Documentación Técnica de Configuraciones de Seguridad en Switches

Este documento describe de forma técnica, organizada y clara las configuraciones implementadas en la red para aumentar la seguridad de la infraestructura LAN. Incluye Port-Security, protección contra VLAN hopping, DHCP Snooping, Dynamic ARP Inspection y protección STP.

4.1 Implementación de Port-Security (Violation Mode, Sticky MAC)

Port-Security es un mecanismo que permite restringir el acceso a un puerto del switch limitando las direcciones MAC permitidas. Esto mitiga ataques como MAC flooding y accesos no autorizados.

- switchport port-security: habilita port-security en el puerto.
- maximum X: cantidad máxima de direcciones MAC permitidas.
- mac-address sticky: aprende automáticamente las MAC conectadas.
- violation restrict: bloquea tramas no autorizadas y genera logs.

Con esto se controla qué dispositivos pueden conectarse y se reduce el riesgo de intrusiones.

4.2 Protección contra VLAN Hopping (DTP, Native VLAN, Pruning)

El VLAN hopping es un ataque donde un intruso intenta saltar de una VLAN a otra sin autorización. Las mitigaciones incluyen:

- switchport mode access: evita que el puerto negocie modos trunk.
- switchport nonegotiate: deshabilita DTP para impedir que el puerto intente formar un trunk.
- Configuración segura de Native VLAN y pruning (en enlaces trunk) para limitar VLANs permitidas.

Con esto se evita que un atacante fuerce un trunk o encapsule tramas 802.1Q maliciosas.

4.3 Protección contra ataques DHCP (DHCP Snooping)

DHCP Snooping previene ataques de rogue DHCP servers (servidores DHCP falsos) que intentan entregar configuraciones IP maliciosas.

- ip dhcp snooping: habilita la función.
- ip dhcp snooping vlan X: aplica la protección a VLAN específicas.
- trust: indica qué puertos están permitidos a enviar respuestas DHCP (normalmente enlaces hacia routers).
- limit rate: limita el número de mensajes DHCP para prevenir flooding.

Esto protege la asignación de direcciones evitando que atacantes tomen el rol de servidor DHCP.

4.4 Protección ARP (Dynamic ARP Inspection – DAI)

DAI evita ataques ARP Spoofing verificando que las respuestas ARP coincidan con la base de datos protegida (normalmente respaldada por DHCP Snooping).

• ip arp inspection vlan X: habilita DAI en VLAN seleccionadas.
• trust: puertos confiables que pueden enviar tramas ARP (típicamente uplinks).
• limit rate: limita la tasa de ARP para prevenir ARP flooding.

Esto garantiza integridad en la resolución ARP y evita ataques de suplantación.

4.5 Protección STP (BPDU Guard, Root Guard)

STP es crítico para evitar loops, pero puede ser vulnerado si un atacante envía BPDUs maliciosas para intentar convertirse en root bridge.

• BPDU Guard: deshabilita el puerto si recibe BPDUs inesperadas (protege puertos de acceso).
• Root Guard: impide que puertos no autorizados puedan convertirse en root port.

Estas protecciones aseguran estabilidad y evitan manipulación del árbol STP.

4.6 Implementación de ACLs de Filtrado según Criterios del Proyecto

Las ACLs (Access Control Lists) son mecanismos que permiten controlar el tráfico que entra o sale de una interfaz, aplicando reglas basadas en protocolos, direcciones IP y puertos. Su objetivo es **filtrar servicios no autorizados, mejorar la seguridad y limitar tráfico malicioso** dentro de la red corporativa.

En este proyecto, las ACLs cumplen tres funciones principales:

1. Permitir únicamente servicios corporativos autorizados.
2. Restringir y controlar el uso de ICMP para evitar reconocimiento o abusos.
3. Aplicar medidas básicas contra ataques DoS y tráfico anómalo.

Componentes principales de las ACLs

• **ACL CORPORATE-FILTER:** controla qué servicios corporativos están permitidos y bloquea tráfico no autorizado como P2P, streaming o puertos comunes de malware.
• **ACL ICMP-PROTECT:** regula los mensajes ICMP, permitiendo diagnósticos internos, pero bloqueando respuestas ICMP externas que podrían ser usadas en ataques.
• **ACL ANTIDOS:** bloquea patrones de tráfico anómalo o malformado (como puertos TCP inválidos) utilizados en ataques de denegación de servicio.

Explicación de cada parte de la configuración

• Filtrado de servicios corporativos
Esta parte de la ACL permite puertos asociados a:
- HTTP/HTTPS
- DNS
- Correo corporativo (POP3, IMAP, SMTP, SSL)
- SSH
- RDP
- VPN (IKE, IPsec)
- Radius para autenticación

Estos servicios son esenciales para la operación interna, por lo que se autorizan explícitamente.

• Bloqueo de tráfico P2P y aplicaciones no corporativas

Se bloquean rangos y puertos comúnmente utilizados por:
- BitTorrent
- Aplicaciones P2P
- Streaming no autorizado (como RTSP o puertos alternativos 8080 y 8888)
- Puertos 3074 usados en videojuegos y tráfico recreativo

Esto evita consumo excesivo de ancho de banda, fuga de información y entrada de malware por aplicaciones no controladas.

• Control de mensajes ICMP
La ACL ICMP-PROTECT evita que dispositivos externos envíen:
- Respuestas ICMP falsificadas
- Señales ICMP usadas en mapeo de red
- Tráfico ICMP malicioso

Aun así, se permite **echo (ping)** originado dentro de la red para fines de diagnóstico.

• Medidas Anti–DoS Básicas
La ACL ANTIDOS bloquea, entre otros:
- Tráfico TCP con puerto 0 (inválido, usado en ataques)
- Paquetes malformados asociados a escaneos o denegación de servicio

Esto agrega una capa adicional de seguridad para evitar sobrecarga o interrupciones en los switches.

Resultado final
Con estas ACLs aplicadas sobre las SVIs de las VLAN en los switches L3, se logra:
- Control granular del tráfico permitido en la red corporativa
- Reducción del riesgo por aplicaciones no autorizadas
- Prevención de escaneo externo y abuso de ICMP
- Mitigación básica de ataques DoS
- Mayor estabilidad, seguridad y cumplimiento de políticas de uso