NETWORK ENTERPRISE-C.A

KYNDRYL

KYNDRYL GRANADA/MADRID

ORGANIZADORES DEL PROYECTO

Cristian Carmona Delgado , Adrian Fernandez Martin

Fecha

NETWORK ENTERPRISE-C.A

Índice

NETWORK ENTERPRISE-C.A

1. ¿Quienes somos ?

Somos una empresa la cual se encarga de recibir pedidos de sus clientes , los cuales piden que le monten una infraestructura de redes , para sus empresas .

Nosotros primero le planteamos una topología de red , que mejor se adecue a sus necesidades y a sus condiciones en cuanto a infraestructura física se refiere , una vez montada la idea mediante dibujos de redes , procedemos a configurar el software de los diferentes aparatos de redes (routers , switches , hosts , firewall , etc …)

El software lo configuramos en un entorno de prácticas para asegurarnos que no hay ningún fallo de seguridad. Esto hace que mediante este entorno nos facilite la presentación de dicha topología al cliente , para que valore el producto.

Una vez el cliente está satisfecho con el laboratorio de pruebas ya montado , empezamos a enviar a personal cualificado para montar dicha topología en su empresa lo más rápido posible .

2. Información sobre clientes

Habitualmente nuestros clientes suelen ser empresas de tamaño pequeño o mediano y no necesitan muchos dispositivos , pero sí un mantenimiento constante de sus dispositivos y acuden a nosotros para que ejerzamos esa labor .

Para ver un ejemplo , nos acaba de entrar un cliente , el cual enseñaremos en este manual cómo serán los procedimientos que seguimos con nuestros clientes , para elaborar la topología , preparar el software en un entorno de prácticas , y la puesta en marcha.

En este caso haremos el procedimiento para la empresa de Antonio Bernardo de las Cabreras el es arrendatario de Indra . Nos ha pedido que quiere una red con accesibilidad a internet , con dispositivos de interconexión y dispositivos finales.

3. Dispositivos de interconexión

Para este proyecto el cliente nos pidió soporte y mantenimiento técnico para acceso a internet gracias a nuestro CPD que contienen los firewalls y los routers , la instalación de los dispositivos en su lugar físico de trabajo . Todo esto debido al contrato que firmó con nosotros para que seamos sus proveedores de recursos.

Estos son los siguientes dispositivos de conexión que usamos con los clientes:

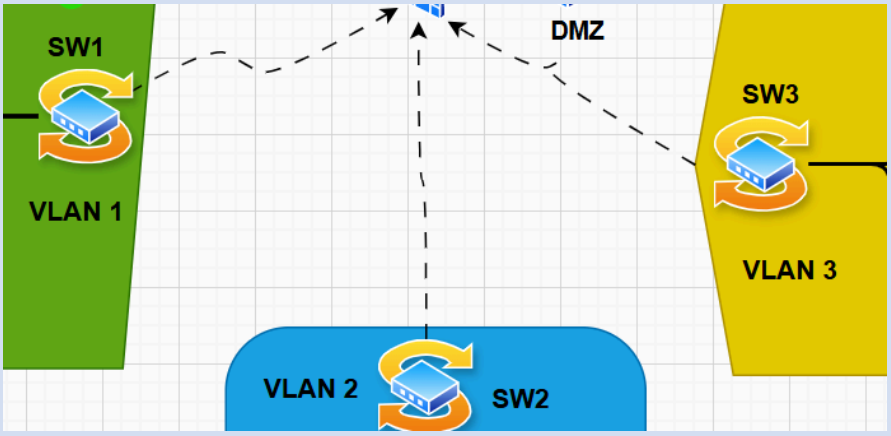
- **FIREWALLS:**El software que controla el tráfico de paquetes de la red entrante como saliente.
- **ROUTERS:**Se encarga de conectar las redes interna y externa , porque es punto de entrada y de salida.
- **SWITCHES:** Son los encargados de conmutar la red interna , y que los dispositivos reciban acceso a internet.
- **DMZ:**Es la que agrega una capa de seguridad a la redes LAN.

