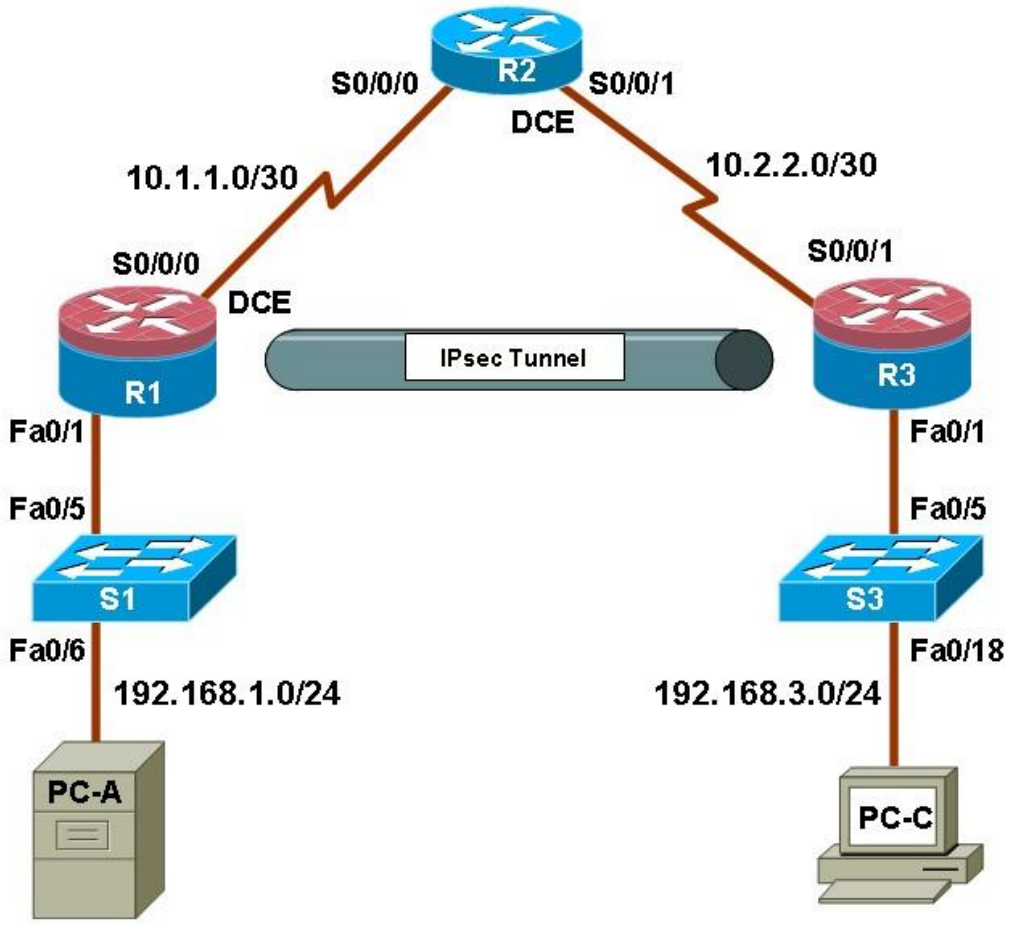
Конфигуриране на Site-to-Site VPN

Топология



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Цел на упражнението

Запознаване с основите на VPN технологията и приложението на Site-to-Site VPN във Cisco устройства. За целта ще се използва симулационна програма Cisco Packet Tracer.

Теория

1. VPN

В днешни дни развиващите се с бързи темпове бизнес среди имат нуждата от лесна и сигурна комуникация с клоновете си. Вариантите за осъществяването на такава връзка е с наета комуникационна линия или Frame Relay. С течение на времето тези линии се очертават финансово неизгодни за по-малките фирми. Допълнително към това с помощта на съвременните технологии голяма част от служителите работят отдалечено(от домовете си, от coffese-и и т.н.).

С развитието на интернет и технологиите се появяват различни решения, които позволяват свързаност между различни офиси и местоположения. Напоследък Internet-базираните VPN се развиват като най-сигурното и удобно средство за свързване на корпоративните центрове с техните отдалечени офиси и мобилни служители.

