SEGURIDAD EN NETWORKING

Unidad 2

Vulnerabilidades, procedimientos, acciones de mitigación y Controles de ISO 27001

ESCUELA DE INGENIERÍA Y CONSTRUCCIÓN

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Luis Ignacio Jaque

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Emilia De la Cruz Barrés

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan

EQUIPO DE DESARROLLO

Welean

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Aplican soluciones de firewalls, considerando políticas de la empresa y vulnerabilidades de redes.

Fuente: https://shutr.bz/3P6ABBm

Introducción

Una de las habilidades más importantes que necesita quienes administran las redes computacionales, es el dominio de las listas de control de acceso (ACL). Las ACL proporcionan capacidades de filtrado de paquetes para controlar el flujo de tráfico.

Los diseñadores de red utilizan firewalls (cortafuegos) para proteger las redes del uso no autorizado. Los firewalls son soluciones de hardware o de software que aplican las políticas de seguridad de la red. Imagine una cerradura en la puerta de una habitación dentro de un edificio. La cerradura permite que solo los usuarios autorizados que poseen una llave o una tarjeta de acceso puedan entrar. De igual forma, un firewall filtra los paquetes no autorizados o potencialmente peligrosos e impide que ingresen a la red.

En un router Cisco, puede configurar un firewall simple que proporcione capacidades básicas de filtrado de tráfico mediante ACL. Los administradores utilizan las ACL para filtrar el tráfico, permitiendo o bloqueando paquetes específicos en sus redes.

1. ¿Qué es un Firewall?

Un firewall (cortafuego) es un dispositivo de red que monitorea los paquetes que entran y salen de las redes, los bloquea o les permite de acuerdo con las reglas que se han establecido para definir qué tráfico es permisible y qué tráfico no lo es.

Inicialmente ubicados en los límites entre redes confiables y no confiables, los firewalls ahora también se despliegan para proteger los segmentos internos de las redes, como los centros de datos, de otros segmentos de las redes de las organizaciones.

Existen varios tipos de cortafuegos que se han desarrollado a lo largo de los años, haciéndose cada vez más complejos y teniendo en cuenta más parámetros a la hora de determinar si se debe permitir el paso del tráfico. Por lo general, se implementan como dispositivos creados por proveedores individuales, pero también se pueden comprar como dispositivos virtuales, es decir, como software que los clientes instalan en su propio hardware.

1.1. Tipos de firewalls

1.1.1. Cortafuegos basados en proxy

Estos cortafuegos actúan como una puerta de enlace entre los usuarios finales que solicitan datos y la fuente de estos. Los dispositivos del host se conectan al proxy, y el proxy hace una conexión separada a la fuente de datos. En respuesta, los dispositivos de origen hacen conexiones al proxy, y el proxy hace una conexión separada al dispositivo host.

Antes de pasar paquetes a una dirección de destino, el proxy puede filtrarlos para aplicar políticas y ocultar la ubicación del dispositivo del destinatario, pero también para proteger el dispositivo y la red del destinatario.

Ventajas	Desventajas
Los equipos fuera de la red que están protegidos sólo pueden recopilar información limitada sobre la red porque nunca están conectados directamente a ella.	La terminación de las conexiones entrantes y la creación de conexiones salientes más el filtrado causan retrasos que pueden degradar el rendimiento. A su vez, esto puede eliminar el uso de algunas aplicaciones a través del cortafuegos porque los tiempos de respuesta se vuelven demasiado lentos.

Tabla 1: Ventajas y desventajas cortafuego basado en proxy. (2022).

Fuente: Cisco Networking Academy.

1.1.2. Cortafuegos de estado

Una mejora del rendimiento en comparación con los cortafuegos basados en proxy se produjo en forma de cortafuegos de estado, que realizan un seguimiento de un reino de información sobre conexiones y hacen innecesario que el cortafuegos inspeccione todos los paquetes. Esto reduce en gran medida el retraso introducido por el cortafuegos.

Al mantener el estado de las conexiones, estos cortafuegos pueden, por ejemplo, no inspeccionar los paquetes entrantes que identifican como respuestas a conexiones salientes legítimas que ya han sido inspeccionadas. La inspección inicial establece que la conexión es permisible, y al preservar ese estado en su memoria, el cortafuegos puede pasar a través del tráfico subsiguiente que es parte de esa misma conversación sin inspeccionar cada paquete.

