Contenido

Asignacion de Responsabilidades Por roles

Gerente de infraestructura (Ramiro Valeriano Gonzalez Rodriguez)

Responsabilidades

1. Crear el plan de direccionamiento IPv4 para todas las sedes, considerando crecimiento futuro.
2. Crear un cuadro descriptivo asociado a las direcciones IPv4 estáticas Y/O dinámicas para servidores, equipos de red, dispositivos intermediarios y equipos finales.
3. Verificar que cada configuración entregada por los ingenieros esté funcionando correctamente, actuando como filtro final antes de la implementación en producción.
4. Elaborar una cotización basada en tres proveedores distintos, evaluando compatibilidad, costos y rendimiento.
5. Trabajar juntamente con el equipo de seguridad para validar las medidas implementadas y configurar accesos SSH a usuarios seguros desde todas las sedes.
6. Se utilizará su Dispositivo final para la demostración final del producto Revisar y aprobar todas las configuraciones realizadas por los ingenieros antes de su implementación.
7. Garantizar que cada dispositivo (routers, switches, servidores) funcione correctamente antes de pasar a producción.
8. Actuar como **filtro técnico final** para asegurar estabilidad, seguridad y cumplimiento del diseño.
9. Creacion de documentación Final y validar la documentación del proyecto y también los contratos

Documentacion a entregar

1. Planificación y direccionamiento

1.1 Plan de direccionamiento IPv4 completo para todas las sedes.
1.2 Subredes detalladas por sede y por VLAN.
1.3 Rango de crecimiento reservado para expansión.
1.4 Tabla de gateways, máscaras

---

2. Validación técnica de configuraciones

2.1 Informe de revisión de configuraciones entregadas por los ingenieros.
2.2 Lista de ajustes realizados antes de la aprobación.
2.3 Evidencias de funcionamiento correcto antes de pasar a producción.
2.4 Acta de aprobación o rechazo de configuraciones por hito.

---

3. Cotización de equipos y servicios

3.1 Cotización comparativa de tres proveedores distintos.
3.2 Lista detallada de equipos requeridos (routers, switches, servidores).

---

4. Validación de seguridad y accesos remotos (SSH)

5.1 Documentación de accesos SSH configurados en los dispositivos.
5.2 Tabla de usuarios autorizados por sede.
5.3 Verificación de acceso seguro desde todas las sedes.

Ingenieros de Redes Senior (Gerson Javier Perez)

Responsabilidades

1. Dirección IP y configuración de infraestructura

1.2 Configurar IPs en interfaces (routers y/o switches) para todas las sedes: Santo Domingo, Santiago y Romana.
1.3 Agregar descripciones en todas las interfaces para documentar la topología.
1.4 Configurar default-gateway en switches capa 2.
1.5 Configurar DHCP para las sedes Romana y Santo Domingo (R-SW1, R-SW2, R-SW6,).
1.6 Configurar intervlan routing y HSRP como mecanismo de redundancia en R-SW1 y R-SW2.
1.7 Configurar EtherChannel (LACP/PAgP) entre switches de la sede central.

2. Configuración básica estandarizada

2.1 Configurar hostnames descriptivos y domain-name.
2.2 Configurar contraseñas seguras, enable secret y encriptación (service password-encryption).
2.3 Configurar banners de seguridad (MOTD, EXEC).
2.4 Asegurar el acceso por consola con autenticación.
2.5 Asegurar acceso remoto (VTY) obligatorio y deshabilitar Telnet.
2.6 Guardar y respaldar configuraciones (startup-config) en cada hito del proyecto.

3. Implementación de protocolos y servicios de red

3.1 Configurar y optimizar OSPF área única para toda la red corporativa.
externos).
3.3 Configurar VLANs y trunking entre switches.