Виртуалните частни мрежи (Virtual Private Network - VPN) представлява сигурна връзка между две страни. Нарича се virtual, защото изгражда тунел, през обществената интернет мрежа, свързваща две отдалечени точки. Private – понеже тази връзка е криптирана и данните преминаващи през нея оставят частни за всички, освен ако нямат съответният ключ. Накрая network, защото преминава през интернет. Чрез VPN ние получаваме:

Цялостност на данните

Шифроване на информацията

Удостоверяване на системата източник

Основата на VPN се състои в изграждането на логическа връзка от точка до точка, наречена тунел. Той служи за предаване на данните, които биват криптирани. Криптирането използва различни математически алгоритми за шифроване на информацията. По този начин се гаранти, че съобщението ще остане кодирано за външни лица, освен ако не са упълномощени.

Процесът по скриването на данните от оригиналният пакет в тялото на нов, се нарича капсулация. Тунелът представлява връзка от точка до точка, която криптира данните преминаващи през нея.

Понастоящем се използват главно две VPN-технологии: за връзка сайт със сайт и за отдалечен достъп:

VPN от сайт до сайт осигуряват интернет-базирана WAN инфраструктура, която разширява мрежовите ресурси на регионалните офиси, домашни офиси и сайтове на бизнес-партньорите. Целият трафик между обектите се криптира с помощта на IPsec протокола и се интегрира с

мрежови функции като маршрутизация, качеството на услугата и поддръжка на Multicast (групово предаване – мрежови протокол, при който мрежовият пакет се изпраща на определено подмножество адресанти). Тези виртуални частни мрежи също предлагат:

надеждеа и висококачествен транспорт на сложен и критичен трафик, като пренос на глас и приложения „клиент-сървър";

опростено поддържане и намалени оперативни задачи при изграждане на мрежата;

интегрирана модерна мрежова интелигентност и маршрутизация за широка гама от типове мрежи.

VPN за отдалечен достъп осигуряват достъп до почти всички типова данни, като глас или видео приложение на от отдалечена работна станция, емулирайки станция на главния офис. С тази VPN може да осигури висока степен на защита, персонализация на отдалечения достъп за всеки, навсякъде, по всяко време и с почти всяко устройство. Тези виртуални частни мрежи:

създават у отдалечения потребител чувството, че работи в главния офис;

доставят VPN-връзка безопасно и лесно за широк кръг от потребители и устройства;

поддържат широка гама от възможности за свързаност, крайни точки и платформи, за да отговорят на динамичните нужди от дистанционен достъп.

Има два основни метода за изграждане на виртуални частни мрежи за отдалечен достъп: чрез IP Security (IPSec) и Secure Sockets Layer (SSL). Всеки метод има своите предимства въз основа на изискванията за достъп на потребителите и организацията на ИТ-процесите. Въпреки че много решения предлагат използване само на IPsec или SSL, много VPN-решения предлагат и двете интегрирани технологии на една платформа с единно управление. Предлагането и на двете технологии дава възможност на организациите да персонализира дистанционния достъп чрез VPN без допълнителен хардуер или увеличаване сложността на управление.

2.Описание на протокола IPSec.

2.1. Общо описание и основни термини, свързани с IPSec.

Целта на IPSec е да осигури стандартни криптографски механизми за сигурност между IPv4 и IPv6 обекти. Между основните услуги са контрол на достъпа, гарантиране на ненакърнимост на данните (integrity) по пътя им от източника до местоназначението, както и удостоверяване за произхода им, разпознаване и отхвърляне на подвеждащи атаки (replays), поверителност (чрез криптиране) и мерки за поверителност на потоците от трафик. Всички тези услуги се предоставят на ниво IP.

В този смисъл може да се каже, че IPSec включва минимални функционални характеристики на една "защитна стена" (firewall). Те се подсилват и от криптографски-базираните удостоверявания и проверки за ненакърнимост на данните, наложени на целия IPSec трафик.

