**Packet Tracer - Sieť VPN B (06)**

A diagram of a computer network

Description automatically generated**Dokumentačná práca**

**Zadanie**

Navrhnite šifrovanú sieť VPN cez internet tak, aby na jednom konci bola lokálna sieť s počítačmi a HTTP serverom, a na druhom konci bolo možné z pripojených zariadení navštíviť web stránku serveru cez VPN tunel, tak aby z inej siete mimo VPN komunikáciu nebolo možné tento HTTP server zobraziť (overte pridaním zariadení v internete).

**Požiadavky**

* Dve samostatne siete prepojené šifrovaným VPN tunelom.
* Server s HTTP protokolom dostupný iba cez VPN a z lokálnej siete.
* Overenie pridaním zariadení v internete.

**Adresná Schéma**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Názov  Zariadenia | Interface | Adresa | Subnet maska | Pripojené zariadenie | |
| Názov zariadenia | Interface |
| Router1 | Gig0/0 | 192.168.10.1 | 255.255.225.0 | Switch1 | Fa0/1 |
| Gig0/1 | 11.0.0.1 | 255.255.255.252 | Router3 | Gig0/1 |
| Router2 | Gig0/0 | 192.168.20.1 | 255.255.225.0 | Switch2 | Fa0/1 |
| Gig0/1 | 12.0.0.1 | 255.255.255.252 | Router3 | Gig0/2 |
| Router3 | Gig0/0 | 192.168.30.1 | 255.255.225.0 | Laptop3.1 | Fa0 |
| Gig0/1 | 11.0.0.2 | 255.255.255.252 | Router1 | Gig0/1 |
| Gig0/2 | 12.0.0.2 | 255.255.255.252 | Router2 | Gig0/1 |
| Switch1 | Fa0/1 | N/A | N/A | Router1 | Gig0/0 |
| Fa0/2 | N/A | N/A | Laptop1.1 | Fa0 |
| Fa0/3 | N/A | N/A | PC1 | Fa0 |
| Fa0/4 | N/A | N/A | Laptop1.2 | Fa0 |
| Fa0/5 | N/A | N/A | Server1 | Fa0 |
| Switch2 | Fa0/1 | N/A | N/A | Router2 | Gig0/0 |
| Fa0/2 | N/A | N/A | Laptop2.2 | Fa0 |
| Fa0/3 | N/A | N/A | Laptop2.1 | Fa0 |
| Fa0/4 | N/A | N/A | Server2 | Fa0 |
| Server1 | Fa0 | 192.168.10.2 | 255.255.255.0 | Switch1 | Fa0/5 |
| Server2 | Fa0 | 192.168.20.2 | 255.255.255.0 | Switch2 | Fa0/4 |
| PC1 | Fa0 | DHCP | DHCP | Switch1 | Fa0/3 |
| Laptop1.1 | Fa0 | DHCP | DHCP | Switch1 | Fa0/2 |
| Laptop1.2 | Fa0 | DHCP | DHCP | Switch1 | Fa0/4 |
| Laptop2.1 | Fa0 | DHCP | DHCP | Switch2 | Fa0/3 |
| Laptop2.2 | Fa0 | DHCP | DHCP | Switch2 | Fa0/2 |
| Laptop3.1 | Fa0 | 192.168.30.2 | 255.255.255.0 | Router3 | Gig0/0 |

**Postup**

**Konfigurácia DNS Protokolu**

DNS protokol zabezpečuje preklad čitateľných názvov domén na IP adresy serverov a naopak. Pomocou nasledujúceho obrázka nastavíme DNS protokol, aby sme mohli mat prístup k vzájomným stránkam. HTTP protokol je na cisco packet serveroch automaticky zapnutý od začiatku, preto ho netreba zapínať. Názov záznamu som zvolil “site1.com” a “site2.com”. Číslami som označoval poradie siete, jednotka v tomto návrhu patrí sieti (192.168.10.0/24), dvojka (192.168.20.0/24). Typ bude record A, pretože v tomto prípade chceme prekladať IPV4. A nakoniec som už iba zvolil príslušnú IPV4 servera s HTTP protokolom (v smerovači “Router1” na „192.168.10.2“ a v „Routri2“ na „192.168.20.2“). Uvažoval som ešte o spoločnom DNS serveri na internete (bola by to jednoduchšia správa), ale priklonil som sa k tomuto riešeniu, pretože ponúka vyššiu bezpečnosť. Takto by útočník, ktorý by sa chcel dostať k DNS serveru, musel najprv preniknúť do jednej zo sietí.

