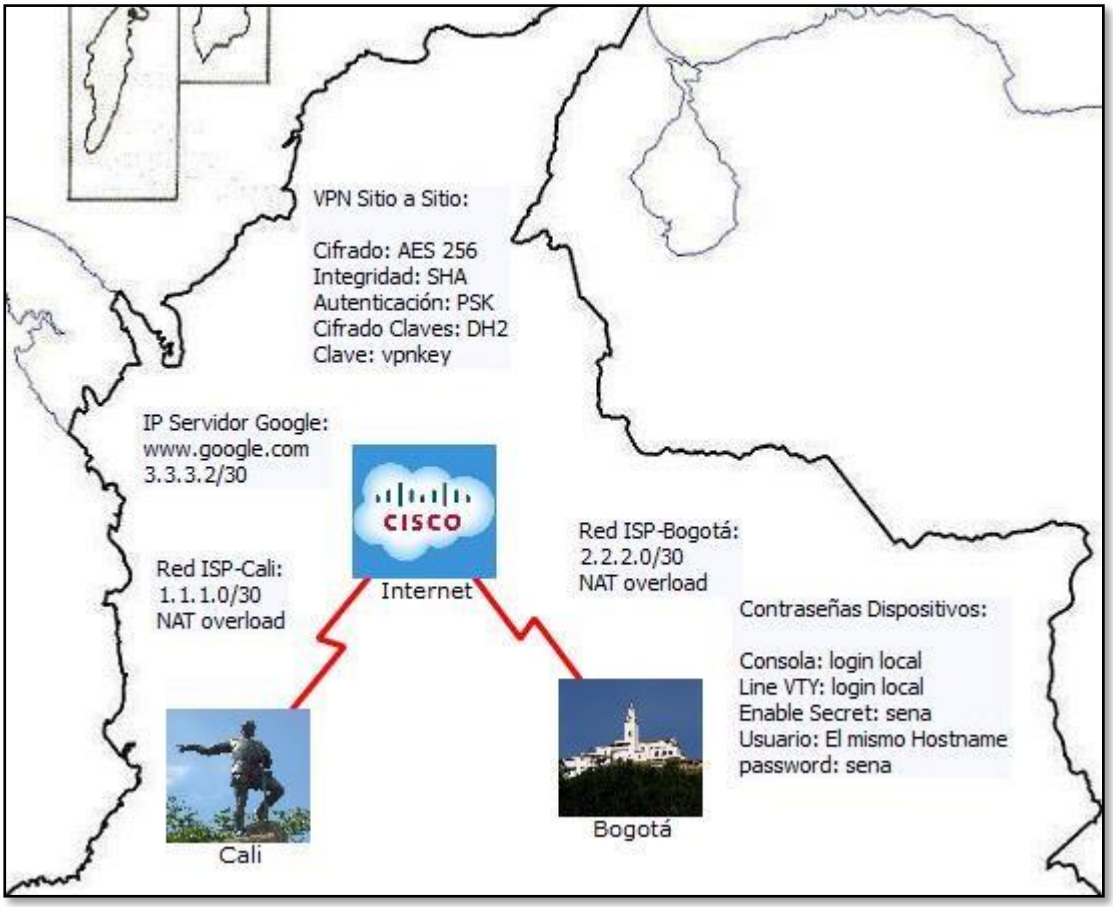
EXAMEN FINAL SEGURIDAD DE REDES WAN

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.



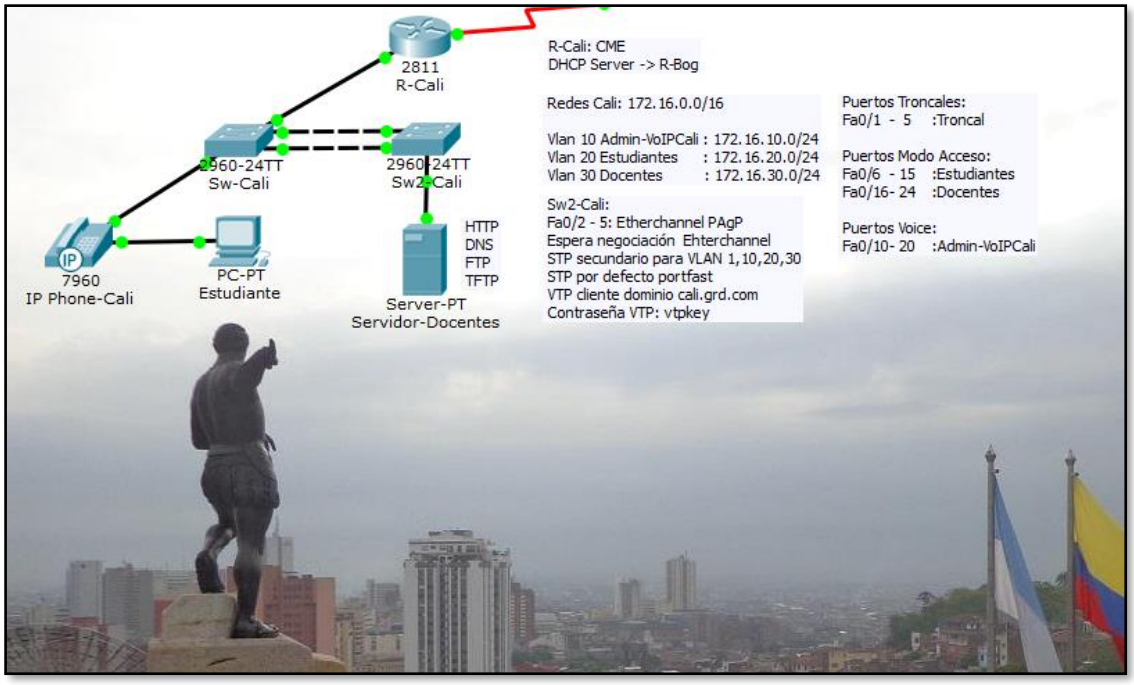
En la imagen anterior se muestra de forma general de cómo están distribuidas las Redes a nivel Nacional, se encuentra información general de contraseñas de equipos, información de VPN y NAT, y el direccionamiento público en Internet. La ISP tiene las primeras IP válidas de cada subred en sus interfaces. Tenga en cuenta que usted no tiene ningún permiso para ingresar a la ISP a realizar cambios, está se encuentra funcionando correctamente y no necesita que realice cambios de configuración en esta parte de la topología.

