**Dokumentácia k sieti VPN s tlačiarňou**

**Popis siete**

V návrhu siete sme vytvorili dve samostatné lokálne siete, ktoré sú prepojené cez VPN tunel. Na jednej strane siete je lokálna sieť s DHCP serverom, počítačmi a sieťovou tlačiarňou, zatiaľ čo na druhej strane je vzdialená sieť s DHCP serverom a počítačom. Komunikácia medzi týmito sieťami je umožnená pomocou tunela vytvoreného cez smerovače.

**Zariadenia:**

* **Router0 a Router1:** Smerovače typu 1941 s pridaným modulom HWIC-2T sme nakonfigurovali tak, aby umožnili prepojenie oboch sietí cez sériové spojenie a vytvorenie VPN tunela. Nastavením statických trás sme zabezpečili smerovanie medzi sieťami.
* **Server1 a Server2:** DHCP servery sme nastavili na automatické prideľovanie IP adries zariadeniam v jednotlivých lokálnych sieťach. To zjednodušuje správu IP adries a minimalizuje manuálne zásahy.
* **Switch0 a Switch1:** Switche sme použili na prepojenie zariadení v rámci lokálnych sietí. Umožňujú jednoduchú a efektívnu komunikáciu medzi zariadeniami.
* **Laptop0:** Predstavuje klienta v lokálnej sieti, ktorý prijíma IP adresu z DHCP servera.
* **Printer0:** Sieťovú tlačiareň sme nastavili s pevnou IP adresou (192.168.1.101), aby bola vždy dostupná na tej istej adrese.
* **PC1:** Predstavuje klienta vo vzdialenej sieti, ktorý tiež prijíma IP adresu z DHCP servera.

**Konfigurácia**

**Konfigurácia Router0 (lokálna sieť)**

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

* Nastavenie IP adresy pre lokálnu sieť, ktorá slúži ako brána pre zariadenia v tejto sieti.

interface Serial0/1/0

ip address 10.0.1.1 255.255.255.252

clock rate 64000

no shutdown

* Nastavenie IP adresy pre sériové rozhranie a zapnutie rozhrania. Hodnota "clock rate" je potrebná na strane DCE.

ip route 192.168.2.0 255.255.255.0 10.0.2.2

* Statická trasa na smerovanie paketov do vzdialenej siete.

interface Tunnel0

ip address 10.0.2.1 255.255.255.252

tunnel source Serial0/1/0

tunnel destination 10.0.1.2

no shutdown

* Vytvorenie tunela medzi lokálnou a vzdialenou sieťou. IP adresy tunela umožňujú virtuálne prepojenie medzi smerovačmi.

**Konfigurácia Router1 (vzdialená sieť)**

interface GigabitEthernet0/0

ip address 192.168.2.1 255.255.255.0

no shutdown

* Nastavenie IP adresy pre vzdialenú sieť, ktorá slúži ako brána pre zariadenia v tejto sieti.

interface Serial0/1/0

ip address 10.0.1.2 255.255.255.252

no shutdown

* Nastavenie IP adresy pre sériové rozhranie a zapnutie rozhrania.

ip route 192.168.1.0 255.255.255.0 10.0.2.1

* Statická trasa na smerovanie paketov do lokálnej siete.

interface Tunnel0

ip address 10.0.2.2 255.255.255.252

tunnel source Serial0/1/0

tunnel destination 10.0.1.1

no shutdown

* Vytvorenie tunela pre bezpečné spojenie medzi smerovačmi.

**Konfigurácia DHCP serverov**

Na Server1 a Server2 sme nastavili DHCP službu s nasledovnými parametrami:

* **Default Gateway:** 192.168.1.1 (Server1), 192.168.2.1 (Server2)
* **DNS Server:** 8.8.8.8
* **Start IP Adress:** 192.168.1.100 (Server1), 192.168.2.100 (Server2)

Toto zabezpečuje automatické prideľovanie IP adries zariadeniam v lokálnych sieťach.

**Konfigurácia Laptop0 a PC1**

V Laptop0 a PC1 sme nastavili IP configuration tak, nech sa používa DHCP a nie statická IP adresa.

**Prečo nebolo použité šifrovanie (IPSec)?**

V Cisco Packet Traceri šifrovanie IPSec nebolo možné implementovať, pretože príkaz na aktiváciu IPSec nebol dostupný. Toto môže byť obmedzenie verzie Packet Traceru alebo nepodporovaná funkcia na dostupných routeroch.

**Bezpečnostné riziká**

* **Nedostatok šifrovania:** Prenosové dáta medzi smerovačmi sú nechránené, čo môže viesť k ich odpočúvaniu.
* **Chybná konfigurácia:** Nesprávne nastavenie IP trás alebo tunela môže viesť k výpadku komunikácie.
* **Prístup k DHCP serverom:** Ak nie sú servery zabezpečené, môže dôjsť k neoprávnenému prístupu a manipulácii s nastaveniami siete.