IPSec се реализира върху хост компютър или като "защитен шлюз" (security gateway - SG) – защитна стена или маршрутизатор с IPSec възможности. Възможно е да се проектира

самостоятелно устройство. Защитата, предлагана от IPSec, се базира на изискванията, дефинирани в базата от данни на политиката за сигурност (Security Policy Database - SPD) от страна на потребителя/администратора или приложна програма. Въз основа на тях IP пакетът се защитава (PROTECT) с помощта на IPSec услугите, отхвърля (DISCARD) или се пропуска без обработване от IPSec (BYPASS).

В основата на архитектурата на IPsec лежи “Сдружение за налагане на политика за сигурност (Security Association - SA). Протоколите, чрез които се реализират услугите на IPSec VPN - AH (добавяне на удостоверително заглавие, хедър, към IP пакета) и ESP (опаковане на полезните данни в IP пакета), използват

SA. Същото важи и за протокола за обмен на ключове Internet Key Exchange (IKE). “Сдруженията” възникват в резултат от прилагането на политика, която дефинира криптирането, създаването на ключове, удостоверяването и всички процеси, които ще бъдат прилагани към данните.

SA представлява еднопосочно съединение, което предлага услуги за сигурност на трафика, който носи, чрез AH или ESP (например: DES , 3DES, AES протокол за криптиране и MD5 или SHA-1 протокол за удостоверяване). За всеки един от протоколите, който се поддържа, AH или ESP, или и двата, трябва да се създаде отделна SA. Ако искаме да имаме двупосочни комуникации между две IPSec системи, ще са ни необходими две SA (по една за всяка от посоките). В този смисъл IKE по подразбиране създава двойки SA. Така че в IPSec VPN съществуват две форми на SA:

ISAKMP (Internet Security Association Key Management Protocol), известни и като IKE. IKE SA е двупосочна и предоставя сигурен комуникационен канал между двете страни, който може да се използва за договаряне на по-нататъшните комуникации.

IPSec SAs. IPSec SA е еднопосочна и се използва за действителната комуникация между устройствата. За двупосочна комуникация трябва да има поне две IPSec SAs – по една за всяка посока предаване и приемане.

IPSec SA могат да се дефинират еднозначно чрез три компонента:

Security parameter index (SPI) – 32-битово число, служещо за идентификация на SA.

IP адреса на получателя.

Идентификатор на протокола за сигурност, който дефинира дали SA е AH или ESP.

Информацията за всички SA се съдържа в Security Association Database (SAD).

Архитектура.

Базовата архитектура на IPSec се описва от стандарта RFC 4301. Върху нея се градят всички реализации. Там се дефинират услугите, които IPSec предлага, как и къде се използват и как пакетите се конструират и обработват.

Повечето от услугите за сигурност на IPSec се осигуряват чрез един от двата протокола за защита на трафика. Authentication Header (RFC 4302) защитава целия IP пакет, а Encapsulating Security Payload (RFC 4303) - само на полезните данни, които носи IP пакетът, т.е. на по-

горните слоеве. В тази схема участват и процедурите и протоколите за управление на криптографските ключове. Точно как и кои процедури/протоколи ще се използват е зависи от волята на администраторите.

Всеки един от протоколите, AH и ESP, поддържа два режима на работа – транспортен и тунелен. Транспортният осигурява защита главно за протоколите на по-горните слоеве. IPSec хедърът се вмъква между IP хедъра и горните слоеве. В тунелен режим целият IP пакет се вмъква в нова дейтаграма, като IPsec хедърът се вмъква между външния и вътрешния хедър.

Транспортен режим.

Концепцията на VPN решенията се основава главно на тунелите. Тунел възниква, в случаите когато оригиналните данни са енкапсулирани в нов пакет и препратени въз основа на атрибутите на протокола на новия пакет. Целта е да се осигури прозрачна връзка за основния протокол. Транспортният режим на IPSec е уникален с това, че не се осъществява енкапсулиране в нов пакет. Оригиналният IP хедър се използва и данните се препращат въз основа на оригиналните атрибути, заложени от протокола.

