Diseño y Seguridad de Redes

Práctica 1: Securización de dispositivos, AAA y Firewall

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 de la sede central

La práctica consiste en configurar firewalls en ciertos casos, y enlaces GRE-IP y VPN

~~Fichero inicial~~

Fichero inicial v2

Diagrama de topología

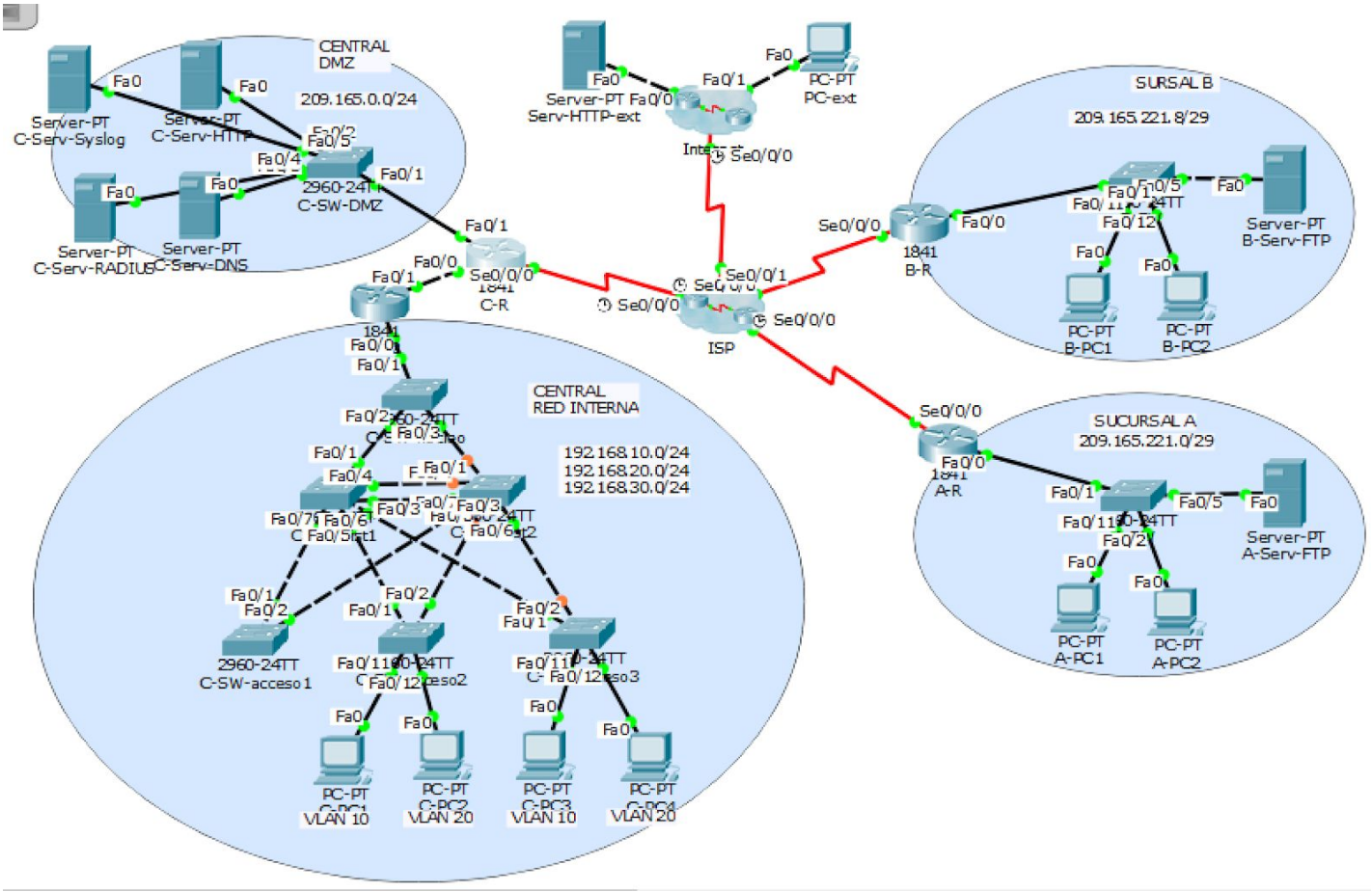

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway
Serv-HTTP-ext	NIC	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	192.168.40.1	255.255.255.252	
C-R2	Fa0/1	192.168.40.2	255.255.255.252	
	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	255.255.255.0	209.165.0.1
C-Serv-DNS	NIC	209.165.0.11	255.255.255.0	209.165.0.1
C-Serv-RADIUS	NIC	209.165.0.12	255.255.255.0	192.168.30.254
C-Serv-Syslog	NIC	209.165.0.13	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. Configuración básica

La Red Interna de la **Sede Central** está configurada con 3 VLANs, identificadas como 10, 20 y 30. Los puertos de los switches de acceso están asignados a las vlans 10 ó 20, y la vlan 30 se reserva para conectarse con los switches.

