TALLER SEGURIDAD DE REDES DE DATOS

Usted ha sido recomendado para realizar una actualización en la red de una empresa que tiene sedes a nivel Nacional, la actualización se enfocará en 2 objetivos principales, el primero es asegurar todos los puntos en los que encuentre falencias de Seguridad, y el segundo asegurar la alta disponibilidad de la red, implementando algunas mejoras que ayuden a tener un desempeño óptimo de la red.

Dentro de los requisitos principales solicitados esta que el tráfico confiable entre las 2 sedes se envíe por medio de una VPN segura, y que todos los equipos puedan tener acceso a Internet a pesar que en cada sede solo cuenta con una IP Pública, además se deben realizar mejoras en la configuración de los dispositivos activos buscando optimizar el desempeño de la red y así no solo asegurar los datos, sino también su disponibilidad.

Después de realizar un relevamiento de Sitio se han descubierto varias falencias en la topología que no solo afectan la seguridad de los datos, sino que también no sacan el mayor desempeño a algunas características de los dispositivos que tiene la compañía, y que con una buena configuración podría asegurar una mayor disponibilidad de la red como tal.

La planificación tomada después del análisis de la compañía, sugiere iniciar a aplicar las mejoras inicialmente en el entorno LAN, y una vez finalizadas se enfoque el trabajo en los enlaces WAN. Por ende se iniciará a realizar los cambios en mejora de la red en los Switchs de la compañía y finalmente se trabajará en los Routers. Para las siguientes mejoras se trabajará en la topología que se ha venido manejando durante todo este proceso, con 2 sedes, Cali y Bogotá.

CAMBIOS GENERALES A REALIZAR EN LOS DISPOSITIVOS:

1. CONFIGURACIÓN RED PRINCIPAL CALI:

Dispositivo	Hostname	Mejoras Generales
Router	R-Cali	VPN, NAT, ACL, HSRP, DHCP…
Switch	Sw-Cali	SSH, RSTP, Portfast, VTP, Etherchannel Snooping DHCP
Switch	Sw2-Cali	SSH, RSTP, Portfast, VTP, Etherchannel Snooping DHCP

1.1 SWITCHS CALI:

- ✓ Configure en los Sw de Cali, SSH, encriptación de contraseñas y seguridad de puertos a los puertos donde haya un Servidor, aplique la seguridad de puerto de forma manual, y modo de violación en restricción. Además verifique si tiene configurado correctamente los puertos troncales y de modo acceso, al igual que la asignación correcta de los puertos a sus respectivas VLAN.

- ✓ Dentro de las configuraciones observamos que en los 2 Switchs se maneja STP, pero no se le está sacando el mejor desempeño a este, por lo tanto **se solicita que ambos Switchs** se configuren para trabajar con **RSTP**, se le habilite la característica de **Portfast** de manera predeterminada globalmente, y se defina a **Sw-Cali como Switch primario** para las VLAN 1**, 10, 20 y 30**, y el **Sw2-Cali se defina como secundario**.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

- ✓ Configure la **versión 2 de VTP**, configure a **Sw-Cali como VTP server y Sw2-Cali como VTP cliente**, el dominio VTP a manejar será **cali.grd.com** y la contraseña de autenticación **clavevtp**.

- ✓ Se desea aprovechar al máximo los 2 enlaces que hay entre los 2 Switchs, pero al no tener agregación de enlaces, el protocolo STP está bloqueando uno de los 2 enlaces. De acuerdo a lo anterior se le solicita configurar con el **Protocolo de Negociación estándar en el enlace Etherchannel en ambos Switchs,** aunque de acuerdo al modo se puede asumir cual será, en la configuración deberá empezar seleccionando **el protocolo solicitado, configure el grupo 10 para los puertos Fa0/2 al Fa0/5, Sw-Cali será el que debe esperar** el establecimiento del enlace y **Sw2-Cali el que la iniciará, recuerde que todos los puertos físicos deben estar en troncal, deben tener la misma nativa y las mismas permitidas.**

- ✓ Configure todos los puertos troncales **Fa0/1 y Po10** para que la **VLAN nativa sea la 10**, y que **solo permita el tráfico de las VLAN 1, 10, 20 y 30**. Finalmente **guarde la configuración** en ambos Switchs y compruebe con los **comandos de visualización y pruebas de conectividad** que toda la LAN Cali quedó funcionando correctamente, si requiere reiniciar algún Switch, realícelo de ser necesario. Utilice los comandos Show.

- ✓ Se ha detectado que constantemente un Servidor DHCP no autorizado ha venido trabajando en la LAN de Cali, al igual que en Bogotá, para evitar que esto continúe causando caídas en la red por asignación de direcciones erradas, y con el fin de asegurar la mayor disponibilidad de la red, se ha solicitado que se **habilite el rastreo (Snooping) de DHCP**, una vez habilitado, configure que este **obligatorio solo para la VLAN 1**, y configure todos los puertos troncales como puertos **DHCP confiables que considere como tal,** Realice esta operación no solo en los Sw de Cali, sino también en el de Bogotá.