Тъй като дейтаграмите се предават от TCP/IP протокола към мрежовия слой, те са снабдени със съответната хедър информация от всеки слой. В края на операциите в мрежовия слой, IPSec премахва оригиналния IP хедър и криптира хедъра и данните на горния протокол. След това IPSec добавя избрания хедър на протокола за сигурност преди отново да приложи оригиналния хедър.

В транспортния режим оригиналният пакет остава същият с изключение на две важни промени: данните са криптирани и в пакета е добавен удостоверяващ протокол. По този начин пакетът получава интегритет, за да се гарантира, че данните не са променяни по време на пренос.

Главното ограничение се състои в това, че в рамките на транспортния режим не могат да се предоставят шлюзови услуги. Ако две системи комуникират в транспортен режим, комуникацията не може да бъде осъществена отвъд крайните точки на VPN. Транспортният режим е запазен за комуникация от типа “точка към точка”. Ако при неговото използване е установен VPN с VPN шлюз, отдалечената система има възможност да комуникира само с шлюза, като не може да обменя данни с вътрешната мрежа.

Съществуват няколко случая, при които използването на транспортния режим е необходимо. VPN чрез транспортен режим пряко към шлюз може да осигури защитено администриране без да съществува безпокойство относно достъпа до вътрешната мрежа. В ситуациите, при които VPN шлюз се управлява отдалечено от трета страна, достъпът й до вътрешната мрежа може да бъде нежелан. Способността за вмъкване на транспортен режим SA в тунелен режим SA осигурява разширена защита отвъд шлюза във вътрешната мрежа.

Тунелен режим.

Тунелният режим е най-разпространен при VPN и широко използван в IPSec имплементациите. Той се използва главно за шлюзови услуги, защото енкапсулирането осигурява способността за предаване на няколко сесии чрез една точка. Това позволява VPN шлюз да деенкапсулира данните и да ги препрати към крайната вътрешна точка.

Тунелният режим енкапсулира пакет, предназначен да комуникира в мрежа, и го енкапсулира в друг пакет за предаване към отдалечена мрежа. Този процес позволява протокол, който е възприет за входна и изходна точка, да пренася друг комуникационен протокол, който обикновено не би могъл да се препрати през мрежата.

В тунелния режим целият оригинален пакет е енкапсулиран и кодиран, като са добавени нов IP хедър и хедър на удостоверителния протокол. Резултатът е нов пакет, който съдържа два IP хедъра.

Вътрешният IP хедър се прилага към оригиналните дейтаграми, които се предават в мрежовия слой, като в края на краищата се енкапсулира в нов пакет. Новият пакет получава външен IP хедър, който съдържа информация, необходима за комуникирането във VPN.

Протоколите за сигурност представляват същността на IPSec и тяхната реализация определя конкретно как да се приложи транспортен или тунелен режим. Те могат да бъдат използвани поотделно или единият да бъде "вмъкнат" в другия.

Така се разширяват възможностите на VPN и тяхното функциониране.

2.2. Протокол Encapsulating Security Payload (ESP).

Протоколът е описан в RFC 4303. ESP предоставя няколко услуги за сигурност - поверителност на данните, интегритет, удостоверяване на източника, услуги срещу повторни атаки (anti-replay) и ограничена поверителност на трафика. Разширяването на поверителността и интегритета на комуникацията са свързани с режима. В тунелен режим вътрешният IP хедър е добре защитен, докато външният не е. В транспортен режим няма вътрешен IP хедър, поради което защитата на мрежовия слой е ограничена. Наборът от предоставяните услуги зависи от избраните опции по време на установяването на Security Association (SA) и конкретната имплементация.

ESP осигурява поверителност посредством криптиране и интегритет на данните с удостоверяване. Използваните за ESP алгоритми се определят от атрибутите за създаване на SA. ESP сам по себе си не е управляван от специфични алгоритми, а представлява отворен стандарт за прилагане на различни такива (например: DES, 3DES, AES). Стандартът дефинира процедури и необходими действия за криптиращия процес, но не дефинира какво може и не може да бъде използвано за криптографската услуга. Прилагането на поверителност не е задължително, но ако е необходимо само удостоверяване, се използва протоколът AH.