// Konfigurácia serveru “Server1”

A screenshot of a computer

Description automatically generated

// Konfigurácia serveru “Server2”

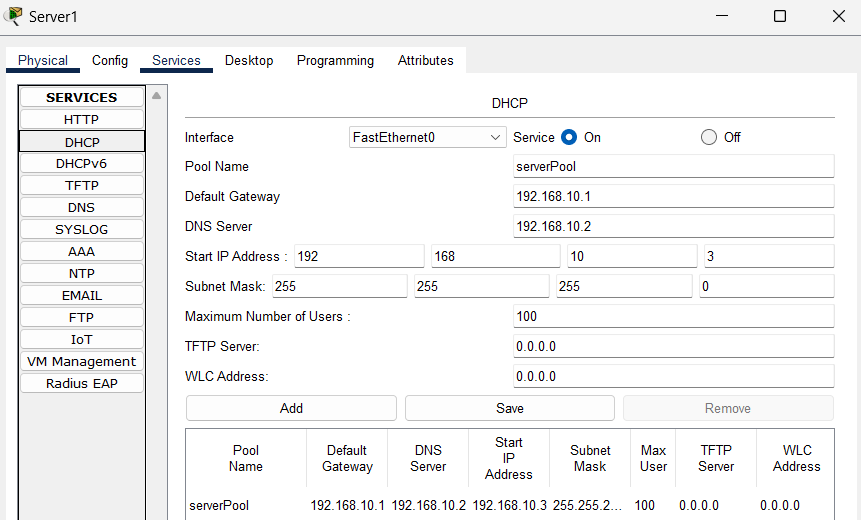
**A screenshot of a computer

Description automatically generated**

**Konfigurácia DHCP Protokolu**

Pomocou nasledujúceho obrázka nastavíme automatické prideľovanie IP adries na zariadenia. Ako default gateway v serveri ”Server1” nastavíme IP adresu smerovača “Router1” a gateway v serveri ”Server2” nastavíme IP adresu smerovača “Router2”. DNS službu poskytujú ony samotné takže do políčka napíšeme ich vlastnú IP adresu. Keďže IP adresa smerovačov sa končí 1 a serverov 2, pri maske 24 sa tak prvá IP adresa sa bude na konci 3. Maska siete bude v obidvoch prípadoch 24 (255.255.255.0). A maximálny počet zariadení nastavíme taktiež v obidvoch prípadoch na 100.

// Konfigurácia serveru “Server1”



// Konfigurácia serveru “Server2”

A screenshot of a computer

Description automatically generated

**Konfigurácia statických ciest**

V termináloch smerovačov „Router1“ a „Router2“ nakonfigurujeme statické smerovacie cesty smerom na “Router3”, v smerovači “Router3” ich prepojíme.

>ip route 0.0.0.0 0.0.0.0 11.0.0.2 // Na smerovači “Router1”

>ip route 0.0.0.0 0.0.0.0 12.0.0.2 // Na smerovači “Router2”

>ip route 192.168.10.0 255.255.255.0 11.0.0.1 // Na smerovači “Router3”

>ip route 192.168.20.0 255.255.255.0 12.0.0.1

**Aktivácia licenčného balíčka s funkciou VPN**

V termináloch smerovačov „Router1“ a „Router2“ následne aktivujeme potrebný licenčný balíček „securityk9“. Aktivácia tohto balíčka zabezpečuje, že zariadenie môže vykonávať pokročilé bezpečnostné operácie pre tento prípad ho budeme potrebovať na IPSEC, VPN, AES, ESP, ISAKMP a crypto mapy.