4. Documentacion a entregar

1 Capturas o exportación de configuraciones fundamentales: hostname, domain-name, SSH, contraseñas, banners y seguridad básica.
2 Configuración documentada de DHCP para sedes Romana y Santo Domingo (pools, gateways, DNS, exclusiones, reservas si aplican).
3 Resumen técnico del intervlan routing implementado, mostrando SVI, gateways y funcionamiento de HSRP con prioridad y estado.
4 Documentación de la creación y asignación de VLANs, incluyendo tagging, trunking y nativas configuradas.
5 Configuración detallada de EtherChannel: modo (LACP/PAgP), interfaces agregadas y verificación del canal.

6 Reporte estructurado de la configuración de OSPF: router-id, áreas, networks, vecinos y verificación de adyacencias.
7 Evidencia de pruebas de conectividad: ping entre VLANs, traceroute entre sedes, estado de HSRP y funcionamiento del fallback.
8 Respaldo de configuraciones finales (startup-config) de todos los dispositivos trabajados.

Ingenieros De seguridad (Angel Luis Adon Santana, leonardo Paulino Tavarez)

Responsabilidades

4.1 Implementar Port-Security en switches de acceso (violation mode, sticky MAC).
4.2 Implementar protección contra ataques de VLAN hopping (DTP, Native VLAN, pruning).
4.3 Configurar protección contra ataques DHCP (DHCP Snooping).
4.4 Configurar protección ARP (DAI – Dynamic ARP Inspection).
4.5 Configurar protección STP (BPDU Guard, Root Guard).
4.6 Configurar ACLs de filtrado según criterios del proyecto.

Documentacion a entregar

1. Informe completo de Port-Security implementado en cada switch de acceso, indicando:

1.1 Puertos protegidos
1.2 Máximo de direcciones MAC
1.3Modo de violación configurado (restrict/shutdown)
1.4MACs aprendidas por sticky
1.5 Capturas de verificación (*show port-security*, *show port-security interface x/y*).

2 Documentación de las medidas aplicadas para prevenir VLAN hopping, incluyendo:
2.1 Deshabilitación de DTP en puertos de acceso
2.2 Configuración correcta de la Native VLAN
2.3VLAN pruning aplicado en enlaces troncales
2.4 Evidencias de configuración (*show interface trunk*, *show vlan brief*).

3 Reporte detallado de la implementación de DHCP Snooping:

3.1 VLANs protegidas por Snooping
3.2 Puertos confiables (uplinks)

3.3Ubicación de la base de bindings

3.4 Capturas de validación (*show ip dhcp snooping*, *show ip dhcp snooping binding*).

4. Documentación de Dynamic ARP Inspection (DAI), indicando:

4.1 VLANs bajo inspección

4.2Relación con los registros del DHCP Snooping binding

4.2 Puertos con rate-limit o inspección activa

4.3Capturas de comandos de verificación (*show ip arp inspection*).

5.Evidencia de la protección STP implementada:

5.1 Puertos con BPDU Guard

5.2Puertos con Root Guard

5.3Verificación del árbol STP y del root bridge en cada VLAN

5.4Capturas de validación (*show spanning-tree summary*, *show spanning-tree interface x/y detail*).

6.Documentación completa de todas las ACL configuradas, incluyendo:

6.1 Nombre o número de la ACL

6.2 propósito de cada lista de control

6.3 tráfico permitido y denegado

6.4 Interfaces donde se aplicó y en qué dirección (in/out)

- Capturas de verificación (*show access-lists*, *show run interface x/y*).

Reporte de pruebas de seguridad realizadas después de las configuraciones, como:

- Intento de conectar un dispositivo no autorizado a un puerto de acceso (validación de port-security)
- Verificación de que un servidor DHCP no autorizado no pueda funcionar (DHCP Snooping)
- Verificación de que los ARP falsificados sean bloqueados (DAI)
- Validación del funcionamiento de ACLs mediante pings autorizados y bloqueados

Administradores de servidores – Sede Santiago (Yeinel De Los Santos Pimentel, Raelina Michelle Ferrera Perez)

Responsabilidades

1. Creación y administración de departamentos (VLANs)

1.1 Crear las VLAN correspondientes a los departamentos:

- VLAN Centro de Datos (10 hosts)
- VLAN Ventas (15 hosts)
- VLAN Administración (5 hosts)