Въпреки че поверителността и удостоверяването са основните услуги, предоставяни от ESP, те не са задължителни. Една от двете обаче трябва да бъде използвана. Основната идея е да се използва ESP при необходимост от удостоверяване и криптиране, а AH – когато е необходимо разширено удостоверяване без криптиране.

2.3. Протокол Authentication Header (AH).

Протоколът, който добавя удостоверително заглавие (хедър) - Authentication Header (AH), е описан в RFC 4302. AH осигурява интегритет на данните, удостоверяване на източника и възможност за използване на защита срещу повторни атаки. AH обаче не предоставя поверителност. Неговата основна функция е да осигури удостоверителни услуги при

комуникацията. Тъй като при AH липсва поверителност, не е необходимо да се дефинира криптиращ алгоритъм.

Както при ESP, положението на AH хедъра зависи от режима на комуникация. В транспортен режим хедърът е вмъкнат след IP хедъра и опциите и преди който и да е протокол от горния слой, включително други IPSec хедъри. В тунелен режим оригиналният пакет е разположен зад хедъра, като новият IP хедър и опции предхождат AH хедъра. От гледна точка на външния IP хедър положението на AH е същото, както в транспортния режим.

2.4. Протокол Internet Key Exchange (IKE).

Протоколът IKE е хибрид от протоколите Oakley и SKEME и действа в рамките, определени от Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP определя формата на пакетите, таймерите за препредаване и изискванията за конструиране на съобщенията. Oakley и SKEME определят стъпките, които двете страни трябва да предприемат за установяване на споделен, удостоверен ключ. Освен това IKE протоколът се грижи да променя периодично ключовете (rekeying), за да осигури тяхната поверителност.

IKE използва концепцията на SA, но физическата конструкция на IKE SA е различна от IPSec SA. IKE SA определя начина, по който се осъществява комуникацията между две страни, например кой алгоритъм да се използва за криптиране на трафика на IKE, как да се удостоверят двете страни и т.н. IKE SA се използва, за да установи необходимите IPSec SA между страните.

Oakley определя “режимите”, а ISAKMP – “фазите”. Връзката между двете е пряка и IKE представя различните начини на размяна, като режими, които действат в една от двете фази.

Във фаза 1 двете страни в ISAKMP установяват сигурен и удостоверен канал, по който да комуникират. Това е т. нар. ISAKMP Security Association. Двата режима, чрез които се осъществява обмяна във Фаза 1, са “Main Mode” и “Aggressive Mode” и се използват само в тази фаза.

Във Фаза 2 съществуват два режима – “Quick Mode” и “New Group Mode”. “Quick Mode” се използва за установяване на SA на базата на основния протокол за сигурност. “New Group Mode” е режим от Фаза 2, но услугите, които предоставя, ползват операциите във Фаза 1.

Във Фаза 2 SA се договарят за услуги като IPsec например, за които е необходим ключ и/или договаряне на параметри. “Quick Mode” завършва обмяната във Фаза 2 и се използва само в тази фаза.

“New Group Mode” следва Фаза 1 и служи за установяване на нова група, която може да бъде използвана при бъдещо договаряне.

ISAKMP SA е двупосочна. Поради това веднъж установена, всяка страна може да инициира Quick Mode, Informational и New Group Mode обмен. ISAKMP SA се идентифицира чрез “бисквитките” на инициатора, следвани от тези на отсрещната страна в комуникацията.

Основната разлика между режимите във Фаза 1 е броят на обменените съобщения за установяване на SA. В Main Mode те са шест, а в Aggressive Mode - три.

Required Resources

- 3 routers with (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with CCP 2.5 installed
- PC-C: Windows XP, Vista, or Windows 7 with CCP 2.5 installed
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