3.1 ROUTERS

Los routers en este caso tiene varios protocolos , uno de ellos sería el OSPF (el cual quisimos implementar pero por tema de limitación de configuración no se llevó a cabo) para determinar la mejor ruta para el tráfico de flujo , si el router 1 deja de funcionar el protocolo actuaría en consecuencia y dirigiría el tráfico de flujo por el router 2. Con ello conseguimos tener redundancia , por lo que obtendremos menos tolerancia a fallos

3.2 SWITCHES

Los switches en este caso tienen también tiene protocolos , este sería el VTP el cual si el switch es modo servidor almacenará en su memoria las distintas vlans y las propagara para los demás switches , en cambio si es modo cliente solo recibe la información del switch modo servidor.



- **SW1:**Es el switch servidor , el cual están creadas las vlans y las propagara para los demás switches , la interfaz que está conectada al firewall está configurada de modo troncal para ello y para los hosts está configurada modo acceso
- **SW2:**Es un switch modo cliente , el cual recibió la información sobre las vlans de el switch modo servidor , la interfaz que está conectada al firewall está configurada

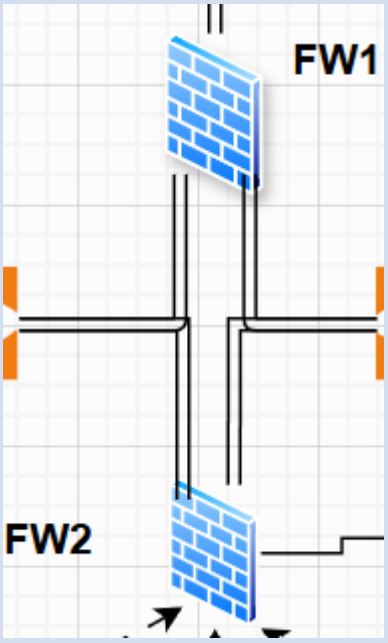
de modo troncal para ello y para los hosts está configurada modo acceso

- **SW3:**Es un switch modo cliente , el cual recibió la información sobre las vlans de el switch modo servidor , la interfaz que está conectada al firewall está configurada de modo troncal para ello y para los hosts está configurada modo acceso

(Para qué hosts obtengan las vlans correspondientes de los switches conectados a ellos debería funcionar " switchport mode access" en la interfaz que va conectado a ellos , esto es a causa de las limitaciones de la virtualización)

3.3 Firewall

El siguiente apartado es el tema de la seguridad de nuestro cliente la cual tiene que ser lo más segura posible porque aunque la informática avance todo técnico en Redes sabe que las redes nunca van a ser seguras al 100% . En nuestro laboratorio las reglas no se aplican por el tema de la virtualización pero esta seria las reglas que hubiésemos aplicado:



Para que nuestro cliente tenga el menor porcentaje de ciberataques le hemos implementado 2 firewall :

- FW1: En este hemos implementado varias reglas :
    1. Hemos bloqueado el puerto 25 con el protocolo SMTP para evitar que nuestro cliente le entre spam malicioso
    2. Hemos abierto el el puerto 22 para hacer conexiones SSH para poder hacer el mantenimiento en remoto (obviamente con su usuario y contraseña para que solo el personal cualificado acceda a él)
    3. Hemos habilitado el puerto 20 para usar el servicio FTP ya que para hacer las copias de seguridad se harán en el CPD el cual está en nuestras oficinas y en otro CPD de Berlín y las copias se guardan en ambos servidores FTP .
    4. Hemos habilitado el puerto 443 para que todo el mundo pueda ver la página web de nuestro servidor apache con el protocolo seguro HTTPS