1.1.3. Cortafuegos de aplicaciones web

Los cortafuegos de aplicaciones web se sitúan de forma lógica entre los servidores que soportan las aplicaciones web e Internet, protegiéndolos de ataques HTML específicos, tales como secuencias de comandos entre sitios, inyección de SQL y otros. Pueden estar basados en hardware o en la nube, o pueden ser introducidos en las propias aplicaciones para determinar si se debe permitir el acceso a cada uno de los clientes que intentan llegar al servidor.

1.1.4. Cortafuegos de última generación

Los paquetes pueden filtrarse utilizando algo más que el estado de las conexiones y las direcciones de origen y destino. Aquí es donde entran en juego las NGFW, incorporan reglas sobre lo que se permite hacer a las aplicaciones individuales y a los usuarios, y mezclan los datos recopilados de otras tecnologías para tomar decisiones mejor informadas sobre el tráfico que se debe permitir y el que se debe reducir.

Ejemplo, algunos de estos NGFWs realizan filtrado de URLs, pueden terminar conexiones de capa de sockets seguros (SSL) y de seguridad de capa de transporte (TLS), y soportar redes de área extendida definidas por software (SD-WAN) para mejorar la eficiencia de cómo se aplican las decisiones dinámicas SD-WAN sobre conectividad.

1.2. Los cortafuegos no son suficientes

Las características que históricamente eran manejadas por dispositivos separados ahora se incluyen en muchas NGFW e incluyen:

1.2.1. Sistemas de prevención de intrusiones (IPS)

Mientras que las tecnologías básicas de cortafuegos identifican y bloquean ciertos tipos de tráfico de red, los IPSes utilizan una seguridad más granular, como el rastreo de firmas y la detección de anomalías, para evitar que las amenazas entren en las redes. Una vez separadas las plataformas, la funcionalidad IPS es cada vez más una característica estándar del cortafuegos.

1.2.2. Inspección profunda de paquetes (DPI)

La inspección profunda de paquetes es un tipo de filtrado de paquetes que mira más allá de la procedencia y destino de los paquetes e inspecciona su contenido, revelando, por ejemplo, a qué aplicación se está accediendo o qué tipo de datos se está transmitiendo. Esta información puede hacer posibles políticas más inteligentes y granulares para que el cortafuegos las aplique. El DPI puede utilizarse para bloquear o permitir el tráfico, pero también para restringir la cantidad de ancho de banda que se permite utilizar a determinadas aplicaciones.

1.2.3. Terminación SSL/TLS

El tráfico encriptado por SSL es inmune a la inspección de paquetes profundos porque su contenido no se puede leer. Algunos NGFWs pueden terminar el tráfico SSL, inspeccionarlo, y luego crear una segunda conexión SSL a la dirección de destino deseada. Esto se puede utilizar para evitar, por ejemplo, que los empleados malintencionados envíen información confidencial fuera de la red segura, permitiendo al mismo tiempo el paso del tráfico legítimo. Aunque es bueno desde el punto de vista de la protección de datos, la OMPD puede plantear problemas de privacidad, con la llegada de la seguridad de la capa de transporte (TLS) como una mejora de SSL, esta terminación y *proxying* puede aplicarse también a TLS.

1.2.4. Sandboxing

Los archivos adjuntos entrantes o las comunicaciones con fuentes externas pueden contener código malicioso. Mediante el *sandboxing*, algunos NGFWs pueden aislar estos archivos adjuntos y cualquier código que contengan, ejecutarlos y averiguar si son maliciosos. La desventaja de este proceso es que puede consumir muchos ciclos de CPU e introducir retrasos notables en el tráfico que fluye a través del cortafuegos.

Las características que podrían incorporarse en las NGFW, es el apoyo a la toma de datos recopilados por otras plataformas y su uso para tomar decisiones de cortafuegos. Por ejemplo, si los investigadores han identificado una nueva firma de malware, el cortafuegos puede captar esa información y comenzar a filtrar el tráfico que contiene la firma.

1.3. Proveedores de cortafuegos más populares

Según el último ranking de Gartner para Firewall de red 2021, los proveedores designados como líderes son Palo Alto *Networks, Fortiner y Check Point Software Technologies*.

¿Cuáles son las principales tendencias que impulsan el mercado de seguridad de firewalls de red según Gartner?

Para 2025, el 30% de las nuevas implementaciones de firewalls distribuidos en sucursales cambiarán a firewall como servicio. En la actualidad no se llega al 10%.