2. CONFIGURACIÓN ROUTERS R-CALI Y R-BOG

- ✓ El Router de Cali al igual que los Switchs de Cali se le debe configurar SSH, revise antes de continuar que las Subinterfaces, y demás configuraciones se encuentren bien de acuerdo a la tabla de direccionamiento que se diseñó al inicio. Para brindar mayor seguridad configure en ambos Router NTP y Syslog, y la habilitación de algunos servicios del Router para llevar registro de la hora de generación de los log.

- ✓ Inicie habilitando 2 Servicios fundamentales para la Seguridad y funcionamiento correcto de Syslog, estos **servicios son la encriptación de contraseñas** (este deberá realizarlo también en Bogotá) y el **servicio de marca de tiempo para los log.**

- ✓ Ahora configure los Servidores que se encuentra en la topología como Servidores NTP y Syslog.. Una vez definido el **Servidor NTP y Syslog**, habilite en NTP **la actualización del calendario**, y en Syslog la **captura de cualquier tipo de registro** (informativo), al igual que los **registros de información de usuarios**. Verifique en los servidores que se almacenaron los eventos de syslog.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

- ✓ Teniendo en cuenta que el Router de Cali empezará a manejar los Pool DHCP de toda la compañía de forma Centralizada se le ha solicitado **configurar en R-Bog el reenvío de peticiones DHCP** de todas las subinterfaces, a R-Cali, de las IP que maneja el R-Cali utilice la IP correspondiente a la subinterfaz de la VLAN Administrativa de Cali**.**

- ✓ Dentro de las proyecciones de la compañía y con el fin que asegurar una alta disponibilidad, está planificado la compra de un 2º Router en Cali, con el fin de tenerlo como equipo de respaldo, y poder utilizar de ahí en adelante una IP virtual como Gateway de cada una de las 3 VLAN principales. Es por lo anterior que **se les solicita configurar en cada subinterfaz de R-Cali la característica de HSRP**, esto con el fin que en un futuro al agregar el 2º Router, este ya quede listo para actuar como el Router principal.

- ✓ Para la configuración de HSRP tenga muy en cuenta las siguientes indicaciones. **Primero**: el **grupo HSRP tendrá el mismo número de la subinterfaz** que se esté configurando (10,20 o 30), y deberá tener como IP virtual una IP que pertenezca a la VLAN (3ra válida de cada subred de acuerdo a su tabla de direccionamiento). Segundo: Para cada subinterfaz, y en su grupo HSRP se deberá configurar la mayor prioridad posible y finalmente configurar igualmente el adelantamiento (preempt). Verifique con los comandos show.

- ✓ Configure una **ruta por defecto con interfaz de salida** que envíe a la ISP todo el tráfico con destino desconocido en su tabla de enrutamiento. Una vez finalice esto inicie con la configuración de la **VPN y NAT**. Pare este proceso se deberá iniciar con la creación de **2 ACL nombradas extendidas. (Ambos Router)**

- ✓ Cree una ACL llamada **ACL-VPN**, en la cual defina el tráfico interesante para activar la **VPN,** la ACL deberá tener solo 2 sentencias, en la primera definirá el trafico interesante (sumarizar de ser necesario), y en la segunda sentencia reconfirmará la denegación implícita. **(Ambos Router)**

- ✓ Luego cree una ACL llamada **ACL-NAT**, en la cual inicialmente se excluirá el tráfico que irá por la VPN, y finalmente se definirá el tráfico interesante para activar **NAT,** la ACL deberá tener solo 3 sentencias, en la primera definirá el tráfico a excluir y que irá por VPN, en la segunda el tráfico interesante (de las redes locales a cualquier otra red - sumarizar de ser necesario), y en la tercera sentencia reconfirmará la denegación implícita. **(Ambos Router)**

- ✓ Ahora inicie con la configuración de la VPN, configure la **política 10** con una autenticación PSK, y las **mejores características tanto en confiabilidad como en integridad**, y **grupo 2** de DH. La contraseña pre-compartida a utilizar será **clavevpn.** En la configuración de IPsec se manejará confiabilidad e integridad también con las mejores características, esta configuración configúrela con el nombre **IPSEC-VPN. (Ambos Router)**

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

- ✓ En el mapa criptográfico que deberá llamar **MAP-VPN** de la secuencia 10, recuerde incluir todos los valores necesarios para el funcionamiento satisfactorio de la VPN, finalmente asígnela a la interfaz adecuada y espere realizar la configuración al otro extremo para comprobar su correcto funcionamiento. Utilice los comandos de visualización necesarios una vez estén configurados ambos extremos. **(Ambos Router)**

- ✓ Configure correctamente los parámetros finales para un funcionamiento correcto de **NAT**, realice la traducción de direcciones internas hacia la interfaz que da salida a Internet, y realice el procedimiento con **sobrecarga** para que puedan salir todos los equipos de las LAN. Recuerde definir el modo NAT de cada una de las subinterfaces. **(Ambos Router)**

- ✓ Finalmente configure una ACL estándar llamada **ACL-VTY** la cual permita el acceso remoto a los Routers solo desde los equipos Servidores, dentro de las sentencias defina primero el servidor de Cali y luego el de Bogotá, utilice en las 2 sentencias la palabra clave host. Al finalizar reconfirme la denegación implícita. Asígnela correctamente y compruebe que quedó debidamente aplicada. **(Ambos Router).** Utilice los comandos show.

