Diseño y Seguridad de Redes

Práctica 2: VPN y ASA

Curso 2017-2018

Descripción

La empresa LabRedes.com dispone de una Sede Central, donde se encuentran la mayoría de sus trabajadores, y donde se alojan diversos servicios de la empresa, tanto públicos como de uso interno. Además, la empresa dispone de dos sucursales remotas, Sucursal A y Sucursal B. Tanto la sede central como las sucursales se encuentran conectadas a Internet. La sede central dispone de direccionamiento privado, pero en las sucursales hay direccionamiento público.

Esta práctica se centra en la Red Interna de la sede central.

La práctica consiste en configurar enlaces GRE-IP y VPN, así como un dispositivo ASA.

Fichero inicial

Diagrama de topología

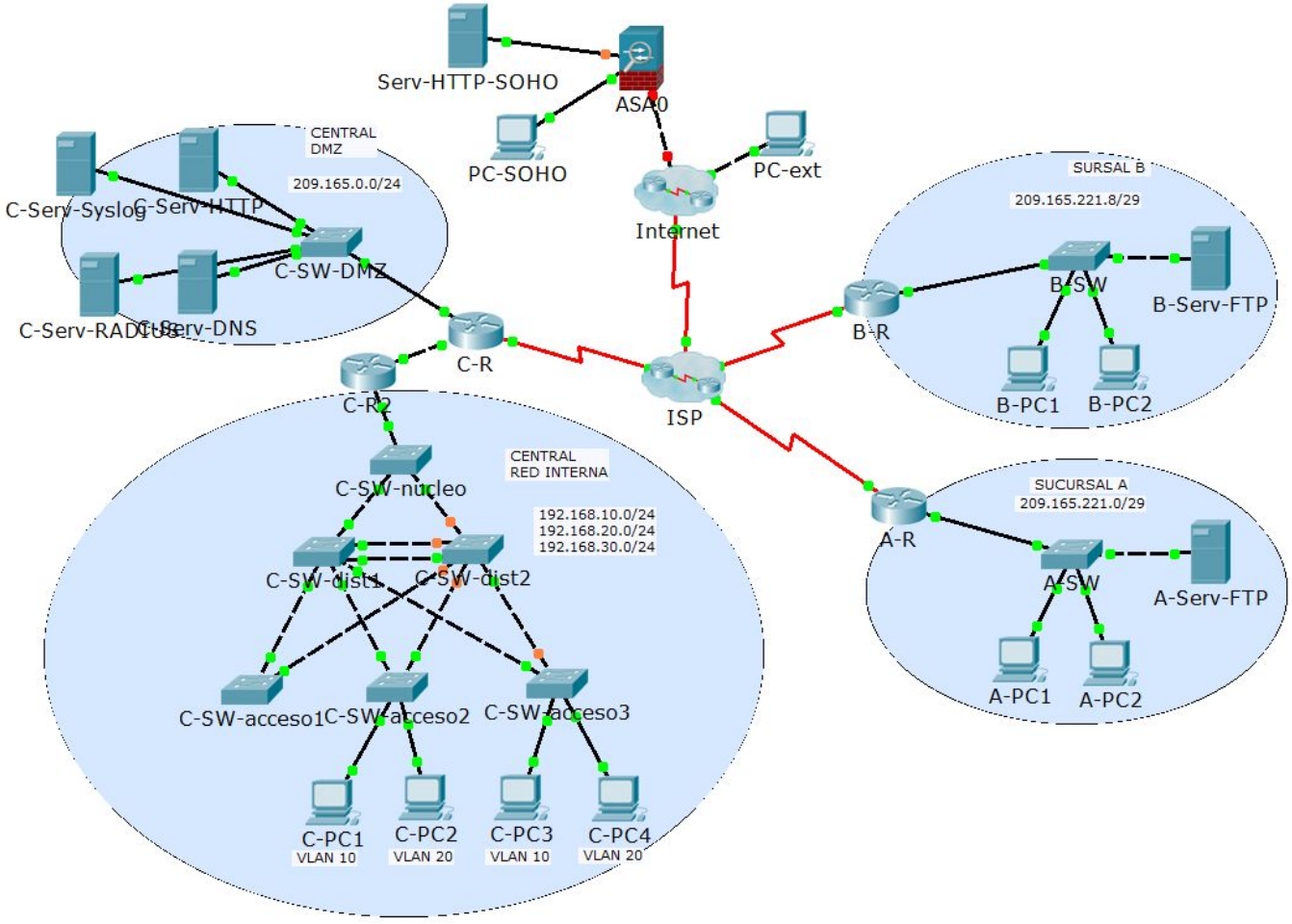

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
Serv-HTTP-SOHO	NIC	dhcp (privada 1)		
PC-SOHO	NIC	dhcp (privada 2)		
ASA	Eth	209.165.232.10	255.255.255.248	209.165.232.9
PC-ext	NIC	209.165.232.18	255.255.255.248	209.165.232.17
C-R	S0/0/0	209.165.210.2	255.255.255.252	
	Fa0/1	209.165.0.1	255.255.255.248	
	Fa0/0.10	192.168.10.254	255.255.255.0	
	Fa0/0.20	192.168.20.254	255.255.255.0	
	Fa0/0.30	192.168.30.254	255.255.255.0	
C-Serv-HTTP	NIC	209.165.0.10	255.255.255.248	209.165.0.1
C-Serv-DNS	NIC	209.165.0.11	255.255.255.248	209.165.0.1
C-Serv-RADIUS	NIC	192.168.30.2	255.255.255.0	192.168.30.254
C-Serv-Syslog	NIC	192.168.30.1	255.255.255.0	192.168.30.254
C-PC1	NIC	192.168.10.1	255.255.255.0	192.168.10.254
C-PC2	NIC	192.168.20.1	255.255.255.0	192.168.20.2544
C-PC3	NIC	192.168.10.2	255.255.255.0	192.168.10.254
