Packet Tracer: VPN

Què és una VPN? Clica aquí.

Introducció

Configurarem una VPN Site-to-Site.

L'objectiu és assegurar el trànsit entre xarxes LAN mitjançant un túnel xifrat que garanteixi la confidencialitat, integritat i autenticitat de les dades.

Aquesta configuració és ideal per a empreses que necessiten connectar oficines remotes de manera segura, aprofitant Internet com a mitjà de transport.

Configuració d'un túnel IPSec

Per establir un túnel xifrat entre els routers utilitzarem polítiques de seguretat, llistes d'accés i clau pre-compartida que només coneixen els routers. Cal que es garanteixi que només el trànsit permès passa a través del túnel.

Les següents instruccions aplicades a cada router configuren la seguretat per a la connexió VPN:

Configuració de la política ISAKMP per establir una sessió segura per l'intercanvi de claus entre els routers. S'estableix que l'autenticació serà mitjançant una clau pre-compartida.

Configuració de la clau pre-compartida per a l'autenticació.

crypto isakmp key <CLAU_PRE_COMPARTIDA> address <IP_PEER>

Definició de polítiques de seguretat.

crypto ipsec transform-set <NOM_TRANSFORM_SET> esp-<ALG_XIFRAT> esp-<ALG_HASH>-hmac

Definició de regla ACL.

access-list <NUM ACL> permit ip <XARXA ORIGEN> <MASCARA 1> <XARXA DESTI> <MASCARA 2>

Creació d'un mapa criptogràfic.

Aplicació del mapa criptogràfic a una interfície.

```
interface <INTERFACE>
crypto map <NOM_MAPA>
```

Finalment, guardem la configuració usant la comanda: wr

Per assegurar que la configuració de la VPN és correcta, podem utilitzar les següents comandes:

show crypto isakmp sa show crypto ipsec sa

Aquestes comandes mostren l'estat de les associacions de seguretat (SA) i el trànsit xifrat a través del túnel amb els paquets enviats i rebuts.

Explicació dels placeholders:

<POLITICA_ID>: Identificador de la política ISAKMP. Les polítiques amb números més baixos tenen més prioritat.

<ALG_HASH>: Algorisme utilitzat per a la integritat.

<ALG_XIFRAT>: Algorisme de xifrat utilitzat.

<LLARGADA_XIFRAT>: Longitud del xifrat en bits.

<GRUP_DIFFIE_HELLMAN>: Grup de Diffie-Hellman utilitzat. Paràmetre que defineix el nivell de seguretat en l'intercanvi de claus criptogràfiques en una connexió VPN.

< VIDA_SESSIO>: Temps, en segons, durant el qual la sessió ISAKMP serà vàlida.

<CLAU_PRE_COMPARTIDA>: La clau pre-compartida per a l'autenticació entre els dispositius.

<IP_PEER>: L'adreça IP / gateway del router remot amb qui es vol establir la connexió VPN.

<NOM_TRANSFORM_SET>: El nom del conjunt de transformació.

<NUM_ACL>: El número de la llista d'accés. Usarem ACL extesa, per tant serà un valor entre 100 i 199.

<XARXA_ORIGEN> i <XARXA_DESTI>: Les xarxes locals que volen establir la connexió VPN.

<MASCARA_1> i <MASCARA_2>: Les màscares de subxarxa de cadascuna de les xarxes locals.
Usarem wildcard: És una màscara utilitzada en ACL per definir rangs d'adreces IP. A diferència de la màscara de subxarxa, que utilitza "1" per identificar bits de xarxa, la màscara wildcard utilitza "1" per als bits que no són de xarxa.

Per exemple:

Xarxa: 192.168.1.0 / 24

En lloc de 255.255.255.0, seria: 0.0.0.255.

<NOM_MAPA>: El nom del mapa criptogràfic.

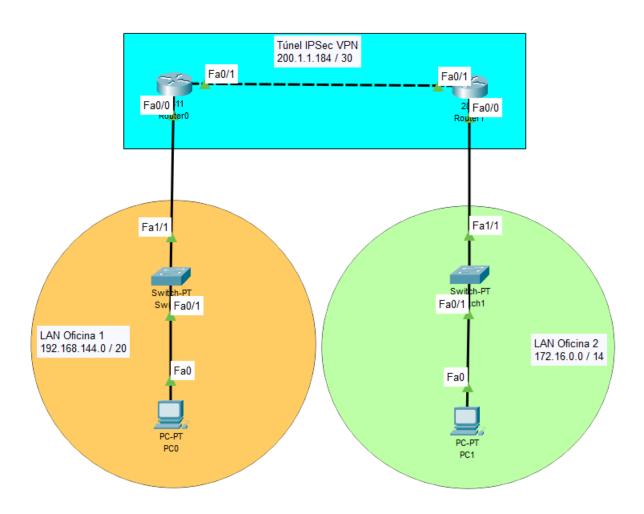
<INTERFACE>: El nom de la interfície on aplicaràs el mapa criptogràfic, per exemple: Fa0/0.

ACTIVITATS

Implementació d'una VPN

Volem establir una VPN Site-to-Site entre dues xarxes (192.168.144.0 / 20 i 172.16.0.0 / 14). La VPN ens permetrà comunicar dues oficines remotes de manera que fos com si estiguessin a la mateixa xarxa.

Per configurar un túnel IPsec VPN utilitzarem routers Cisco 2811, aquests routers suporten IPSec per a connexions segures entre dues xarxes diferents.



Passos principals en la configuració:

1. Configurar xarxes i assignació d'adreces IPs:

LAN Oficina 1 → 192.168.144.0 / 20 IP PC: última IP disponible per assignar.

IP Gateway router: primera IP disponible per assignar.

LAN Oficina 2 → 172.16.0.0 / 14

IP PC: última IP disponible per assignar.

IP Gateway router: primera IP disponible per assignar.

Túnel IPSec VPN → 200.1.1.184 / 30 2 adreces disponibles per a dispositius.

- 2. Configurar **enrutament estàtic** perquè els routers puguin dirigir el trànsit correctament entre les xarxes remotes, cal definir camins manuals entre xarxes, per tal que els routers sàpiguen cap a on enviar el trànsit quan no tenen contacte directe amb la xarxa destí.
- 3. Creem el **túnel xifrat**. Alguns dels valors que usarem:
 - Identificador de la política ISAKMP: 10, prioritat mitjana.
 - Algorisme de generació de hash: sha, un dels més segurs.
 - Algorisme de xifrat i longitud: aes (256 bits), molt segur i eficient.
 - Grup de Diffie-Hellman per l'intercanvi de claus: 2 (1024 bits).
 - Durada sessió ISAKMP: 24 hores, per tenir un equilibri entre seguretat i eficiència.
 - Clau pre-compartida: El vostre nom de pila.
- 4. **Comprovar** que, efectivament, els paquets encriptats arriben al seu destí.

BIBLIOGRAFIA I WEBGRAFIA

- ${\it ``CBT nuggets"}. \ {\it $\underline{}$https://www.cbtnuggets.com/blog/technology/networking/how-ipsec-site-to-site-vpn-tunnels-work}$
- «Netgate Docs». https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html
- «itexamanswers». https://itexamanswers.net/8-4-1-2-packet-tracer-configure-verify-site-site-ipsec-vpn-using-cli-answes.html



Autor: Xavier Baubés Parramon Aquest document es llicència sota Creative Commons versió 4.0. Es permet compartir i adaptar el material però reconeixent-ne l'autor original.