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

La planificación tomada después del análisis de la compañía, sugiere iniciar a aplicar las mejoras inmediatamente en la WAN. Por ende, se iniciará a realizar los cambios en mejora de la red en los en los Routers directamente.

CAMBIOS GENERALES A REALIZAR EN LOS DISPOSITIVOS:

1. CONFIGURACIÓN COMPARTIDA EN R-CALI Y R-BOG (30 A 45 MINUTOS)



- ✓ 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 **TRAFICO-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 **TRAFICO-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)**

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

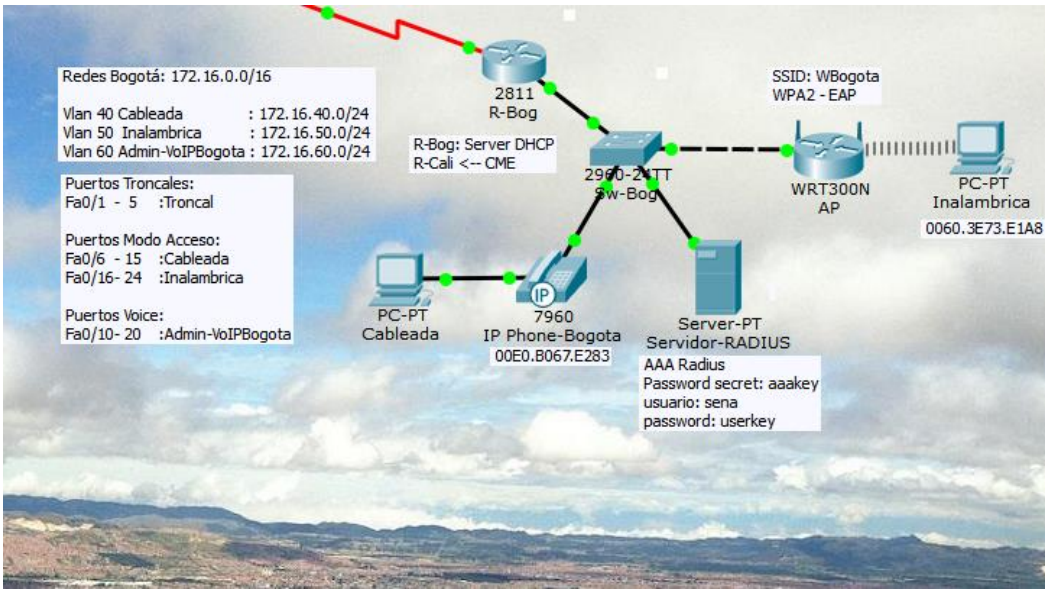
- ✓ Ahora inicie con la configuración de la VPN, configure la **política 1** con una autenticación PSK, y las **mejores características tanto en confidencialidad como en integridad**, y **grupo 2** de DH. La contraseña pre-compartida a utilizar será **vpnkey.** En la configuración de IPsec se manejará confidencialidad e integridad también con las mejores características, esta configuración configúrela con el nombre **VPN-SITIO-A-SITIO. (Ambos Router)**

- ✓ En el mapa criptográfico que deberá llamar **MAPA-VPN** de la secuencia 1, 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 **ACCESO-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 (**172.16.30.254**) y luego el de Bogotá (**172.16.50.254**), 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)**

2. CONFIGURACIÓN RED SUCURSAL BOGOTÁ



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

ROUTER BOGOTÁ (15 A 30 MINUTOS)

- ✓ 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.

- ✓ 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 **FILTRO_WIFI,** la cual en su primera sentencia bloquee todo el tráfico FTP originado **desde la Red inalámbrica (172.16.50.0/24) hacia el Servidor de Cali** (Sea muy puntual, use en todas las sentencias la palabra clave host, y en esta primera sentencia utilice un rango de puertos). También se solicita que bloquee el tráfico TFTP y el Ping en este caso también **desde la Red inalámbrica hacia el Servidor de Cali** (realizarlo en el orden que se solicita).

- ✓ Se requiere que también se permita desde la Red inalámbrica hacia ese mismo servidor y hacia cualquier destino, todo el tráfico HTTP, HTTPs, DNS, RTP, SCCP, por lo que se recomienda que para simplificar se permita en una última sentencia todo **el tráfico desde cualquier origen a cualquier destino.** Todo lo solicitado anteriormente deberá quedar en la ACL nombrada **FILTRO_WIFI** y esta solo deberá tener 4 sentencias. 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.

Una vez finalizado todo compruebe mediante los comandos **show y ping** el correcto funcionamiento de todo, ingrese desde el PC inalámbrico y el PC de Cali a www.cali.grd.com y www.google.com, y realice llamadas del Teléfono IP de Cali a Bogotá. **Tiempo Total:** 45 minutos, **Máximo:** 1Hora 15 minutos.

Cualquier duda consúltela con el instructor a cargo de la prueba.

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