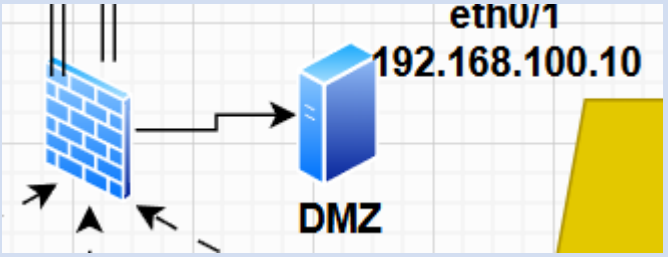
5. Hemos bloqueado el puerto 3306 para que nadie pueda acceder desde fuera de la red a nuestros servidores de base de datos MySQL
6. Hemos habilitado los puertos 993 (IMAPS) y 995 (POP3S) para la entrada y salida de correos mediante los protocolos seguros

- FW2: En este hemos implementado varias reglas:
  1. Hemos bloqueado el puerto 25 con el protocolo SMTP otra vez para evitar que nuestro cliente le entre spam malicioso por si el FW1 fallará
  2. Hemos abierto el el puerto 22 para hacer conexiones SSH para poder hacer el mantenimiento en remoto (obviamente con su usuario y contraseña para que solo el personal cualificado acceda a él)
  3. Hemos habilitado el puerto 20 para usar el servicio FTP ya que para hacer las copias de seguridad se harán en el CPD el cual está en nuestras oficinas y en otro CPD de Berlín y las copias se guardan en ambos servidores FTP .
  4. Limitar tráfico de protocolos que no se usan en la red
  5. Hemos habilitado el puerto 443 para que todo el mundo pueda ver la página web de nuestro servidor apache con el protocolo seguro HTTPS
  6. Hemos habilitado los puertos 993 (IMAPS) y 995 (POP3S) para la entrada y salida de correos mediante los protocolos seguros.
  7. Hemos habilitado el puerto 3306 para que puedan acceder desde dentro de la red a nuestros servidores de base de datos MySQL solo aquellas personas que tengan acceso

3.4 DMZ

En esta área de nuestra empresa añadimos una capa mayor de seguridad a la red local de la empresa , con ello permitimos que los usuarios accedan al servidor de red interna mediante redes externas por parte de los usuarios .

Cuando los firewall ya están funcionando correctamente la DMZ ya tendría el uso que le queríamos darle.
Así sería en nuestro esquema :



4. Dispositivos finales

En esta propuesta para la empresa de Antonio hemos colocado los siguientes dispositivos finales para su empresa según sus necesidades :

- Servidor Web: Este servidor será el que albergue la página web de nuestro cliente.
- Impresora: Este dispositivo será el encargado de imprimir todos los archivos necesarios que los clientes de la red necesiten.

- Granja de Servidores: En este lugar será donde la empresa guarde la información de copias de seguridad , bases de datos , tendrán los protocolos DHCP , FTP , POP3S , IMAPS ,DNS.
- Hosts: Serán el lugar de trabajo de los empleados de la empresa de Antonio

5. Roles y responsabilidades

Roles de cada uno:

- **Administrador de Servidores y Sistemas :** En este sector se encargaría de supervisar los sistemas que no tengan ningún fallo , tengan alguna caída o se produzca alguna incidencia. Responsable: Adrian.
- **Administración de los dispositivos de seguridad:** En este sector sería para el mantenimiento del servicio de los firewall y de la DMZ. Responsable : Cristian
- **Responsable de la red:** En este sector es el más importante porque sería el que mantiene y monitorea las redes locales y sería el encargado de supervisar el soporte que ofrecemos en pleno funcionamiento tanto para los clientes como para nuestra empresa, eso implica la zona de nuestro CPD , controlando los dispositivos de interconexión , el tráfico de red (segmentos). Responsable: Adrián
- **Ciberseguridad (Supervisión/Monitorización):**En este sector sería el encargado de ir actualizando los diferentes dispositivos de interconexión debido a que diariamente se producen nuevas brechas de seguridad debido a los nuevos métodos del

malware y este sería el encargado de aplicar nuevos parches para dichas brechas. Responsable: Cristian

6. Anexos

ANEXO I TOPOLOGÍA EN DRAW

(ANEXO en Archivo aparte)

ANEXO II TOPOLOGÍA EN YAML Y CONFIGURACIONES

(ANEXO en Archivo aparte)