>enable (or en) // Prepnutie sa do privilege módu

>show version // Vypísanie stavu smerovača

>configure terminal (or conf t) // Prepnutie sa do konfiguračného módu

// Aktivácia licenčného balíčka s funkciou VPN

>license boot module c1900 technology-package securityk9

>exit // Odídenie z konfiguračného módu

// Uloženie aktuálnej bežiacej konfigurácie do štartovacej konfigurácie

>copy running-config startup-config (or copy run start)

>reload // Reštartovanie smerovača

**Konfigurácia access listu**

Na reguláciu vstupu packetov napíšeme nasledovné zoznamy pravidiel na smerovače „Router1“ a „Router2“. Ich úlohou je definovať packety na zašifrovanie, povoliť packety zo vzájomných sieti, zakázať packety z ostatných sieti na servery a povoliť prístup všetkým sieťam k ostatným zariadeniam. Dôvod je aby medzi sieťami 192.168.10.0/24 a 192.168.20.0/24 bola bezpečná šifrovaná komunikácia a zároveň aby len oni navzájom mali prístup k serverom “Server1” a “Server2”.

// Router1

>access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255

>access-list 101 permit ip 192.168.20.0 0.0.0.255 host 192.168.10.2

>access-list 101 deny ip any host 192.168.10.2

>access-list 101 permit ip any any

// Router2

>access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

>access-list 101 permit ip 192.168.10.0 0.0.0.255 host 192.168.20.2

>access-list 101 deny ip any host 192.168.20.2

>access-list 101 permit ip any any

**Konfigurácia ISAKMP politiky a prednastaveného kľúča**

V tomto kroku nastavíme ISAKMP politiku pre definovanie pravidiel, ako sa má vyjednávať a overovať bezpečná komunikácia cez VPN. ISAKMP sa používa na výmenu bezpečnostných kľúčov a overenie ešte pred samotným vytvorením šifrovaného tunela. Prioritu väčšinou nastavujem po 10 a pre prioritu platí čim menšie číslo tým vyššia priorita. V tomto prípade bude len jedna politika, takže na čísle až tak nezáleží (zvolil som prioritu 10). Enkrypcia predstavuje typ šifrovania, ktorý bude použitý pri vytváraní ISAKMP spojenia. Na šifrovanie dát som zvolil najsilnejší algoritmus aký smerovač ponúkal, AES 256. Autentifikácia, spôsob akým budú zariadenia autentifikované je nastavená pomocou prednastaveného tajného kľúča (jediná možnosť). Diffie-Hellmanova skupina je algoritmus, ktorý umožňuje dvom stranám bezpečne vymeniť si šifrovacie kľúče. Zvolil som najbezpečnejšiu ponúkanú (skupinu 5) s dĺžku kľúča 1536 bitov. Zdieľaný kľuč som v tomto návrhu siete zvolil jednoduchý, ľahko zapamätateľný (secret), s IP druhého smerovača ku ktorému sa bude pripájať.

// Router1

>crypto isakmp policy 10 // Priorita politiky 10

>encryption aes 256 // AES enkrypcia s dĺžkou kľúča 256bit

>authentication pre-share // Autentizácia pomocou zdieľaného kľúča

>group 5 // Zabezpečená výmena šifrovacích kľúčov

>crypto isakmp key secret address 12.0.0.1 // Kľuč a IP druhého zariadenia

// Router2

>crypto isakmp policy 10

>encryption aes 256

>authentication pre-share

>group 5

>crypto isakmp key secret address 11.0.0.1

**Konfigurácia transformačnej sady IPSec**

V prvom kroku vo fáze 2 nastavovaní IPSec VPN tunela vytvoríme transformačnú sadu, ktorá zabezpečí šifrovanie a overenie pravosti dát. Názov transformačnej sady, ktorým ju identifikujeme som nazval “net1->net2” a “net2->net1”. Ako šifrovací algoritmus na enkrypciu dát som zvolil AES s dĺžkou kľúča 256bitov, pretože je najbezpečnejší a jeden z najpoužívanejší z pomedzi ponúkaných smerovačov. Algoritmus na overenie pravdivosti dát, ktorý zabezpečuje, aby prenášané dáta neboli počas prenosu modifikované, som zvolil SHA spolu s mechanizmom HMAC. SHA-HMAC som zvolil pretože je spoľahlivejší ako MD5-HMAC a celkovo sa poväzuje ako aktuálny bezpečnostný štandard. Protokol som mal na vyber z “AH” a “ESP”. Vhodnejší mi prišiel ESP, pretože na rozdiel od AH je šifrovaný.