C-PC4	NIC	192.168.20.2	255.255.255.0	192.168.20.254
C-SW-nucleo	VLAN30	192.168.30.11	255.255.255.0	192.168.30.254
C-SW-dist1	VLAN30	192.168.30.12	255.255.255.0	192.168.30.254
C-SW-dist2	VLAN30	192.168.30.13	255.255.255.0	192.168.30.254
C-SW-acceso1	VLAN30	192.168.30.14	255.255.255.0	192.168.30.254
C-SW-acceso2	VLAN30	192.168.30.15	255.255.255.0	192.168.30.254
C-SW-acceso3	VLAN30	192.168.30.16	255.255.255.0	192.168.30.254
B-R	S0/0/0	209.165.212.2	255.255.255.252	
	Fa0/0	209.165.221.9	255.255.255.248	
B-Serv-FTP	NIC	209.165.221.10	255.255.255.248	209.165.221.9
B-PC1	NIC	209.165.221.13	255.255.255.248	209.165.221.9
B-PC2	NIC	209.165.221.14	255.255.255.248	209.165.221.9
A-R	S0/0/0	209.165.211.2	255.255.255.252	
	Fa0/0	209.165.221.1	255.255.255.248	
A-Serv-FTP	NIC	209.165.221.2	255.255.255.248	209.165.221.1

A-PC1	NIC	209.165.221.5	255.255.255.248	209.165.221.1
A-PC2	NIC	209.165.221.6	255.255.255.248	209.165.221.1

Tareas

Tarea 1. Configurar un túnel GRE-IP entre sucursales

Establezca un túnel con encapsulación GRE sobre IP entre las dos sucursales. Establezca el encaminamiento necesario para que el tráfico entre sucursales utilice dicho túnel, y compruebe que esto es así realizando un traceroute entre equipos de ambas sucursales y viendo que los routers de Internet no aparecen en el camino.

En caso de tener direccionamiento privado en las sucursales ¿se podría prescindir de NAT para comunicar equipos diferente subred? Compruebe dicha afirmación creando una subred en la interfaz ~~Gigabit~~ libre de A-R y B-R, comunicándolas por el túnel anterior, **sin utilizar NAT**.