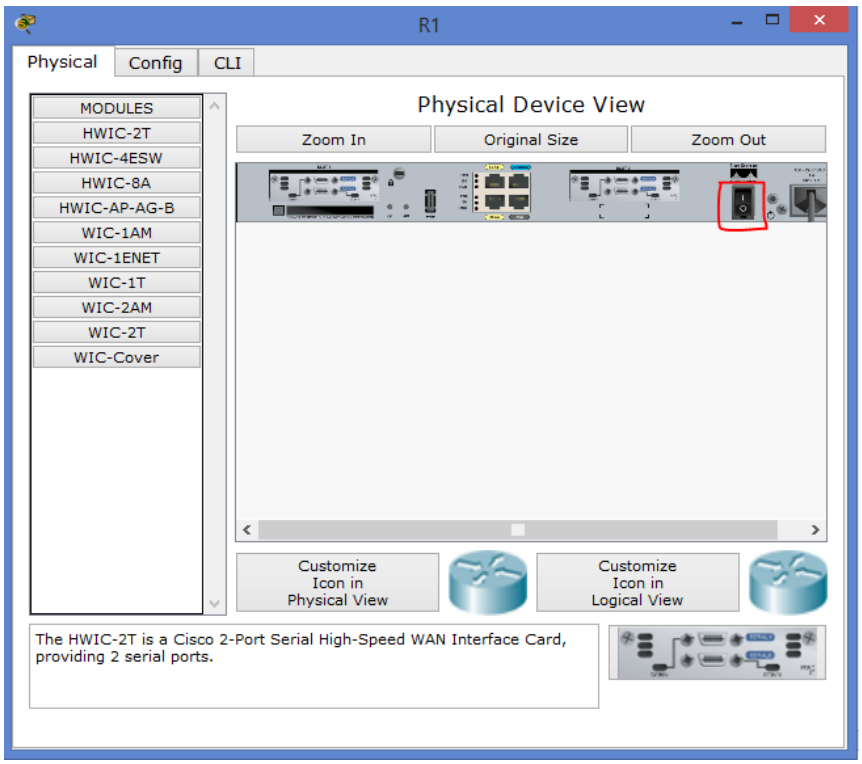
Практическа задача

Част 1: Базова конфигурация на устройствата

В първата част на упражнението ще се конфигурират имена и адреси на отделните интерфейси на рутери, статични пътища по подразбиране, парола за telnet сесии, конзолата и различните режими на работа.

Стъпка 1: Свързване на кабелите и пускане на устройствата.

Свържете устройствата как е показано на топологията. След като това кликнете на R1 и в раздела Physical може да видите самият рутер. Кликнете на Power бутона, за да го включите.



Стъпка 2: Основни настройки за всички рутери.

a. При първоначално зареждане ще ви опита: Continue with configuration dialog? [yes/no]: no

b. Конфигурирайте имена на устройствтата R1, R2 и R3.

c. Конфигурирайте адреси на интерфейсите на рутерите, като използвате таблицата в началото на упражнението.

d. За да предотвратите рутера да се опитва да превежда неправилно въведените команди, като имена на хостове, деактивирайте DNS търсенето на всички рутери.

R1(config)# **no ip domain-lookup**

Стъпка 3: Конфигуриране на EIGRP протокол на R1, R2, и R3.

a. На R1, използвайте следните команди.

```
R1(config)# router eigrp 101
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 10.1.1.0 0.0.0.3
R1(config-router)# no auto-summary
```

b. На R2, използвайте следните команди.

```
R2(config)# router eigrp 101
R2(config-router)# network 10.1.1.0 0.0.0.3
R2(config-router)# network 10.2.2.0 0.0.0.3
R2(config-router)# no auto-summary
```

c. На R3, използвайте следните команди.

```
R3(config)# router eigrp 101
R3(config-router)# network 192.168.3.0 0.0.0.255
R3(config-router)# network 10.2.2.0 0.0.0.3
R3(config-router)# no auto-summary
```

Стъпка 4: Конфигурирайте компютрите PC-A и PC-C.

Конфигурирайте статични адреси. (в таблицата по-горе са показани адресите

Стъпка 5: Проверете връзката между компютрите и рутерите.

a. Ping от R1 до R3 (192.168.3.1).

b. Ping от PC-A до R1 LAN (192.168.1.1) от PC-C до R3 LAN (192.168.3.1).

Стъпка 6: Конфигурирайте минимална дължина на използваните пароли.

Използвайте командата **security passwords, за да конфигурирате минимална дължина паролата от 10.**

```
R1(config)# security passwords min-length 10
```

Стъпка 7: Конфигурирайте конзолата и VTY сесиите.