El *Firewall* como servicio, (también conocido como FWaaS), ayuda a llevar las capacidades tradicionales de firewall a la nube, y permite a las empresas ampliar las políticas de seguridad a usuarios y dispositivos que trabajen desde cualquier ubicación.

Para finales de 2025, el 35% del gasto del usuario final en firewalls de red se incluirá dentro de los acuerdos de licencia empresarial (ELA) con el mismo proveedor. (En 2021 esa cantidad es inferior al 10%).

Figura 1: Cuadrante mágico de Gartner para firewalls de red 2021.

Fuente: Blog tecnozero.

En este Cuadrante Mágico, Gartner evaluó las fortalezas y debilidades de los 19 proveedores que considera más importantes en el mercado, que son:

Alibaba Cloud, Amazon Web Services, Barracuda, Cato Networks, Check Point Software Technologies, Cisco, Forcepoint, Fortinet, H3C, Hillstone Networks, Huawei, Juniper, Microsoft, Palo Alto Networks, Sangfor, SonicWall, Sophos, Versa Networks y WatchGuard.

El mercado de *firewalls* de redes empresariales se compone principalmente de dispositivos de *hardware*, aunque cada vez son más importantes los dispositivos virtuales implementados en la nube pública (*Amazon Web Services, Microsoft Azure y Google Cloud*), en la nube privada y los centros de datos.

2. ¿Qué es una Lista de Acceso (ACL)?

Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

Cuando se las configura, las ACL realizan las siguientes tareas:

- Limitan el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloqueen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.

- Proporcionan control del flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de *routing* para asegurar que las actualizaciones provienen de un origen conocido.

- Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área. Por ejemplo, se puede restringir el acceso a la red de Recursos Humanos a los usuarios autorizados.

- Filtran el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.

- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

Los routers no tienen ACL configuradas de manera predeterminada, por lo que no filtran el tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing. Sin embargo, cuando se aplica una ACL a una interfaz, el router realiza la tarea adicional de evaluar todos los paquetes de red a medida que pasan a través de la interfaz para determinar si el paquete se puede reenviar.

Además de permitir o denegar tráfico, las ACL se pueden utilizar para seleccionar tipos de tráfico para analizar, reenviar o procesar de otras formas. Por ejemplo, se pueden utilizar ACL para clasificar el tráfico a fin de permitir el procesamiento por prioridad. Esta capacidad es similar a tener un pase vip para un concierto o un evento deportivo. El pase vip brinda a ciertos invitados privilegios que no se ofrecen a los asistentes que poseen entradas de admisión general, como prioridad de entrada o el ingreso a un área restringida.

En la siguiente figura, se muestra una topología de ejemplo a la que se le aplicaron ACL.

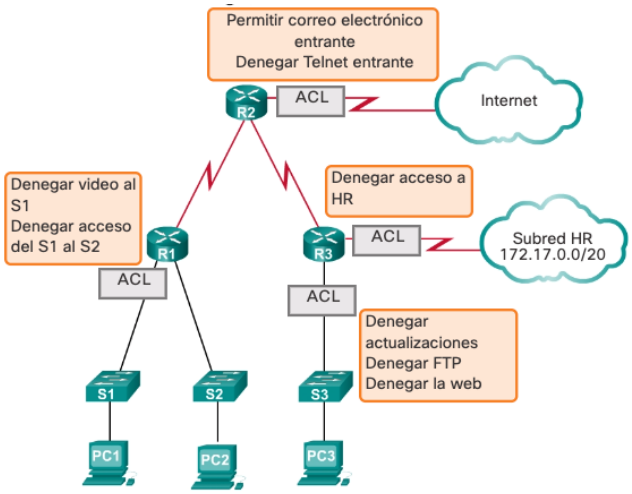


Figura 2: ¿Qué es una ACL?

Fuente: Cisco Networking Academy (2022).

2.1. Filtrado de paquetes

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como "entradas de control de acceso" (ACE). Las ACE también se denominan comúnmente "instrucciones de ACL". Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las ACE. Este proceso se denomina filtrado de paquetes

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios determinados. El filtrado de paquetes puede producirse en la capa 3 o capa 4, como se muestra en la figura 3. Las ACL estándar filtran sólo en la Capa 3. Las ACL extendidas filtran en las capas 3 y 4.