// Router1

>crypto ipsec transform-set net1->net2 esp-aes 256 esp-sha-hmac

// Router2

>crypto ipsec transform-set net2->net1 esp-aes 256 esp-sha-hmac

**Konfigurácia IPSec a jej pridelenie**

V tomto kroku (druhom vo fáze 2) nakonfigurujeme krypto mapu, konfiguráciu, ktorá viaže všetky nastavenia potrebné pre IPSec tunel (ako peer IP, transformačnú sadu, PFS, access-list) do jedného súvislého celku. Názov som zvolil “MAP1” pri obidvoch smerovačov. Na priorite až tak nezáleží, pretože v návrhu obsahujú obidva smerovače iba jednu krypto mapu. V tomto prípade som zvolil číslo 10. Peer je adresa vzdialeného zariadenia / smerovača v tomto prípade “12.0.01” a “11.0.0.1”. PFS, funkciu ktorá zabezpečuje že pri každom novom šifrovanom prenose sa používajú unikátne šifrovacie kľúče. Ako pri ISAKMP politike som ju zvolil na piatu Diffie-Hellmanovu skupinu pretože ponúka kľuč s najdlhšou ponúkanou dĺžkou kľúča. „Security-association lifetime“ udáva dĺžku životnosti kľúčov pred vytvorením nových (nastavil som ju aby mala životnosť 24 hodín, pretože to považujem za priemerný čas medzi bezpečnosťou a zaťažovaním). Potom som priradil v minulých krokoch nakonfigurovanú transformačnú sadu a access-list. Ku koncu už iba pridelíme k WAN interfacu smerovača aktuálne nastavenú krypto mapu.

// Router1

>crypto map MAP1 10 ipsec-isakmp // Názov mapy VPN-MAP

>set peer 12.0.0.1 // WAN IP „Routra2“

>set pfs group5 // DH skupina

>set security-association lifetime seconds 86400 // 24 Hodín

>set transform-set net1->net2 // Transformačná sada

>match address 100 // ACL

>int g0/1 // WAN Interface

>crypto map MAP1 // Pridelenie krypto mapy

// Router2

>crypto map MAP2 10 ipsec-isakmp

>set peer 11.0.0.1 // WAN IP „Routra1“

>set pfs group5

>set security-association lifetime seconds 86400

>set transform-set net2->net1

>match address 100

>int g0/1

>crypto map MAP2

**Pridelenie ACL smerovačom**

V jednom z predchádzajúcich krokov, kde sme nastavili IPSEC ACL, sme nastavili aj klasický ACL. V tomto kroku ho pridelíme na WAN interface aby filtroval prichádzajúce (inbound) packety. Fungovalo by to podobne, keby sme ho pridelili LAN interface, aby filtroval odchádzajúce packety, ale zbytočne by to zaťažovalo smerovač.

// Router1

> int g0/1 // WAN Interface

> ip access-group 101 in // Priradenie ACL 101

> show ip interface GigabitEthernet0/0 // Overenie

// Router2

> int g0/1

> ip access-group 101 in

> show ip interface GigabitEthernet0/0

**Bezpečnostné riziká**

V tomto návrhu siete som sa snažil nasimulovať šifrovane VPN spojenie medzi dvoma sieťami cez internet. Avšak je tam pár potenciálnych medzier, ktoré by sa dali využiť na neoprávnený prístup. Tu je popis niekoľkých potenciálnych bezpečnostných rizík:

1. **Slabá bezpečnosť medzi sieťami "192.168.10.0/24” a “192.168.20.0/24”**

~ Medzi sieťami "192.168.10.0/24” a “192.168.20.0/24” je slabá bezpečnosť. Ak by útočník prenikol do jednej, mal by veľký prístup k druhej. Aby sa tomuto vyhlo, bolo by potrebné implementovať firewally a bezpečnostné prvky medzi týmito sieťami. Tieto opatrenia by umožnili definovať prísnejšie pravidlá prístupu a filtrovanie medzi sieťami, napríklad povoliť len konkrétne porty alebo protokoly, ktoré sú nevyhnutné pre komunikáciu medzi zariadeniami, a zablokovať všetky ostatné.

1. **Nešifrovaná komunikácia s HTTP serverom**

~ V tomto návrhu je podľa zadania na serveri pristúpený HTTP protokol. Bez šifrovania cez protokol HTTP sú údaje prenášané v textovej podobe, čo môže umožniť ich zachytenie a manipuláciu útočníkmi. Riešením v tomto prípade na ochranu citlivých informácií je potrebné použiť iba HTTPS na šifrovanie komunikácie medzi zariadením a serverom.