INFORME TÉCNICO

SEPRELAD - SECRETARIA DE PREVENCIÓN DE LAVADO DE DINERO

Ticket 334023

5/05/2022

Cecilio Da Silva 1001 esq. Federación Rusa
Tel. /Fax.: 616-4000
Asunción - Paraguay

Francisco Sosa
Francisco Sosa
Técnico de Networking

REPORTE DEL CASO

Breve descripción del caso:

La entidad Secretaría de Prevención de Lavado de Dinero – SEPRELAD solicitó soporte para la realización de configuraciones de red, en específico la generación de troncales VLAN para la separación de los servicios de entidad en diferentes dominios de broadcast.

El pedido incluye la configuración de VLANs para aprovisionar los APs de la entidad por medio de un controlador WIFI de marca TRENDnet, se busca, además, que la red WIFI sea aislada a la LAN, para ello es necesario realizar las configuraciones respectivas en los equipos de red. Actualmente, un equipo Fortigate 240D que cumple la función de switch central, por el modo en el que se encuentra configurado el mencionado equipo no es realizar la configuración de las troncales sin generar afectación a toda la infraestructura de red interna. Por tanto, para poder avanzar con las configuraciones son necesarios los siguientes puntos.

- Acceso y privilegios a todos los equipos de red de la entidad (Cisco, Juniper, Fortinet, TRENDnet, etc.) para realizar las configuraciones de VLANs/redes. No se tiene acceso a un switch Cisco Catalyst ubicado en la última posición del rack ubicado en la oficina de Informática y de los switches TRENDnet ubicados en el rack de la oficina del frente de la entidad. Sin el acceso y gestión de estos equipos, no se podrá asegurar el funcionamiento de los servicios luego del cambio de configuraciones.
- Identificar los puertos físicos en los equipos de red en los cuales es necesario configurar una VLAN/red especifica, ya sea los puertos en los que van conectados los APs WIFI o los que van a las tomas de red de los usuarios, de lo contrario al realizar los cambios, los usuarios quedarían sin servicio.
- Validar a qué servicio corresponden cada uno de los enlaces conectados en el Fortigate 240D, y los requerimientos de VLAN/red de estos.

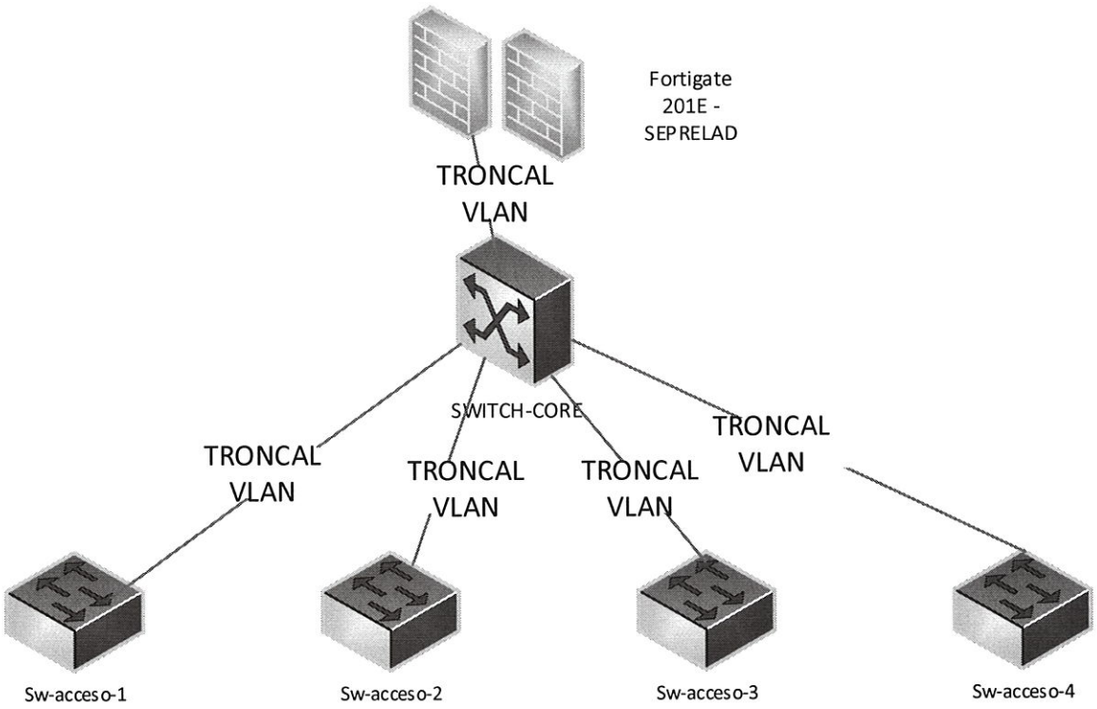
Con respecto a como continuar con las configuraciones se ofrecen dos alternativas:

- Cambiar el modo de funcionamiento de los puertos del Fortigate 240D. Esto traerá afectación a los puertos conectados a dicho equipo, motivo por el cual es importante identificar todos los puertos conectados al mismo para realizar la mejor planificación posible.
- Utilizar otro equipo, especializado en switching para el efecto. Se observa que la entidad posee un Juniper EX-4200T que podría utilizarse como switch central, para ello se requiere validar las conexiones del Fortigate 240D ya que las mismas deben son las que pasaran a conectarse al Juniper, por tanto, es importante confirmar que el cableado físico hasta el mismo no sea un inconveniente. Se hace notar que el equipo Juniper EX4200T ya es un equipo que el fabricante lo cataloga como EOL (end-of-life) (referencia: https://supportportal.juniper.net/s/article/End-of-Life-Announcement-EX2200-EX3300-EX4200-EX4500-and-EX4550-Related-Products). Una

Francisco Sosa
Francisco Sosa
Técnico de Networking

recomendación podría ser la de renovación de hardware en lo que respecta al switch core de la entidad.

El esquema que se busca alcanzar es el siguiente:



Conclusiones:

La topología que observa más arriba constituye la forma ideal de operación de una infraestructura interna de red, ofreciendo mayor seguridad al separar los segmentos de red, obligando que el trafico entre redes distintas sea filtrado por el firewall.

Francisco Sosa
Técnico de Networking
TEISA

Ing. Francisco Sosa
TEISA