Tarea 2. Configuración de VPNs (1)

Configurar una VPN IPsec Site-to-Site para el tráfico entre la subred DMZ de la sede central, y la subred de la sucursal B (redes de direccionamiento público en ambos casos). A continuación se muestran los parámetros a utilizar en la fase 1 de ISAKMP y en la fase 2 de IPsec:

Parámetros de fase 1 ISAKMP	
Método	**ISAKMP**
Encryption Algorithm	**AES**
Number of Bits	**256**
Hash Algorithm	**SHA-1**
Authentication Method	**Pre-share**
Key Exchange	**DH 2**
IKE SA Lifetime	**86400**
ISAKMP Key	**Vpnpass101**

Parámetros de fase 2 IPsec	
Parámetros	**IPsec**

Transform Set	**esp-aes** **esp-sha-hmac**
Key Exchange	**DH 2**
SA Establishment	**ipsec-isakmp**

Una vez configurados los routers y grabada la configuración, reiniciar todos los routers implicados en la VPN. Verificar la configuración de VPN comunicando PCs de diferentes sucursales.

Comprobar que los paquetes DMZ y Sucursal B están encriptados pero no lo están entre DMZ y Sucursal A. Comprobar que en una ruta (traceroute) entre DMZ y Sucursal B no aparecen IPs de los routers de Internet.

Tarea 3. Configuración de VPNs (2)

Configurar una VPN IPsec Site-to-Site para el tráfico entre la subred de la VLAN 30 de la sede central, y la subred de la sucursal A. En este caso, la VLAN 30 tiene direccionamiento privado. Utilizar los mismos parámetros de IPsec que en el apartado anterior.

Para que funcione correctamente no debe olvidarse de excluir el tráfico de VLAN 30 a Sucursal A del NAT de C-R, asegurarse de que dicho tráfico se manda a Internet, y asegurarse que el tráfico de Sucursal A hacia las direcciones privadas de VLAN 30, en R-A, es enviado también hacia Internet (aunque los routers de Internet no lo interpreten).

Comprobar con traceroute que el tráfico de la Sucursal A a cualquier equipo de la VLAN 30 (usando la dirección IP privada como destino) llegan a través del túnel. Comprobar también (viendo los contadores de los SAs) que los mensajes de syslog y AAA se envían de la Sucursal A a los servidores encapsulados en dicho túnel IPsec.

> ~~NOTA: Se deberá habilitar en ZPF de entrada al router de A, tanto el puerto 500 de UDP, como el protocolo ESP. En caso de encontrar problemas, realizarlo en otro fichero sin ZPF activado en el router A-R.~~

Tarea 4. Configuración de un dispositivo ASA

Configure el firewall ASA de una empresa (SOHO, siglas de Small-Office - Home-Office) de forma que:

- Tenga una configuración básica
- Utilice 3 zonas, inside para PCs, outside hacia Internet y dmz hacia servidores. Cree más equipos si lo desea y asigne los puertos extra. Asigne dos rango de direcciones privadas internas a su elección.
- Se comporte como servidor DHCP para los PCs. Use direcciones estáticas en los servidores.
- Realice NAT con PAT sobre la dirección pública para los PCs internos.
- Realice NAT ~~dinámico~~ estático 1:1 para los servidores con las demás direcciones restantes del rango al que pertenece su dirección externa.

- Permita el tráfico al servidor HTTP, y a otros servicios que cree en la DMZ, desde Internet. Permita ICMP de dentro hacia dmz y outside.

Entrega

A la finalización de la práctica se deberá entregar una memoria que recoja:

- Comandos utilizados por cada tarea, comentando las decisiones tomadas
- Comentarios sobre las pruebas llevadas a cabo (comandos show, pings, *traceroutes*, conexiones ftp…), y capturas (textuales o imagen) de los resultado de las mismas
- Backup de la configuración de los routers y switches implicados (*running config*). Un fichero por cada dispositivo.
- Fichero PKT