1.2 Coordinar con los ingeniero de red para que estas VLANs tengan conectividad y direccionamiento adecuado.

---

2. Implementación de servicios en servidores de Santiago

2.1 Servidor DNS corporativo

- Configurar DNS utilizando el sufijo: EMPRESA DEL GRUPO.com.do
- Crear los registros necesarios (A, MX, CNAME, PTR) para soportar:

    el servidor web ○ el

    servidor de correo ○

        el propio servidor

    DNS

    otros servidores de la sede

2.2 Servidor DHCP

- Configurar DHCP para todas las VLANs de Santiago:

    Centro de Datos

        Ventas

        Administración

- Definir exclusiones y rangos para cada departamento.
- Asegurar que el DHCP atienda únicamente subredes de la sede Santiago.

2.3 Servidor Web corporativo(Encargado al Gerente de infraestructura)

- Montar la página web con la URL: www.EMPRESA DEL GRUPO.com.do
- Colocar el contenido que se entregó en el proyecto.
- Verificar el acceso al sitio desde todas las VLANs y sedes.

2.4 Servidor FTP / RADIUS

- Configurar servidor FTP para almacenamiento seguro.
- Implementar servidor RADIUS para autenticación centralizada (para routers/switches si aplica AAA).
- Crear un usuario para cada integrante del grupo en FTP/RADIUS.

2.5 Servidor de correo

- Configurar el servicio de correo con el dominio: EMPRESA DEL GRUPO.com.do
- Crear una cuenta de correo para cada integrante del grupo.
- Configurar registros DNS MX necesarios.
- Probar envío y recepción entre VLANs y entre sedes.

---

3. Integración con la red

3.1 Asegurar conectividad adecuada entre servidores y las VLANs creadas.
3.2 Verificar que los servidores respondan correctamente a peticiones desde Santo Domingo y Romana.
3.3 Coordinar con los ingenieros de red para el enrutamiento OSPF y filtrado según se requiera.

---

4. Documentación

4.1 Documentar la configuración de cada servidor (paso a paso). 4.2 Registrar rangos de DHCP, registros DNS y cuentas creadas.
4.3 Crear evidencias (capturas, pruebas de ping, acceso a servicios).
4.4 Entregar documentación final que será incluida en el informe del proyecto.

Ingeniero de telecomunicaciones (WAN) (ISP)(Erick Gabriel Encarnación Báez, Isaias Garcia Piadosa)

1.Configuracion del ISP

1.1 Configuración del enlace ISP en los routers de borde de cada sede.
1.2 Configuración del servicio DHCP con las direcciones IPv4 públicas proporcionadas por el ISP.

1.3 Implementar y verificar túneles VPN IPsec entre la sede principal y las sucursales.

1.4 Asignar el direccionamiento privado correspondiente a cada sede mediante la VPN.

1.5 Configurar rutas estáticas o de respaldo necesarias para la salida a Internet o enlaces alternos

2.Documentacion a entregar

1. Documentación del enlace ISP para cada sede, incluyendo tipo de conexión, gateway público, rango público asignado y parámetros entregados por el proveedor.
2. Configuración completa del router de borde por sede, mostrando interfaces WAN, DHCP del ISP, direcciones IPv4 públicas y verificación de conectividad externa.
3. Tabla detallada con las IPs públicas y privadas utilizadas en cada sede, indicando su función (WAN, túnel, gestión, servicios).
4. Documentación técnica completa de la implementación de VPN Ipsec
5. Evidencia de verificación del túnel VPN (capturas de *show crypto isakmp sa*, *show crypto ipsec sa*, *show interface tunnel* si usa GRE).
6. Tabla del direccionamiento privado asignado a cada sede a través de la VPN, indicando redes, gateway e integración con las VLAN internas.
7. Configuración y justificación de rutas estáticas o rutas de respaldo implementadas para la salida a Internet o enlaces alternos.
8. Pruebas de conectividad inter-sede a través de la VPN (pings, traceroute, reachability a servicios internos).