Използвайте командата exec-timeout, за да конфигурирате при 5 минути неактивност да ви изключи автоматично. За да синхронизирате нежелани съобщения и съобщенията от debug-а използвате командата logging synchronous.

a. Парола за конзолата

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

b. Парола за Telnet сесии

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# login
```

a. Повторете командаите и на R2 и R3.

Стъпка 9: Криптирайте паролите, които са в чист текстови вид.

Използвайте командата **service password-encryption, за да криптирате паролите на конзолата, VTU и AUX**.

```
R1(config)# service password-encryption
```

Стъпка 10: Запате текущата конфигурацията на всичи три устройства.

```
R1# copy running-config startup-config
```

Част 2: Конфигурайте Site-to-Site VPN

Във втората част на упражнението ще конфигурите IPsec VPN тунел между R1 и R3.

Задача 1: Конфигуриране на IPsec VPN на R1 и R3

Стъпка 1: Проверка на връзката между R1 и R3.

a. Ping от PC-A до PC-C

Стъпка 2: Позволете IKE политиките на R1 и R3.

```
R1(config)# crypto isakmp enable

R3(config)# crypto isakmp enable
```

b. Създйте Internet Security Association and Key Management Protocol (ISAKMP) политиката

```
R1(config)# crypto isakmp policy 10
```

c. Разгледайте различните IKE параметри позволени в Cisco IOS.

```
R1(config-isakmp)# ?
ISAKMP commands:   authentication  Set authentication method for
protection suite   default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite   exit
Exit  from  ISAKMP  protection  suite  configuration  mode      group
Set the Diffie-Hellman group   hash            Set hash algorithm for
protection suite   lifetime         Set lifetime for ISAKMP security
association   no             Negate a command or set its defaults
```

Стъпка 3: Конфигурирайте ISAKMP на R1 и R3.

a. Конфигурийрате ISAKMP политиката.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha
R1(config-isakmp)# group 5
```

```
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# end

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# end
```

c. Проверете IKE политиката.

```
R1# show crypto isakmp policy
Global IKE policy
Protection suite of priority 10  encryption algorithm: AES -
   Advanced Encryption Standard (256 bit keys).
   hash algorithm:            Secure Hash Standard
   authentication method:     Pre-Shared Key
   Diffie-Hellman group:      #5 (1536 bit)
   lifetime:                  3600 seconds, no volume limit
```

Стъпка 4: Конфигурийте pre-shared ключове на R1 и R3.

```
R1(config)# crypto isakmp key cisco123 address 10.2.2.1

R3(config)# crypto isakmp key cisco123 address 10.1.1.1
```

Стъпка 5: Конфигурирайте IPsec transform set и време на живот.

a. Конфигуриране на transformset

```
R1(config)# crypto ipsec transform-set 50 ?
  ah-md5-hmac   AH-HMAC-MD5 transform   ah-sha-
hmac   AH-HMAC-SHA transform
  comp-lzs      IP Compression using the LZS compression algorithm
esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
esp-aes       ESP transform using AES cipher   esp-des       ESP
transform using DES cipher (56 bits)   esp-md5-hmac  ESP transform
using HMAC-MD5 auth   esp-null      ESP transform w/o cipher
  esp-seal      ESP transform using SEAL cipher (160 bits)   esp-sha-
hmac  ESP transform using HMAC-SHA auth
```

b. Кофигуриране на transform set на R1 и R3.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#exit
```

c. Конфигуриране на време на живот.

