протоколу STP на комутаторах ЛОМ. Перевірити можливість функціонування мережі при відключенні порту Fa0 / 0/1 маршрутизатора R7, при відключенні порту Gi0 / 1 комутатора SW7-1, при відключенні Комутатора SW7-1 або при відключенні порту Fa0 / 1 комутатора SW7-3.

2.4.Запитання і завдання

1. Пояснити відмінності в роботі між механізмами BPDU Guard, BPDU Filter і Root Guard. Описати області застосування і призначення кожного з цих механізмів захисту.

2. Пояснити вибір портів активації механізму Root Guard на комутаторах рівня ядра-розподілу філії.

3. Розробити проект впровадження механізму Loop Guard для захисту ЛОМ від утворення односпрямованих каналів зв'язку.

4. Змоделювати DoS-атаку на мережеву інфраструктуру при підключенні до ЛОМ комутатора з найменшим значенням параметра BID.

5. Змоделювати атаку типу BPDU spoofing на протокол STP шляхом підключення до ЛОМ комутатора порушника та отримання ним ролі кореневого моста.

2.5. Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

2.6. Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 3.

Захист ЛОМ від атак канального рівня

Мета роботи:

Метою лабораторної роботи є вивчення методів проектування, розгортання і налаштування механізмів захисту в комутованих ЛОМ від атак канального рівня типу MAC-flooding і MAC-spoofing.

3.1. Короткі теоретичні відомості

Одним з механізмів захисту ЛОМ від атак є механізм port security, реалізований на комутаторах. Механізм port security дозволяє здійснювати фільтрацію кадрів, що надходять на окремі порти комутатора ЛОМ, на основі MAC-адреси джерела.

При активізації даного захисного механізму на порту комутатора створюється список асоційованих (дозволених) з ним MAC-адрес. Кадри, що надходять на порт комутатора з активізованою функцією port security, MAC-адреси яких не належать даному списку, знищуються. При цьому сам порт комутатора може переходити в режим shutdown.

Існує два методи побудови списку дозволених MAC- адрес - метод статичного призначення та метод динамічного вивчення.

Метод статичного призначення дозволених MAC-адрес застосовується на комутаторах доступу ДМЗ, центрів обробки даних і т. Д. При цьому на порту комутатора зазначається конкретний MAC-адресу.

Метод динамічного вивчення адрес визначає максимальну кількість MAC-адрес, асоційованих комутатором з портом протягом деякого часу. Такий спосіб побудови таблиці адрес, як правило, застосовувати на рівні доступу ЛОМ або в мережах філій.

При порушенні безпеки - при вступі на захищається порт комутатора кадру із забороненим MAC-адресою - можлива одна з трьох подій: порт відключається (режим захисту shutdown), кадр відкидається комутатором (режим захисту protect), кадр відкидається комутатором, збільшується лічильник порушень порту і генерується SNMP-повідомлення (режим захисту restrict).

У динамічно змінюваної мережевій інфраструктурі рекомендується обмежуватися одним MAC-адресою для порту комутатора і використовувати режим protect, в серверних групах - статично задавати списки MAC-адрес і використовувати режим shutdown, в VoIP-сегментах - обмежуватися двома або трьома MAC-адресами з активізацією режиму restrict .Додатковим механізмом формування списку MAC- адрес є механізм sticky. Він дозволяє

додати статично задані або динамічно вивчені MAC-адреси в конфігураційний файл ОС комутатора.

3.2. Постановка задачі

У сегменті ЛОМ філії (див. Рис. 3), побудованому на базі двох комутаторів рівня доступу Cisco Catalyst +2960 і комутатора рівня ядра-розподілу Cisco Catalyst 3560, забезпечити захист від атак типу MAC-flooding і MAC-spoofing.

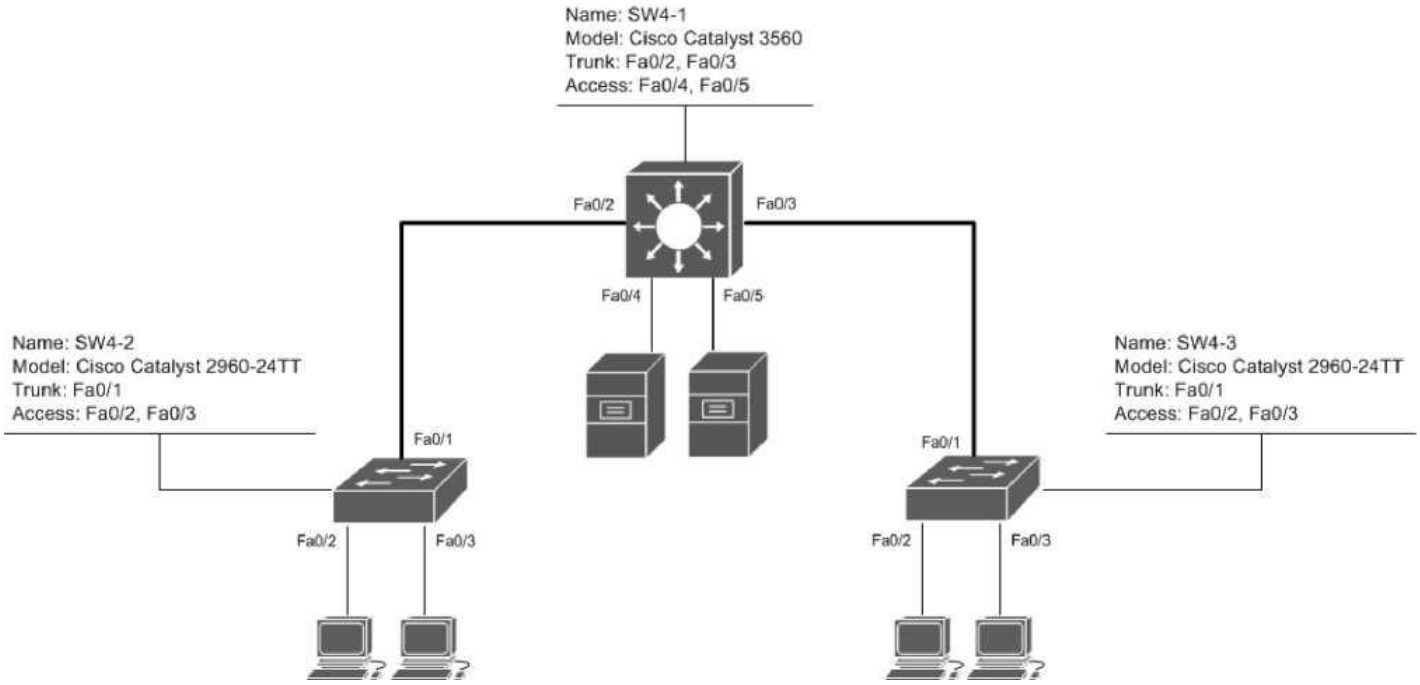

Рисунок 3 – Схема з’єднання обладнання до ЛОМ філії банку

3.4. Послідовність дій

Крок 1. На комутаторі рівня доступу SW4-3 налаштувати механізм port security в динамічному режимі для робочих станцій:

```
interface range fa0 / 2-3
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation protect
```

Крок 2. виконати аналогічні налаштування механізму port security на комутаторі SW4-2.