3. CONFIGURACIÓN RED SUCURSAL BOGOTÁ

Dispositivo	Hostname	Mejoras Generales
Router	R-Bog	VPN, NAT, ACL, AAA, DHCP Relay
Switch	Sw-Bog	SSH, DHCP snooping, Portsecurity, BPDUguard
WRT300N	AP	WPA2-EAP, Disable SSID Broadcast

3.1 AP Y PC INÁLAMBRICO:

- ✓ Se encuentra en el AP y en la red inalámbrica en general una brecha enorme de inseguridad, ya que manejan esta red con autenticación Abierta, se solicita configurar autenticación **EAP** con cifrado **WPA2**, se debe tener en cuenta la IP del Servidor Radius, configure correctamente con la clave secreta **clavewifi**.

- ✓ Una vez configurado el AP, ingrese al PC Inalámbrico y conéctelo a la red inalámbrica con el usuario **sena**, y la contraseña **claveradius,** espere un tiempo prudente para que se realice la conexión, puede ir adelantando otro punto mientras esto ocurre. Tenga en cuenta que este mismo usuario se utilizara más adelante para la autenticación desde el Router de Bogotá. Una vez conectado el PC a la red inalámbrica, vaya al Linksys y **deshabilite la difusión del SSID**.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP

3.2 SW-BOG:

- ✓ Un inconveniente que se ve muy común en la red es que se conectan Switchs adicionales sin la autorización del Administrador de la Red, generando tráfico no autorizado adicional, por medio de un sniffer (husmeador de red) se logró detectar que en la oficina a donde llegan los puertos **Fa0/6 hasta el Fa0/12** es que se viene presentando la problemática de conexión de **Switchs no Autorizados**, se solicita que en esto puertos se **habilite la vigilancia de BPDU**.

- ✓ Finalmente en el Sw-Bog **configure seguridad en el último puerto FastEthernet**, que es en el cual se conecta el Servidor Radius, se solicita habilitar la seguridad de puertos, y permitir **máximo 3 MAC** por ese puerto, esto teniendo en cuenta que si hay una posible falla, al realizar un cambio rápido de Servidor un 2º o 3ro no se vea bloqueado. También se solicita que todo el aprendizaje que se realice de las **MAC confiables se realice de forma automatizada**, y que en el caso de haber una **violación del puerto este inmediatamente se apague**. Compruebe captura de MAC generando tráfico por ping al server de cali.

3.3 ROUTER BOGOTÁ

- ✓ Se regresa de nuevo al Router Bogotá a realizar algunas configuraciones finales, en este momento ya debe estar funcional la VPN y el NAT, al igual que la ACL para el filtrar el ingreso de forma remota al Router por línea VTY.

- ✓ En esta oportunidad se solicita que se Filtre el tráfico de la Red WiFi, ya que es una red que es una de las redes que debe estar más restringida. Para esto se solicita lo siguiente: Crear una ACL nombrada **BLOCK-WIFI,** la cual en su primera sentencia bloquee todo el tráfico PING originado **desde la Red inalámbrica hacia el Servidor de Cali** (Sea muy puntual, use en todas las sentencias la palabra clave host), también bloquee el tráfico FTP (en esta sentencia utilice un rango de puertos). También se solicita que bloquee el tráfico TFTP , pero permita el trafico HTTP, HTTPs, DNS y DHCP **desde la Red inalámbrica hacia el Servidor de Cali** (realizarlo en el orden que se solicita y de forma específica).

- ✓ Antes de aplicar la ACL compruebe que el equipo tiene acceso a cualquier tipo de tráfico, finalmente aplique correctamente la ACL en el lugar más recomendado, verifique que el filtrado funciona adecuadamente.

- ✓ Finalmente en el Router de Bogotá, y con el fin de aprovechar el Servidor Radius de esta Ciudad se recomendo que el Router de Bogotá realizara su autenticación por medio de AAA, para esto habilite AAA y configure correctamente tanto la IP del Servidor Radius como la clave secreta aaakey, cree la configuración de autenticación llamada **SEGURIDAD** en donde como primera alternativa se busque al Servidor Radius y como segunda la base de datos de usuarios local del router, finalmente asocie el nuevo tipo de autenticación a las lineas tanto de Consola como VTY del Router. Pruebe conectividad con el Servidor y salga de todos los modos para comprobar de nuevo el tipo de autenticación de usuarios.

CONCLUSIONES: Una vez finalizado ya estará en la capacidad de implementar una seguridad importante a los dispositivos de la red, compruebe mediante los comandos **show y ping** el correcto funcionamiento de toda la topología. Ingrese a los Servidores de las ciudades y al de internet.

Diseñado por: Gustavo Rodríguez Salinas
Instructor Regional Valle
CCNA, CCAI, CCNP