El router encamina entre las diferentes VLANs y hace NAT hacia el exterior (no hacia DMZ).

Asigne las direcciones IP correspondientes a los switches en la interfaz especial vlan 30 y, si se desea acceder a ellos desde fuera de dicha VLAN, se deberá establecer el gateway con el comando `ip default-gateway` en un switch.

Configure NAT para que los PCs de las VLANs 10 y 20 puedan acceder a Internet.

Tarea 2. Configurar syslog y NTP

Configurar, para los routers y switches, registro de mensajes de log en el servidor C-Serv-Syslog, utilizando sellos de tiempo. Todos los **routers** deberán tener sus relojes sincronizados (actualizando su reloj hardware) con ese mismo servidor de Syslog, mediante una conexión autenticada con la contraseña **ccnas123ntp**.

- Comprobar el correcto funcionamiento de ambas configuraciones forzando la generación de mensajes de log y observando cómo se almacenan en el servidor de Syslog. Tenga en cuenta que la conexión con el servidor de Syslog depende de la tarea 1. Para provocar mensajes de log, puede realizar conexiones fallidas a los routers, puesto que deberían estar configurados para registrarlas.
- En el simulador no funciona, pero en una sesión SSH abierta al router, el comando `terminal monitor` forzaría a que los mensajes de log, además de llegar a la consola del router, se propagasen por dicha sesión SSH y se podrían ver en remoto.

Tarea 3. Reforzar la seguridad de los routers y switches

Los routers y switches tendrá un usuario local con permiso para administrarlos completamente. Siendo **admin** el nombre de usuario y **ccnas123adm** la contraseña para todos ellos.

Además, todos ellos deberán configurarse con la contraseña de *enable* **ccnas123en**, y la contraseña **ccnas123con** para proteger los accesos por consola.

Adicionalmente, se creará un usuario **supervisor** con contraseña **ccnas123sup** que podrá únicamente reiniciar el dispositivo (comando `reload`), además de realizar las tareas del nivel de ejecución sin privilegios.

Para permitir el acceso remoto seguro se deberá habilitar SSH versión 2, y configurar el acceso autenticado por todas las líneas vty de forma que sólo se pueda realizar por medio de SSH.

➲ En pasos posteriores se habilitará AAA y acceso autenticado. De momento se puede, sin embargo, autenticar los accesos remotos utilizando un usuario de la base de datos local.

Se deberán tener en cuenta los errores de conexión, realizando tareas adicionales para evitar accesos no autorizados, y registrando dichos errores (sólo en los dispositivos que se pueda).

Tarea 4. AAA con autenticación frente a RADIUS

Habilite la autenticación en el router contra el servidor RADIUS presente en la sede de la organización. Configure el servidor RADIUS con un acceso “RADIUS” usando una clave de conexión, y cree en dicho servidor el usuario **remoteAdmin** con contraseña **ccnas123remadm**.

Configure los routers para autenticar usuarios contra dicho servidor y, en caso de fallo, utilizar la base de datos local del router.

➲ Comprobar que el router se conecta correctamente con el servidor RADIUS y que los usuarios válidos son aquellos autorizados en dicho servidor. Comprobar también el funcionamiento del mecanismo de autenticación de backup apagando temporalmente el servidor RADIUS.

Tarea 5. Configurar un firewall de filtrado de paquetes en la sucursal B

Configurar ACLs en el router perimetral de la sucursal B para:

- impedir el tráfico de entrada a la red interna de la sucursal B
- permitir sólo a los PCs de la red de la sucursal B (no a su servidor) acceder a Internet para navegar
- permitir todo el tráfico hacia/desde los equipos de la otra sede y de la central

Comprobar que los equipos de la sucursal B siguen teniendo acceso Internet, al servidor de la otra sucursal y a los de la DMZ de la sede central (incluídos los routers).

Tarea 6. Configurar un firewall ZPF en la Sede Central

Configurar un firewall ZPF en el router C-R de la Sede Central para permitir que:

- los PCs de la red interna puedan salir hacia fuera independientemente del protocolo que utilicen, permitiendo el tráfico de regreso
- se pueda acceder desde internet al servidor DNS y HTTP de la DMZ
- se pueda acceder, desde la Red Interna, A y B al servidor RADIUS y SysLog
- los equipos de DMZ puedan obtener actualizaciones externas (HTTP y DNS)
- el resto del tráfico entre zonas no se permitirá

Comprobar que los equipos de la sucursal A (VLANs 10 y 20, que son los únicos que pueden salir por NAT) siguen teniendo acceso Internet, a los servidores de la DMZ de la central.

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