Крок 3. На комутаторі рівня ядра-розподілу SW4-1 налаштувати механізм port security в статичному режимі з прив'язкою до заданого MAC-адресою для порту FastEthernet0 / 4:

```
interface fa0/4
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security   mac-address
xxxx.yyyy.zzzz
switchport port-security violation shutdown
```

Крок 4. На комутаторі рівня ядра-розподілу SW4-1 налаштувати механізм port security в статичному режимі з опцією sticky для порту FastEthernet0 / 5:

```
interface fa0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

Крок 5. Перевірити коректність налаштувань механізму безпеки port security комутаторів ЛОМ шляхом моделювання атаки типу MAC-spoofing. Задати MAC-адресу робочої станції, підключеної до порту комутатора зі статичним методом формування списку MAC-адрес, невідповідний вимогам політики безпеки. Переконатися в перекладі порту комутатора в режим shutdown або protect.

Крок 5. Перевірити коректність налаштувань механізму безпеки port security комутаторів ЛОМ шляхом моделювання атаки типу MAC-flooding. На порт комутатора з динамічним методом формування списку дозволених MAC-адрес підключити комутатор з декількома робочими станціями. Переконатися в перекладі порту комутатора в режим shutdown або protect.

3.5. Запитання і завдання

1. Описати призначення і принцип роботи механізму port security sticky для статичного методу формування MAC- адрес.

2. Пояснити рекомендацію завдання максимальної кількості MAC-адрес на порту комутатора з динамічним методом формування списку з двох або трьох дозволених MAC-адрес.

3. Чи можливе застосування механізму port security для захисту від атак типу ARP spoofing і DHCP spoofing?

3.6.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

3.7.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 4.
Побудова маршрутизованої ЛОМ

Мета роботи:

Метою лабораторної роботи є навчання методам побудови і налаштування маршрутизованої ЛОМ з високою доступністю на основі протоколу маршрутизації OSPF.

4.1.Короткі теоретичні відомості

Архітектура сучасних корпоративних ЛОМ повинна володіти наступними основними властивостями: ієрархічність, модульність, стійкість і масштабованість. Класична ієрархічна модель ЛОМ складається з трьох рівнів ядра, розподілу (агрегування) і доступу. У сучасних корпоративних ЛОМ, як правило, можна виділити блок розподілу і блок сервісів, що об'єднуються ядром мережі. Від правильного проектування блоку розподілу залежить стабільність і коректність роботи всієї ЛОМ.

В даний час основними варіантами архітектури блоку розподілу є багатоланкова архітектура (multitier), архітектура з маршрутизованим доступом (routed access) та архітектура з віртуальною комутацією. Підходи різняться в кордоні між рівнями реалізації, використовуваними мережевими технологіями і протоколами рівнів L2 і L3, а також можливостями в реалізації відмовостійкості, надмірності і балансування навантаження.

Альтернативою традиційному блоку розподілу з класичною багатоланкової архітектурою служить архітектура блоку розподілу з реалізацією функцій маршрутизації на рівень доступу, що дозволяє побудувати повністю маршрутизовані ЛОМ. У такій архітектурі комутатори доступу функціонують як пристрої третього рівня, магістральні канали між комутаторами рівнів доступу і розподілу замінені маршрутизованими каналами рівня L3.

Таким чином, кордон сполучення мережевих рівнів L2 і L3 переміщена в ієрархії ЛОМ з рівня розподілу на рівень доступу. При цьому на всіх комутаторах доступу створюються унікальні віртуальні ЛОМ, для яких шлюзами є комутатори доступу.

Створення стандартного маршрутизатора для кожної віртуальної ЛОМ на комутаторі доступу виконується через механізм Switch Virtual Interface (SVI). Для забезпечення високої доступності використовуються механізми маршрутизації, а не спеціалізовані протоколи сімейств FHRP і STP.

Даний підхід містить суттєві переваги порівняно з класичним підходом: простота проектування та реалізації, простота відладки і управління, єдині механізми відновлення та управління.

При проектуванні і конфігуруванні маршрутизованих ЛОМ на основі протоколу OSPF використовуються такі основні принципи:

1. Створення дворівневої моделі маршрутизації магістраль (область 0), реалізована в ядрі мережі, і решта областей, реалізовані в сегментах мережі, підключених до магістралі через комутатори рівня розподілу. Останні виступають як прикордонних маршрутизаторів області. Обмеження розсилки OSPF-повідомлень шляхом визначення і настройки пасивних інтерфейсів на комутаторах рівня доступу.

2. Наявність L3-з'єднання між комутаторами рівня розподілу, а також між комутаторами рівня доступу та рівня розподілу. Використання трикутних топологій між рівнями доступу, розподілу і ядра.

3. Зменшення кількості поширюваних OSPF-повідомлень про стан зв'язків і розміру таблиць маршрутизації шляхом визначення і настройки тупикових і повністю тупикових областей, а також шляхом виконання підсумовування маршрутів на прикордонних маршрутизаторах.

Гідності повністю маршрутизованих ЛОМ:

- простота реалізації та супроводу;
- наявність розвинених засобів діагностики та усунення несправностей;
- висока швидкість і передбачуваність відновлення після відмов;
- уніфікація засобів і механізмів побудови всіх рівнів.

Основною вимогою для забезпечення можливості побудови маршрутизуються ЛОМ є наявність на всіх комутаторах унікальних VLAN.

Постановка задачі

Виконати налаштування комутаторів ЛОМ банку, що забезпечують реалізацію архітектури повністю маршрутизуються ЛОМ з високою доступністю.

4.2.Послідовність дій

Крок 1. Побудувати мережу, у відповідності зі схемою маршрутизації, представленої на рис. 4. При необхідності ввести необхідні елементи і включити додаткові механізми. Виконати налаштування інтерфейсу SVI на комутаторі рівня доступу SW8:

```
vlan 192
interface vlan192
ip address 10.194.192.1 255.255.255.0
```

```
interface fastEthernet 0/10
switchport access vlan 192
```

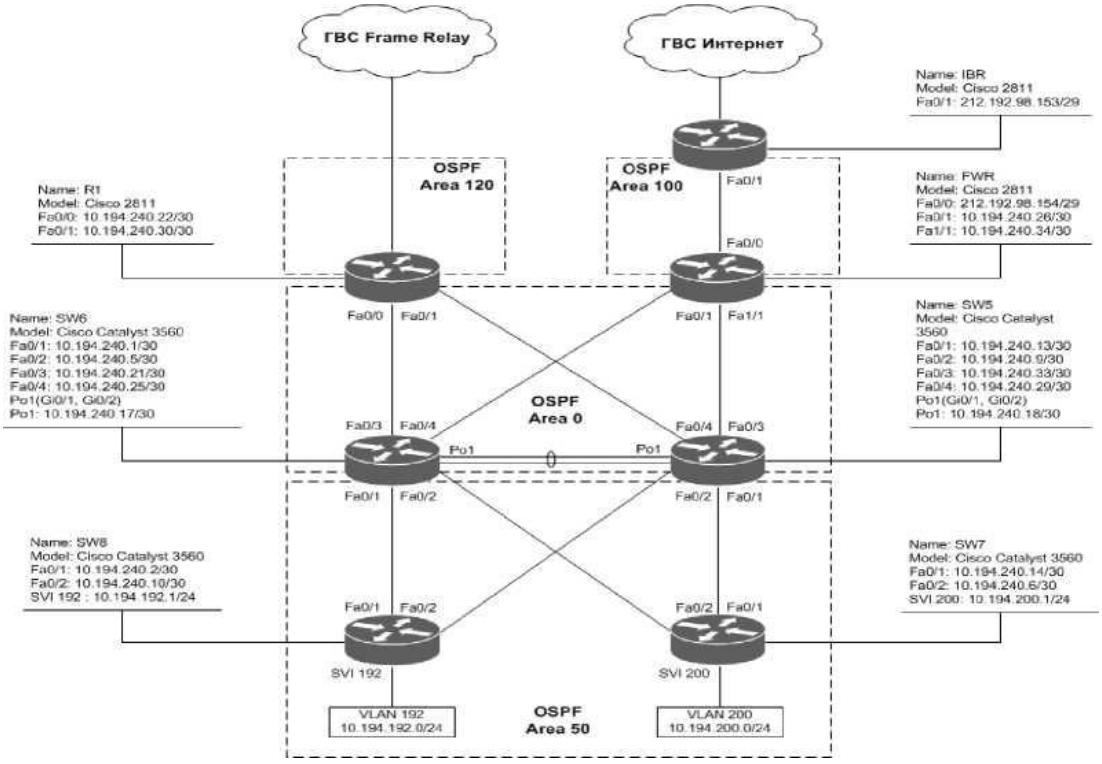

Рисунок 4 – Схема маршрутизації в ЛОМ

Крок 2. Виконати налаштування протоколу маршрутизації OSPF на комутаторі рівня доступу SW8, забезпечивши аутентифікацію сусідів і ініціалізацію пасивних інтерфейсів:

```
router ospf 10
log-adjacency-changes
area 50 stub
passiveinterface default
no passive-interface fastEthernet 0/1
no passive-interface fastEthernet 0/2
network 10.194.0.0 0.0.255.255 area 50
interface fastEthernet 0/1
no switchport
ip address 10.194.240.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 10 md5 H4&hdn3&
interface fastEthernet 0/2
```

```
no switchport
ip address 10.194.240.10 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 10 md5 H4&hdn3&
```

Крок 3. Виконати аналогічні налаштування на комутаторі рівня доступу SW7 згідно зі схемою, представленої на рис. 4.

Крок 4. Виконати налаштування протоколу маршрутизації OSPF на комутаторі рівня ядра-розподілу SW5, забезпечивши аутентифікацію сусідів, ініціалізацію пасивних інтерфейсів аутентифікації сусідів і повністю тупикових областей. Для останньої виконується настройка:

```
router ospf 10
area 50 stub no-summary
```

Крок 5. Виконати аналогічні налаштування на комутаторі рівня ядра-розподілу SW6.

Крок 6. Виконати аналогічні налаштування протоколу маршрутизації OSPF на маршрутизаторах R1, IBR і FWR. На прикордонному маршрутизаторі автономної системи IBR додатково налаштувати оголошення зовнішнього маршруту в OSPF-систему:

```
router ospf 10
network 212.192.98.152 0.0.0.7 area 100
default-information originate
```

Крок 7. Перевірити доступність всіх вузлів і відмовостійкість ЛОМ.

Крок 8. Переконатися в проходженні пакетів за різними альтернативних маршрутах (технологія ECMP). Виконати налаштування по зміні вартості інтерфейсів комутаторів так, щоб всі IP-пакети проходили тільки через комутатор SW5, а при його відмові через комутатор SW6. Переконатися в проходженні пакетів по одному маршруту:

```
interface fastEthernet 0/2
ip ospf cost 2
```

4.3.Запитання і завдання

1. Визначити в схемі маршрутизації ЛОМ механізми та засоби забезпечення відмовостійкості і масштабування.

2. Які складнощі можуть виникнути в процесі реалізації політик безпеки (між мережевому екрануванні, організації VPN) при побудові маршрутизованих ЛОМ?

3. Змоделювати процес асиметричною маршрутизації ЛОМ. Яким вимогам повинні задовольняти засоби захисту інформації за підтримки асиметричною маршрутизації?

4.4.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

4.5.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 5.

Захист мережевої інфраструктури

Мета роботи:

Метою лабораторної роботи є вивчення методів і засобів захисту мережевої інфраструктури від НСД, а також принципів проектування мереж управління.

5.1. Короткі теоретичні відомості

Для захисту пристроїв мережевої інфраструктури від НСД, забезпечення її стійкості і безвідмовного функціонування використовуються такі основні налаштування безпеки:

1. Відключення невикористовуваних протоколів, мережевих служб і механізмів (DNS, CDP, TELNET, DHCP, FINGER, ECHO, маршрутизація від джерела, proxy-arp, ICMP redirect, ICMP mask- reply та ін.).

2. Налаштування планувальника завдань для забезпечення можливості передачі ресурсів процесам управління.

3. Обмеження доступу до мережевої інфраструктури тільки з мережі управління або з автоматизованих робочих місць адміністраторів.

4. Забезпечення синхронізації часу на всіх пристроях для коректного аналізу подій (у тому числі і подій безпеки). Для цього налаштовується синхронізація часу із зовнішнім джерелом по протоколу NTP з аутентифікацією пакетів.

5. Повідомлення і збереження інформації про збої (SNMP, SYSLOG, автоматичне збереження файлів crashinfo, створюваних ОС при фатальних збоях апаратного або програмного забезпечення).

6. Попередження осіб, які підключилися до пристрою, про заборону тих чи інших дій. Для цього на всіх пристроях налаштовується видача попереджуючого повідомлення про заборону НСД до даного пристрою. Реєстрація та облік для всіх видів доступу. Реєстрація осіб, які здійснюють доступ до пристрою, виконуваних ними дій і часу для подальшого аудиту.

7. Дозвіл управління пристроєм лише по захищених протоколам типу SSH і SNMP з вузлів мережі управління і встановленням обмежень на тривалість сесій.

8. Налаштування механізмів парольного захисту: використання стійких паролів, включення хешування та шифрування паролів.

В архітектурі мереж з високим рівнем безпеки, як правило, виділена будується мережа управління, що виконує окремі функції передачі інформаційних потоків рівня управління. Мережа управління, що використовує фізично виділені канали, називається мережею поза смугового управління (out-of-band network). Мережа управління, що використовує канали передачі даних, називається мережею внутрішньо полосного управління (in-band network).

Як правило, мережа поза смугового управління будується в корпоративних ЛОМ та ЦОД. При цьому використовуються виділені, віртуальні комутатори і маршрутизатори.

Мережі внутрішньо полосного управління використовуються для управління мережами філій і зовнішніми пристроями периметра. При побудові мереж управління активно використовуються сучасні технології віртуалізації мереж - технології VLAN, VRF, path isolation, механізми MPLS.

5.2. Постановка задачі

Організувати управління мережним устаткуванням філії з мережі поза смугового управління. Виконати налаштування щодо забезпечення захисту маршрутизаторів СПД. Для централізованого управління доступом адміністраторів до мережевого обладнання банку використовувати технологію AAA.

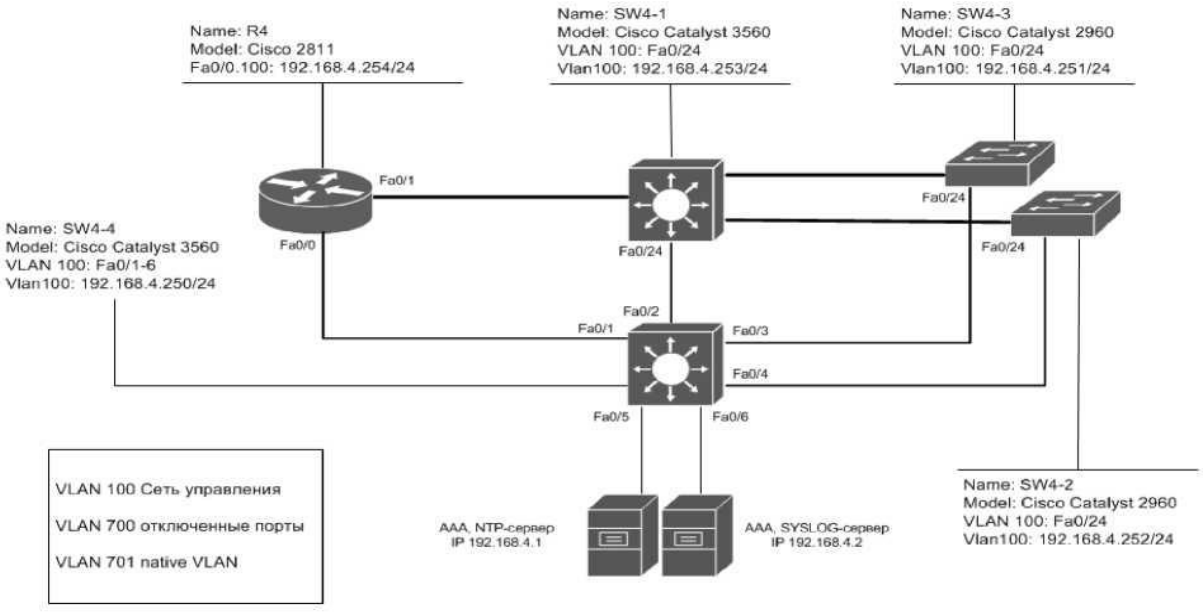

Рисунок 4 – Мережа управління ЛОМ

5.3. Послідовність дій

Крок 1. Підключитися до маршрутизатора R4 через консольний порт з робочої станції адміністратора мережі.

Крок 2. Поставити ім'я маршрутизатора і домен. Згенерувати криптографічні ключі, використовувані в криптографічному протоколі SSH, для чого задати ім'я вузла мережі і домен:

```
hostname R4
ip domain-name net.bank
crypto key generate rsa
```

Крок 3. Включити доступ до маршрутизатора по протоколу SSHv2, задати кількість спроб аутентифікації:

```
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
```

Крок 4. Налаштувати видачу попереджуючого повідомлення про підключення до мережного обладнання:

```
banner login #
**************************************************
*       Bank Router
*       UNAUTHORIZED ACCESS IS PROHIBITED     *
*       You have accessed network equipment.  *
*       You must have authorized permission to access     *
 *      or configure this device. All activities          *
 *      performed on this device are monitored and        *
 *      logged.                                           *
**************************************************#
```

Крок 5. Створити локального користувача і встановити пароль на доступ до конфігураційного режиму:

```
username noc secret 5 *jfl(jf33aq
enable secret Kmme5bb$
```

Крок 6. Відключити служби DNS і CDP, включити шифрування паролів в конфігураційному файлі:

```
no ip domain-lookup
no cdp run
service password-encryption
```

Крок 7. Виконати налаштування доступу до маршрутизатора по технології AAA на основі протоколу TACACS +:

```
tacacs-server host 192.168.4.1 key 8t8Gd2k1;p
tacacs-server host 192.168.4.2 key r38voa8feq
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
```

Крок 8. Налаштувати віддалений доступ до маршрутизатора за дозволених IP-адрес робочих станцій мережі управління філії:

```
ip access-list extended iacl-vty
permit tcp 192.168.4.0 0.0.0.63 any eq 22
deny ip any any
line con 0
exec-timeout 5 0
login authentication default
line vty 0 15
exec-timeout 10 0
transport input ssh
access-class iacl-vty in
```

Крок 9. Виконати налаштування служби реєстрації подій та їх відправки на сервер реєстрації подій філії (IP-адреса 192.168.4.2) по протоколу SYSLOG:

```
service timestamps log datetime msec
service timestamps debug datetime msec
logging 192.168.4.2
logging trap debugging
logging buffered 512000
```

Крок 10. Виконати налаштування протоколу SNMP для доступу до маршрутизатора з сервера моніторингу:

```
snmp-server community Hn4bUn3ba ro
snmp-server community mf5FNOd2d rw
```

Крок 11. Виконати налаштування протоколу NTP для синхронізації часу з сервером точного часу (IP-адреса 192.168.4.1):

```
ntp authenticate
```

```
ntp authentication-key 1 md5 Yghd6qh2!
ntp trusted-key 1
ntp server 192.168.4.1 key 1
```

Крок 12. Виконати налаштування комутаторів ЛОМ філії для підключення до мережі поза смугового управління відповідно до схеми, представленої на рис. 6. На комутаторах налаштувати віртуальний інтерфейс типу SVI:

```
interface vlan100
ip address 192.168.4.250 255.255.255.0
no shutdown
ip default-gateway 192.168.4.254
```

Крок 13. На маршрутизаторі R4 виконати налаштування щодо обмеження доступу до мережі управління з ЛОМ передачі даних:

```
ip access-list extended iacl-in-management
permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
deny ip any any
ip access-list extended iacl-out-management
permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255
deny ip any any
interface fa0/0.100
encapsulation dot1q 100
ip access-group iacl-out-management out
ip access-group iacl-in-management in
```

Крок 14. Перевірити коректність функціонування мережі управління, а також реєстрацію подій на сервері SYSLOG.

5.4. Запитання і завдання

1. У мережі однієї з філій банку побудувати мережу внутрішньо порожнинного управління.

2. Переконатися в неможливості доступу в мережу управління з ЛОМ передачі даних і навпаки.

5.5. Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

5.6.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 6.

Захист периметра мережі

Мета роботи:

Метою лабораторної роботи є вивчення основних технологій між мережевого екранування, методів і засобів управління безпекою інформаційних потоків на між мережевих екранах і мережевих маршрутизаторах.

6.1. Короткі теоретичні відомості

Брандмауер - апаратний, програмно-апаратний або програмний комплекс, який реалізує функції управління, контролю та фільтрації мережевих інформаційних потоків між двома і більше АС по деякому набору правил, що визначаються політикою безпеки.

Брандмауери поділяються на різні типи залежно від наступних характеристик:

1. Забезпечується з'єднання між одним вузлом і мережею або між двома або більше різними мережами;

2. Відбувається контроль потоку даних на мережевому рівні або більш високих рівнях еталонної моделі 180/081;

3. Відслідковується стан активних з’єднань чи ні.

Залежно від охоплення контрольованих потоків даних брандмауера, як правило, поділяються на:

1. Традиційні брандмауери, які зазвичай являють собою спеціалізований пристрій або комп'ютер, розміщений на кордоні двох або більше мереж. Такі типи екранів контролюють вхідні і вихідні потоки даних в кожній з підключених мереж;

2. Персональні брандмауери - програмні або модулі антивірусного ПЗ, що встановлюються на окремому комп'ютері і призначені для захисту тільки цього комп'ютера від несанкціонованого доступу.

Залежно від рівня, на якому відбувається управління доступом, існує поділ на:

1. Брандмауери, що працюють на мережному рівні, коли фільтрація відбувається на основі мережевих адрес відправника і одержувача пакетів, номерів портів транспортного рівня і статичних правил, заданих адміністратором;

2. Брандмауери, що працюють на рівні додатків, які здійснюють контроль за переданими даними на більш високих рівнях моделі ОБІ. Такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації в залежності від прийнятої адміністратором політики та налаштувань пристрою. Такі типи МО зазвичай

працюють у режимі проксі-сервера різних додатків, а не маршрутизації на мережевому рівні.

Залежно від реалізації можливості відстеження активних сполук брандмауери бувають:

1. Без інспекції станів - не відслідковують поточні з'єднання (наприклад, TCP), а фільтрують потік даних виключно на основі статичних правил;

2. З інспекцією станів - з відстеженням поточних з'єднань і пропуском тільки таких пакетів, які задовольняють логіці і алгоритмам роботи відповідних протоколів і додатків. Дані брандмауера дозволяють ефективніше боротися з різними типами DoS-атак і вразливостям деяких мережевих протоколів. Крім того, вони забезпечують функціонування таких протоколів, як H.323, SIP, FTP, що використовують складні схеми передачі даних між вузлами, погано піддаються опису статичними правилами, і найчастіше несумісні зі стандартними МО без інспекції станів.

Додатковими механізмами захисту і управління інформаційними потоками, реалізованими, як правило, в брандмауерах, є технології NAT, AAA, VPN і IDPS.

Технологія NAT застосовується як для забезпечення доступу вузлів з немаршруттзовані адресами до ГВП Інтернет, так і для реалізації механізмів захисту мережі, наприклад, для ізоляції мереж управління або проходження пакетів через VPN-шлюз.

Існують наступні види NAT: динамічна трансляція адрес на рівні портів, динамічна трансляція на рівні портів з вибіркою IP-адрес, трансляція з динамічною вибіркою IP-адрес і статична трансляція.

6.2. Постановка задачі

Налаштувати правила управління доступом серверів і робочих станцій з ЛОМ в мережу Інтернет і з неї до серверів АС, розташованих в ДМЗ згідно табл. 1. Реалізувати механізм первинної фільтрації пакетів на прикордонному маршрутизаторі IBR. Доступ в мережу Інтернет з мережі 10.194.200.0/24 здійснюється по технології NAT.

Таблиця 1- Політика безпеки управління мережевими потоками інформації

№	Джерело	Призначення	Правило
1	Мережа 10.194.192.0/24	Інтернет	Заборонити
2	Мережа 10.194.200.0/24	Інтернет	NAT
3	Мережа 10.194.200.0/24	Недовірені DNS-сервера	Заборонити
4	Мережа 10.194.200.0/24	Інтернет, протокол HTTP	Дозволити
5	Проксі-сервер №-адрес 10.194.210.10	Зовнішній DNS-сервер IP-адрес 212.192.98.162, протокол	Дозволити
6	Термінальний сервер №-адрес 10.194.210.11	Зовнішній DNS-сервер IP-адрес 212.192.98.162, протокол DNS	Дозволити
7	Проксі-сервер №-адрес 10.194.210.10	Інтернет, протокол HTTP	Дозволити, через NAT
8	Термінальний сервер №-адрес 10.194.210.11	Інтернет, протокол HTTP	Дозволити через PAT
9	DNS-сервер №-адрес 212.192.98.162	Інтернет, протокол DNS	Дозволити
10	DNS-сервер №-адрес 212.192.98.162	Інтернет	Заборонити
11	Веб-сервер №-адрес 212.192.98.163	Інтернет	Заборонити
12	Мережа Інтернет	IP-адрес 212.192.98.162, протокол DNS	Дозволити
13	Мережа Інтернет	IP-адрес 212.192.98.163, протокол HTTP	Дозволити
14	Будь-яка Мережа	Будь-яка Мережа	Заборонити

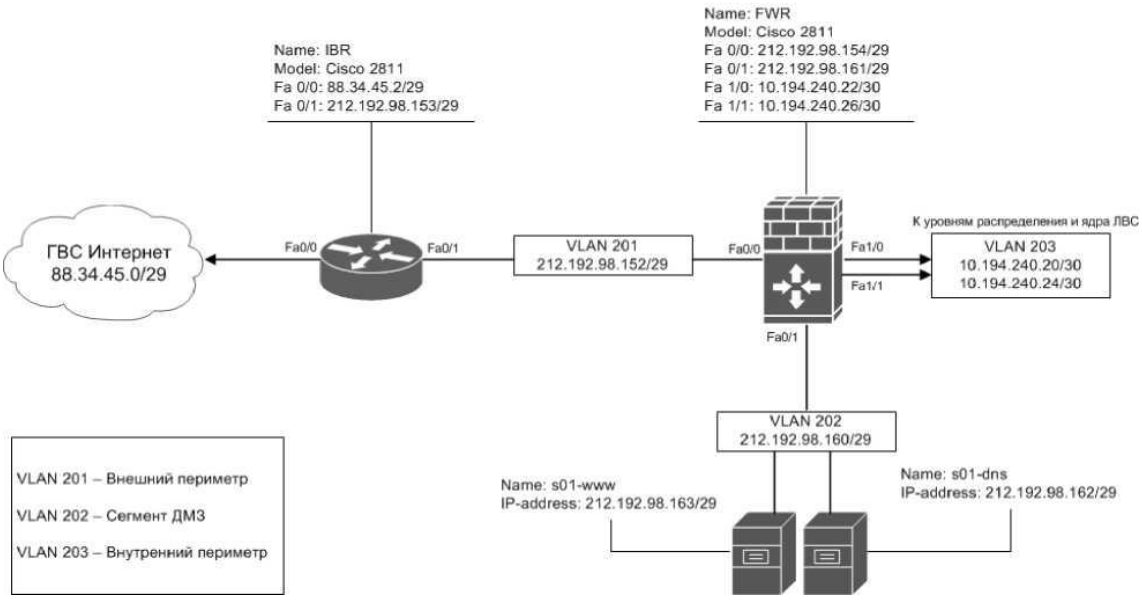

Рисунок 6 –Схема периметри Інтернет

Доступ з мережі 10.194.192.0/24 в Інтернет заборонений і здійснюється через термінальний сервер s01-term (IP-адреса 10.194.210.11). Додатково в ЛОМ існує проксі-сервер s01 -proxy (IP- адреса 10.194.210.10). Для реалізації технології NAT виділяються IP-мережі 212.192.98.168/29 і 212.192.98.154/32 відповідно. У сегменті ДМЗ розташовані DNS-сервер s01-dns (IP-адреса 212.192.98.162) і WWW-сервер s01-www (IP-адреса 212.192.98.163). Налаштувати політику управління доступом до даних серверів на основі порядку функціонування WWW- і DNS-служб.

6.3. Послідовність дій

Крок 1. Побудувати сегмент периметра Інтернет відповідно до схеми, представленої на рис. 6.

Крок 2. Налаштувати IP-інтерфейси, VLAN і маршрутизацію по протоколу OSPF.

Крок 3. Виконати налаштування технології трансляції адрес на екранувальній маршрутизаторі FWR:

```
ip nat pool pool-net200 212.192.98.169 212.192.98.174 netmask 255.255.255.248
ip access-list standard acl-nat
permit 10.194.200.0 0.0.0.255
pertmit host 10.194.210.10
ip access-list standard acl-pat
permit host 10.194.210.11
ip nat inside source list acl-nat pool pool- net200
ip nat inside source list acl-pat interface fa0/0
interface fal/1
ip nat inside
interface fal/0
ip nat inside
interface fa0/0
ip nat outside
```

Крок 4. Налаштувати фільтрацію інформаційних потоків в відповідної з табл. 1:

```
ip access-list extended acl-LAN
deny ip 10.194.192.0 0.0.0.255 any
deny tcp 10.194.200.0 0.0.0.255 any eq 53
deny udp 10.194.200.0 0.0.0.255 any eq 53
```

```
permit     udp  host 10.194.210.10   host 212.192.98.162   eq 53
permit     tcp  host 10.194.210.10   host 212.192.98.162   eq 53
permit     udp  host 10.194.210.11   host 212.192.98.162   eq 53
permit     tcp  host 10.194.210.11   host 212.192.98.162   eq 53
deny tcp host 10.194.210.10 any eq 53
deny udp host 10.194.210.10 any eq 53
deny tcp host 10.194.210.11 any eq 53
deny udp host 10.194.210.11 any eq 53
permit tcp 10.194.200.0 0.0.0.255 any eq 80
permit tcp host 10.194.210.11 any eq 80
deny ip any any
ip access-list extended acl-DMZ
permit tcp host 212.192.98.162 any eq 53
permit udp host 212.192.98.162 any eq 53
deny ip host 212.192.98.163 any
deny ip any any
ip access-list extended acl-INTERNET
permit tcp any host 212.192.98.162 eq 53
permit udp any host 212.192.98.162 eq 53
permit tcp any host 212.192.98.163 eq 80
deny ip any any
interface fa0/0
ip access-group acl-INTERNET in
interface fa0/1
ip access-group acl-DMZ in
interface fa1/0
ip access-group acl-LAN in
 interface fa1/1
ip access-group acl-LAN in
```

Крок 5. Виконати налаштування механізму інспекції станів CBAC на маршрутизаторі FWR:

```
ip inspect audit-trail
ip inspect dns-timeout 15
ip inspect tcp synwait-time 15
```

```
ip inspect tcp finwait-time 20
ip inspect tcp idle-time 120
ip inspect udp idle-time 20
ip inspect name cbac-dmz http
ip   inspect   name  cbac-dmz   tcp
ip   inspect   name  cbac-dmz   icmp
ip   inspect   name  cbac-dmz   udp
ip   inspect   name  cbac-lan   http
ip   inspect   name  cbac-lan   tcp
ip   inspect   name  cbac-lan   icmp
ip   inspect   name  cbac-lan   udp
ip   inspect   name  cbac-internet   http
ip   inspect   name  cbac-internet   tcp
ip   inspect   name  cbac-internet   icmp
ip   inspect   name  cbac-internet   udp
interface fa0/0
ip inspect cbac-internet in interface fa0/1
ip inspect cbac-dmz in interface fa1/0
ip inspect cbac-lan in interface fa1/1
ip inspect cbac-lan in
```

Крок 6. На прикордонному маршрутизаторі периметра мережі IBR налаштувати механізм первинної фільтрації пакетів:

```
ip access-list extended iacl-internet
deny ip host 0.0.0.0 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
deny ip 224.0.0.0 31.255.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.0.15.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 212.192.98.152 0.0.0.7 any
deny ip 212.192.98.160 0.0.0.7 any
permit ip any any
ip access-list extended iacl-DMZ
```

```
permit ip 212.192.98.152 0.0.0.7 any
permit ip 212.192.98.160 0.0.0.7 any
deny ip any any interface fa0/0
ip access-group iacl-internet in
interface fa0/1
ip access-group iacl-DMZ in
```

Крок 7. Перевірити коректність функціонування обладнання периметра Інтернет, можливість доступу з мережі Інтернет до загальнодоступних сервісів і в мережу Інтернет з корпоративної ЛОМ.

6.4. Запитання і завдання

1. Проаналізувати політику безпеки управління інформаційними потоками, представлену в табл. 2.

2. Доповнити політику безпеки управління інформаційними потоками правилами для проектованої вами електронної поштової системи.

3. Забезпечити доступ до мережі Інтернет з мереж філій через ГВС.

6.5.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

6.6.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 7.

Криптографічний захист каналів передачі даних

Мета роботи:

Метою лабораторної роботи є навчання методам і засобам захисту каналів передачі даних ГОМ на основі технології віртуальних приватних мереж.

7.1. Короткі теоретичні відомості

При організації обміну і передачі інформації в ГОМ, як правило, виходять з моделі порушника, в якій останній контролює канали передачі даних, а також має можливість спотворювати інформацію, передану між абонентами (модель активного порушника). Для захисту інформації застосовують різні спеціалізовані протоколи безпеки, які працюють на одному (або кількох) рівнях моделі ISO / OSI. Нижче представлений короткий перелік найбільш поширених протоколів безпеки. Так, на канальному рівні працюють протоколи PPTP, L2TP, L2F, на мережевому рівні працюють протоколи IPv6 і IPSec, на транспортному рівні - протокол SSL / TLS і на прикладному - SSH, PGP, S / MIME.

Для обміну ключової інформації в рамках одного або декількох доменів застосовують протокол Kerberos, в масштабах ГВП використовують інфраструктури обміну відкритими ключами PKI. Крім цього, більшість протоколів передачі даних включають в себе можливість проведення аутентифікації сторін перш, ніж буде встановлено інформаційний канал зв'язку.

Вибір протоколу для захисту переданих даних диктується необхідними ресурсами і можливостями передбачуваного порушника. Для захищеного обміну даними між мережами, рас-покладеними віддалено один від одного, або між абонентами і се-тьма, як правило, застосовується сімейство протоколів мережевого рівня IPSec.

Захист даних на мережевому рівні володіє тим гідністю, що для транспортних і сеансових протоколів робота по захисту даних стає прозорою. У цьому випадку немає необхідності створювати спеціальне ПЗ для захисту переданих даних протоколами верхніх рівнів.

Захищена передача даних, реалізована на транспортному рівні, використовується переважно в моделі клієнт - сервер. Відповідно клієнт і сервер повинні підтримувати спеціальний протокол. Прикладом може служити протокол SSL і його модифікація - TLS.

Вибір схеми для розподілу ключової інформації залежить від моделі порушника. Для моделі з активним порушником під-ходять тільки ті схеми, в яких учасники

інформаційного домена заздалегідь знають відомий тільки їм секрет, або у них є загальний довірений посередник.

Великого поширення набули способи розподілу ключів на основі протоколу Kerberos і на основі інфраструктури відкритих ключів. Обидва способи припускають загального довіреної посередника, в ролі якого виступає або контролер домену, або засвідчує центр.

Схема, заснована на попередньому знанні загального секрету, припускає адміністративно організаційне рішення, коли, наприклад, адміністратори мережі домовляються про використаний пароль або ключі.

Віртуальна приватна мережа (VPN) - це технологія, що використовує криптографічні механізми для захищеної передачі даних по загальній або виділеній мережевій інфраструктурі.

У загальному випадку технологія VPN вирішує наступні завдання: організації зв'язку між філіями, підключення партнерів й клієнтів, а також мобільних співробітників до корпоративної СПД.

Термін «приватна мережа» позначає приналежність обладнання мережі підприємства і гарантію конфіденційності інформації, що передається по цій мережі. Такі мережі не дуже поширені, набагато частіше підприємство орендує канали зв'язку для своїх філій.

При оренді каналів підприємство ділить пропускну спроможність магістральних каналів з іншими абонентами провайдера. Смуга пропускання орендованого каналу повністю виділяється підприємству і є його власністю. Корпоративні дані практично не доступні для абонентів, які не є користувачами корпоративної СПД або мережі провайдера.

Також можлива організація VPN на базі ГОМ Інтернет, що, з одного боку, має переваги в простоті і низькій вартості реалізації, але разом з тим не гарантує заданої пропускної здатності.

Виділяють такі види VPN: внутрішньо корпоративні (intranet VPN) - для організації зав’язків з філіями, віддаленого доступу (remote access VPN) - для організації доступу до ресурсів компанії співробітників і клієнтів, між корпоративні (extranet VPN) - для організації зав’язків з партнерами та клієнтами.

У VPN для криптографічного захисту даних на мережевому рівні призначене сімейство протоколів IPSec, що забезпечує виконання наступних завдань: шифрування переданих даних, забезпечення їх автентичності та цілісності, а також розмежування доступу (фільтрація IP-потоків) і захист від повторної передачі IP-дейтаграм.

До складу сімейства IPSec входять протокол аутентифікації (AH), протокол шифрування (ESP) і протокол обміну ключами (IKE). Протокол IKE розроблений на основі протоколів ISAKMP, Oakley і SKEME і призначений для узгодження використовуваних алгоритмів, ключів, тривалості їх дії та інших параметрів. Результатом такого узгодження є односпрямована безпечна асоціація (security association - SA). Робота протоколу IKE включає два етапи. Перший - ідентифікація та аутентифікація сторін, встановлення захищеного каналу для узгодження параметрів (результат - створення IKE SA). Другий - встановлення захищеного каналу передачі даних.

Протоколи сімейства IPSec можуть працювати в транспортному і тунельному режимах. У транспортному режимі заголовок вихідної дейтаграми залишається незмінним, а в тунельному режимі відбувається формування нового IP-заголовка для AH або ESP-пакета.

Виділяють такі основні варіанти застосування протоколу IPSec: вузол - вузол, вузол - мережу та мережу - мережу. При цьому основними схемами включення VPN-шлюзів в сегменті LVP є паралельна і послідовна.

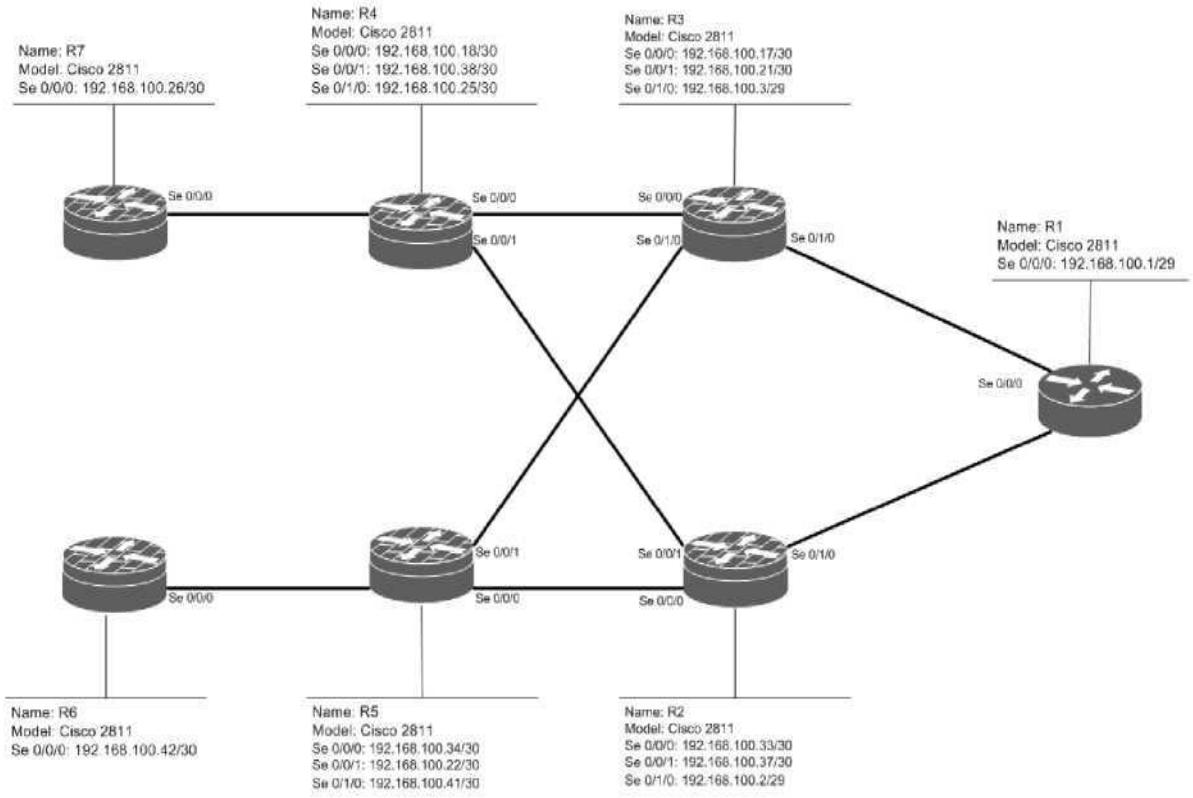

Рисунок 8. Схема організації віртуальної приватної мережі

7.2. Постановка задачі

Забезпечити криптографічно захищене підключення мереж філій до мережі центрального офісу з орендованих каналах передачі даних (рис. 8), а також криптографічно захищений віддалений доступ клієнтів через ГВС Інтернет до АС «Клієнт - Банк» (рис. 9). Для забезпечення гарантій захисту каналів зв'язку для підключення клієнтів через ГВС Інтернет використовувати немаршрутизовані IP-адреси інфраструктури АС «Клієнт-Банк». Централізоване управління доступом забезпечити шляхом використання протоколу Radius та інфраструктури AAA.

7.3. Послідовність дій

Крок 1. Створити та налаштувати політику безпеки протоколу ISAKMP з наступними параметрами: метод аутентифікації - PSK, алгоритм шифрування - AES, алгоритм хешування - SHA1, номер групи Діффі-Хеллмана - 5, довжина вироблюваного ключа - 1536 біт:

```
crypto isakmp policy 10
authentication pre-share encryption
aes hash sha group 5
```

Задати ключі аутентифікації маршрутизаторів за методом PSK:

```
crypto isakmp key B4H^3PdQ address Router IP address
```

Крок 2. Створити та налаштувати політику криптографічного захисту каналів передачі даних.

```
crypto ipsec transform-set WAN esp-aes esp-sha- hmac
```

Крок 3. Визначити захищаються інформаційні потоки через механізм ACL:

```
ip access-list extended cryptoacl-wan
permit ip  10.194.0.0  0.0.255.255  10.194.0.0  0.0.255.255
```

Крок 4. Налаштувати криптографічну карту шифрування інформаційних потоків на каналі передачі даних між маршрутизаторами і ініціалізувати її на зовнішньому інтерфейсі:

```
crypto map WAN-map 10 ipsec-isakmp
set peer Router IP address
set transform-set WAN
match address cryptoacl-wan interface se0/0/0
crypto map WAN-map
```

Крок 5. Виконати налаштування протоколу IPSec на всіх маршрутизаторах СПД:

Крок 6. Виконати налаштування служби AAA і протокол Radius на VPN-концентраторі:

```
aaa new-model
aaa authentication login ASCB group radius
aaa authorization network ASCB local
radius-server host 192.168.20.11 key Fhlewre$
```

Крок 7. Створити та налаштувати політику ISAKMP.

```
crypto isakmp policy 10
authentication pre-share
encryption aes
group 5
```

Крок 8. Виділити діапазон видаваних IP-адрес для віддалених клієнтів АС «Клієнт-Банк»:

```
ip local pool ASCB 192.168.20.100 192.168.20.200
```

Крок 9. Налаштувати параметри групи віддаленого доступу:

```
crypto isakmp client configuration group ASCB
key ClientBankKey pool ASCB
netmask 255.255.255.0
```

Крок 10. Налаштувати політику криптографічного захисту даних:

```
crypto ipsec transform-set CB esp-aes esp-sha-hmac
```

Налаштувати криптографічну карту шифрування потоків віддаленого доступу:

```
crypto dynamic-map d-ASCB 10
set transform-set CB
crypto map s-ASCB client authentication list ASCB
crypto map s-ASCB isakmp authorization list ASCB
crypto map s-ASCB client configuration address
respond
crypto map s-ASCB 10 ipsec-isakmp dynamic d-ASCB
```

Ініціалізувати криптографічну карту:

```
interface fa0/0
crypto map c-ACSB
```

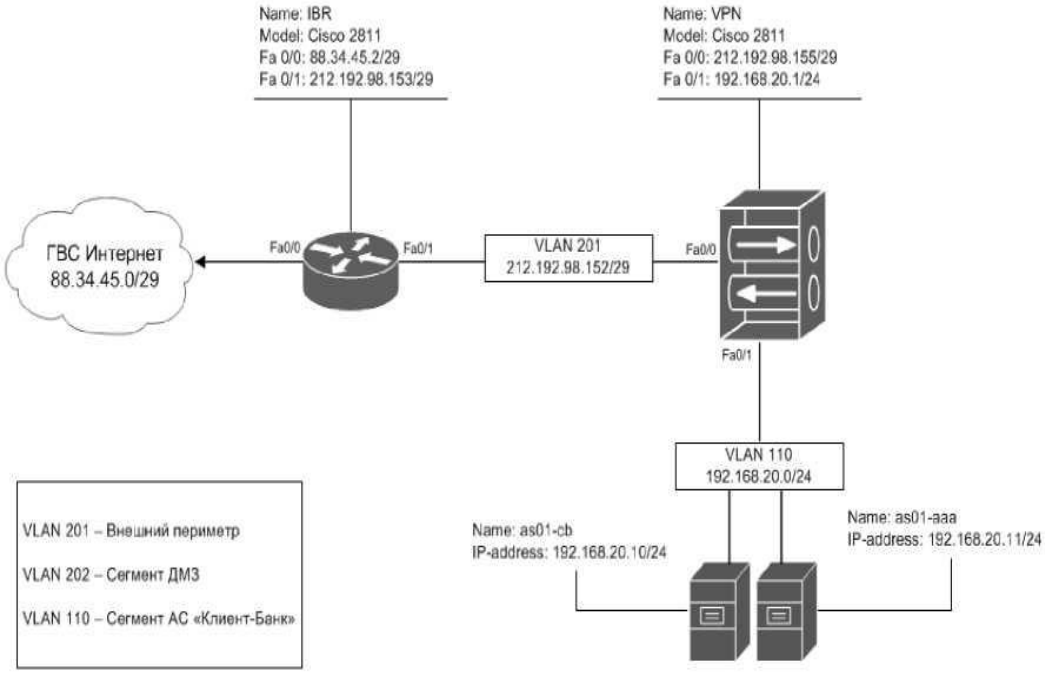

Рисунок 9. Схема організації захищеного віддаленого підключення до АС «Клієнт-Банк»

Крок 11. Перевірити коректність функціонування СПД та доступність послуг АС «Клієнт-Банк». Вивчити структуру шифрованих мережевих пакетів. Перевірити доступність АС центрального офісу відмову каналів зв'язку або мережевого устаткування.

7.4. Запитання і завдання

1. Вивчити рекомендації до вибору параметрів криптографічного захисту протоколів IPsec.

2. Переконатися в неможливості доступу в сегмент АС «Клієнт-Банк» з ГВП та корпоративної СПД без знання параметрів та ключів криптографічного захисту IPsec.

7.5.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

7.6.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.

Лабораторна робота № 8.

Захист WLAN

Мета роботи:

Метою лабораторної роботи є ілюстрація застосування базових методів і засобів захисту бездротової ЛОМ, що є частиною корпоративної ЛОМ.

8.1.Короткі теоретичні відомості

На відміну від провідних мереж Ethernet бездротові ЛОМ сімейства стандартів 1EEE 802.11 використовують загальнодоступний радіоканал для зв'язку з абонентами. Цей факт лежить в основі цілого ряду нових проблем безпеки і призводить до того, що в даний час бездротові ЛОМ найбільшою мірою, порівняно з іншими типами мереж, схильні до атак.

У корпоративних мережах передачі даних елементи бездротових ЛОМ IEEE 802.11 (точки доступу, маршрутизатори) використовуються, як правило, для розширення мережевої інфраструктури. При аналізі безпеки бездротових ЛОМ виділяють наступні основні загрози:

- несанкціоноване підключення до пристроїв і мереж;
- неконтрольоване використання інфраструктури;
- перехоплення і модифікація даних;
- порушення доступності;
- позиціювання пристрою.

Основними механізмами забезпечення безпеки бездротової ЛОМ є:

- базові методи захисту та протоколи аутентифікації IEEE 802.11i;
- управління доступом відповідно до стандарту IEEE 802.1x;
- сегментування мереж за допомогою технології VLAN;
- управління доступом до мережі на основі атрибутів користувачів і засобів доступу;
- між мережеве екранування і VPN;
- виявлення і запобігання вторгнень на канальному рівні.

Варто відзначити, що всі основні механізми та засоби безпеки бездротових мереж орієнтовані, як правило, на захист канального рівня. Захист на більш високих рівнях мережевої моделі реалізується на базі типових для дротових мережевих КС механізмах.

При організації захищеної бездротової ЛОМ, як правило, відштовхуються від категорії інформації, переданої в мережі і оброблюваної на серверах або робочих станціях, підключених до цієї мережі. Залежно від неї формуються вимоги безпеки, яким повинна задовольняти КС. Наприклад, у мережі можуть бути виділені наступні сегменти бездротової ЛОМ, побудовані у відповідності з різними вимогами безпеки: сегмент гостьового доступу до мережі Інтернет, сегмент доступу до мережі Інтернет з мобільних пристроїв співробітників, сегмент доступу до веб-ресурсів загального призначення і сегмент для з'єднання двох ЛОМ за допомогою точок доступу.

8.2.Постановка задачі

Побудувати захищений бездротовий сегмент ЛОМ (див. Рис. 8), що розширює інфраструктури ЛОМ і дозволяє організувати підключення користувачів до неї з використанням механізмів WPA2.

8.3.Послідовність дій

Крок 1. Виконати підключення бездротового маршрутизатора до ЛОМ філії.

Крок 2. Виконати налаштування маршрутизатора WR04-1. Призначити пристрою IP-адресу та маску мережі з мережі управління ЛОМ філії. Призначити SSID - «bank04», метод аутентифікації - «WPA2», вказати параметри підключення до сервера RADIUS (IP-адреса 192.168.4.1, shared secret - «Nh$c@vv3», AES).

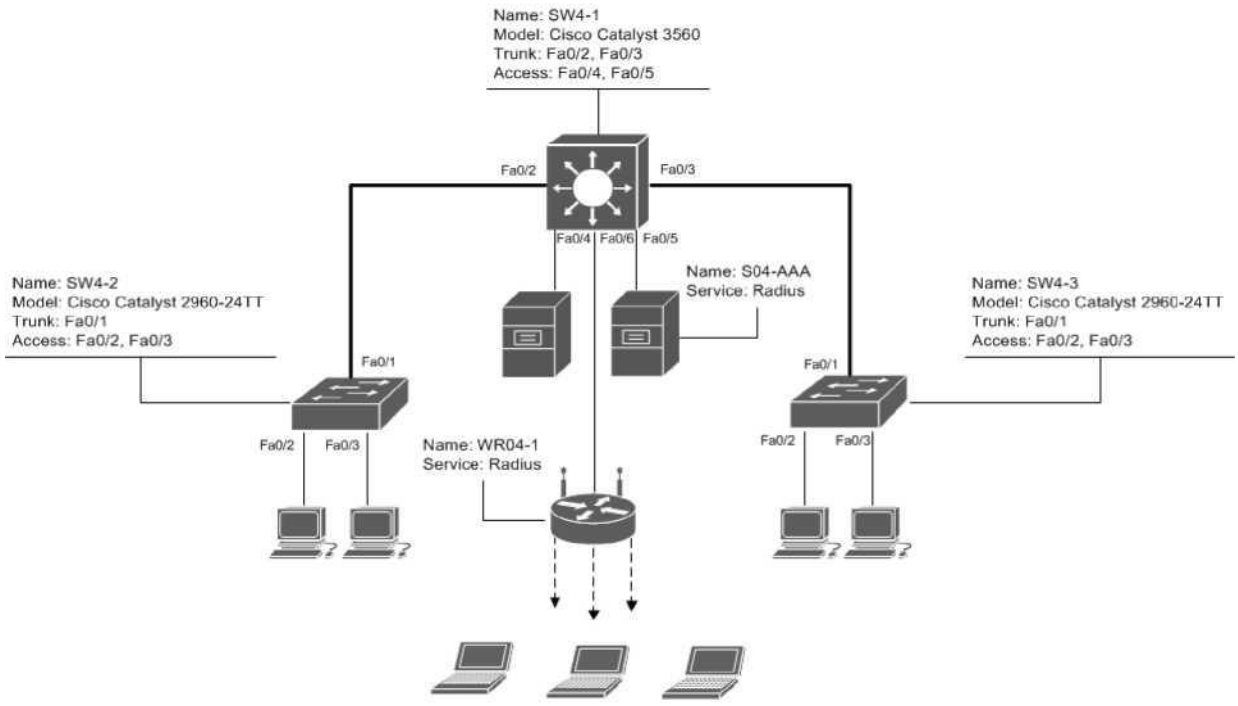

Рисунок 8. Схема організації бездротового сегмента ЛОМ філії

Крок 3. На сервері S04-AAA створити клієнта WR04-1, задати його мережеві параметри. Створити користувача для підключення: UserName - «user», Password - «Miemnma2».

Крок 4. На мобільної робочої станції в параметрах бездротового підключення вказати параметри SSID, метод аутентифікації, UserlD і Password. Перевірити можливість мережевої взаємодії в ЛВС філії і доступ до ГОМ.

8.4.Запитання і завдання

1. Організувати додатковий бездротовий сегмент ЛОМ, призначений для гостьового доступу недовірених користувачів в мережу Інтернет. Забезпечити неможливість доступу з недовірених сегмента в ЛВС філії.

2. Вивчити рекомендації і відомі підходи до побудови бездротових ЛОМ.

3. Запропонувати технічне рішення (розробити схему) з організації доступу з бездротового сегмента до ЛОМ корпоративної мережі з використанням технологій VPN.

8.5.Вимоги до звіту

1. Назва роботи.
2. Мета роботи.
3. Короткі теоретичні відомості.
4. Хід роботи.
5. Висновки.

8.6.Рекомендована література

1 Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco. : пер. с англ. М. : Вильямс, 2003. 976 с.

2 Хилл Б. Полный справочник по Cisco. : пер. с англ. М. : Вильямс, 2004. 1078 с.

3 Хьюкаби Д., Мак-Квери С. Руководство Cisco по конфигурированию коммутаторов Catalyst : пер. с англ. М. : Вильямс, 2004. 560 с.