```
R1(config)# crypto ipsec security-association lifetime seconds 1800

R3(config)# crypto ipsec security-association lifetime seconds 1800
```

Стъпка 6: Определете трафика, който ще минава през тунела.

За да може да се възползвате от IPsec криптирането във VPN, трябва да дефинирате разширена листа за достъп(Access List), която да казва да рутера кой трафик да бъде криптиран.

a. Конфигурате на интересен трафик на R1.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

b. Конфигурате на интересен трафик на R3.

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Стъпка 7: Създайте и изполватейте криптирана карта (crypto map).

Криптирана карта асоциира трафика от листата за достъп със IPsec и IKE настройките. След като е създадена тя може да бъде приложенана един или повече интерфейси(те трябва да бъде тези които съотевтстват на IPsec пиъра).

a. Създаване на crypto map на R1, с име CMAP и да използва 10 като пореден номер.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer  and
a valid access list have been configured.
```

b. Използвайте **match address** *access-list* командата, за да кажете криптираната карта с коя листа за достъп се използва.

```
R1(config-crypto-map)# match address 101
```

c. За да видите възможните опции на командата set използвайте ?.

```
R1(config-crypto-map)# set ?
Identity             Identity restriction.
Ip                   Interface Internet Protocol config commands
isakmp-profile     Specify isakmp Profile  nat
         Set NAT translation  peer
Allowed Encryption/Decryption peer.  pfs
Specify pfs settings
security-association Security association parameters
transform-set      Specify list of transform sets in priority order  e.
```

Задайте адреса на отдалечената точка. В нашият случай това е R3 – 10.2.2.1.

```
R1(config-crypto-map)# set peer 10.2.2.1
R1(config-crypto-map)# set pfs group5
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

f. Направете огледално копие и на същите команди на R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.1.1.1
R3(config-crypto-map)# set pfs group5
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R3(config-crypto-map)# exit
```

g. Приложете картата на съответния интерфейс..

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map CMAP
*Jan 28 04:09:09.150: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config)# end
```

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map CMAP
*Jan 28 04:10:54.138: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config)# end
```

Задача 2: Проверка на Site-to-Site IPsec VPN конфигурацията

Стъпка 1: Проверка на IPsec конфигурацията на R1 и R3.

a. Използвайте командата **show crypto ipsec transform-set**, за да покажете конфигурираната IPsec политика във формата на transform set.

```
R1# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }  will
negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
will negotiate = { Transport,  },


R3# show crypto ipsec transform-set
Transform set 50: { esp-256-aes esp-sha-hmac }  will
negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
will negotiate = { Transport,  },
```

b. Изполваствайте **show crypto map** командата, за да покажете crypto map.

```
R1# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.2.2.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

  Current peer: 10.2.2.1
  Security association lifetime: 4608000 kilobytes/900 seconds
PFS (Y/N): Y
  DH group:  group5
  Transform sets={
         50: { esp-256-aes esp-sha-hmac  } ,
        }
  Interfaces using crypto map MYMAP: Serial0/0/0

R3# show crypto map
Crypto Map "CMAP" 10 ipsec-isakmp
  Peer = 10.1.1.1
  Extended IP access list 101
  access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

  Current peer: 10.1.1.1
  Security association lifetime: 4608000 kilobytes/900 seconds
PFS (Y/N): Y
```

```
DH group:  group5
Transform sets={
       50: { esp-256-aes esp-sha-hmac  } ,
      }
Interfaces using crypto map MYMAP: Serial0/0/1
```

c. Използвайте **show crypto map** командата, за да покажете crypto map.

С **show crypto isakmp sa** командата показвате, че не съществуваIKE SAs.

```
R1# show crypto isakmp sa
 dst src state    conn-id slot status
```

d. Използвайте show crypto ipsec sa командата, за да покажете неизползваните SA между R1 и R3.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.1 port 500      PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0      current
outbound spi: 0x0(0)
      inbound esp sas:
inbound ah sas:
inbound pcp sas:
outbound esp sas:
outbound ah sas:
outbound pcp sas:
```

Резултати

След приключване на упражнението студентите ще имат познания в областта на VPN технологията, IPsec протоколът, Протокол Encapsulating Security Payload, Протокол Internet Key Exchange (IKE) и приложението им върху Cisco устойства при изграждането на Site-to-Site VPN.

Използвана литература

1. Cisco Security v1.1
2. Компютърни мрежи и комуникации – Иван Цонев, Станимир Станев
3. Дебра Литълджон Шиндър – „Компютърни мрежи”
4. James S Tiller :VPN - A Technical Guide to IPSec Virtual Private Networks

5. www
   - www.cisco.com