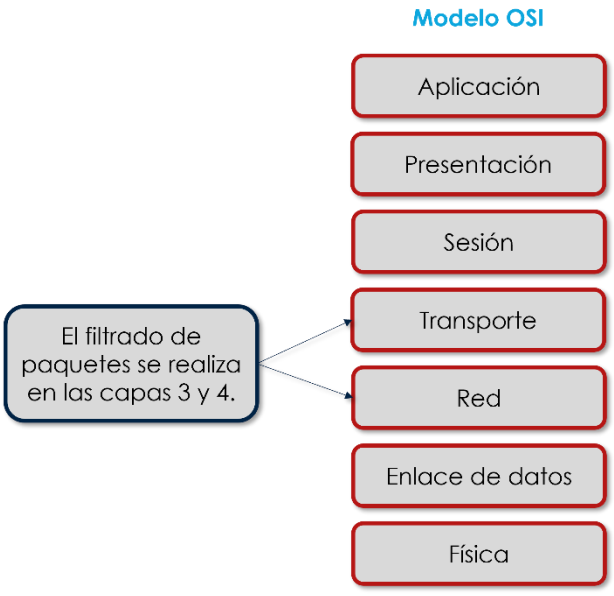


Figura 3 : Filtrado de paquetes.

Fuente: Cisco Networking Academy (2022).

El criterio de filtrado establecido en cada ACE de una ACL de IPv4 estándar es la dirección IPv4 de origen. Un router configurado con una ACL de IPv4 estándar recupera la dirección IPv4 de origen del encabezado del paquete. El router comienza en la parte superior de la ACL y compara la dirección con cada ACE de manera secuencial. Cuando encuentra una coincidencia, el router realiza la instrucción, que puede ser permitir o denegar el paquete. Una vez que se halla una coincidencia, las ACE restantes de la ACL, si las hubiera, no se analizan. Si la dirección IPv4 de origen no coincide con ninguna ACE en la ACL, se descarta el paquete.

La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no tiene, por lo menos, una instrucción permit bloqueará todo el tráfico.

2.2. Funcionamiento de las ACL

Las ACL definen el conjunto de reglas que proporcionan un control adicional para los paquetes que ingresan por las interfaces de entrada, para los que retransmiten a través del router y para los que salen por las interfaces de salida del router. Las ACL no operan sobre paquetes que se originan en el router mismo.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente, como se muestra en la siguiente figura.

Figura 4: ACL de entrada y salida.

Fuente: Cisco Networking Academy (2022).

- **ACL de entrada:** los paquetes entrantes se procesan antes de enrutarse a la interfaz de salida. Las ACL de entrada son eficaces, porque ahorran la sobrecarga de enrutar búsquedas si el paquete se descarta. Si las ACL permiten el paquete, este se procesa para el routing. Las ACL de entrada son ideales para filtrar los paquetes cuando la red conectada a una interfaz de entrada es el único origen de los paquetes que se deben examinar.

- **ACL de salida:** los paquetes entrantes se enrutan a la interfaz de salida y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica el mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

2.3. Introducción a las máscaras *wildcard* en ACL

2.3.1. Máscara wildcard

Las ACE de IPv4 incluyen el uso de máscaras *wildcard*. Una máscara *wildcard* es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección debe examinar para obtener una coincidencia.

Como ocurre con las máscaras de subred, los números 1 y 0 en la máscara wildcard identifican lo que hay que hacer con los bits de dirección IPv4 correspondientes. Sin embargo, en una máscara wildcard, estos bits se utilizan para fines diferentes y siguen diferentes reglas.

Las máscaras de subred utilizan unos y ceros binarios para identificar la red, la subred y la porción de host de una dirección IPv4. Las máscaras wildcard utilizan unos y ceros binarios para filtrar direcciones IPv4 individuales o grupos de direcciones IPv4 para permitir o denegar el acceso a los recursos.

Las máscaras wildcard y las máscaras de subred se diferencian en la forma en que establecen la coincidencia entre los unos y ceros binarios. Las máscaras wildcard utilizan las siguientes reglas para establecer la coincidencia entre los unos y ceros binarios:

- Bit 0 de máscara wildcard: se establece la coincidencia con el valor del bit correspondiente en la dirección.
- Bit 1 de máscara wildcard: se omite el valor del bit correspondiente en la dirección.

En la siguiente figura se muestra cómo las diferentes máscaras wildcard filtran las direcciones IPv4. Recuerde que, en el ejemplo, el valor binario 0 indica un bit que debe coincidir y el valor binario 1 indica un bit que se puede ignorar.

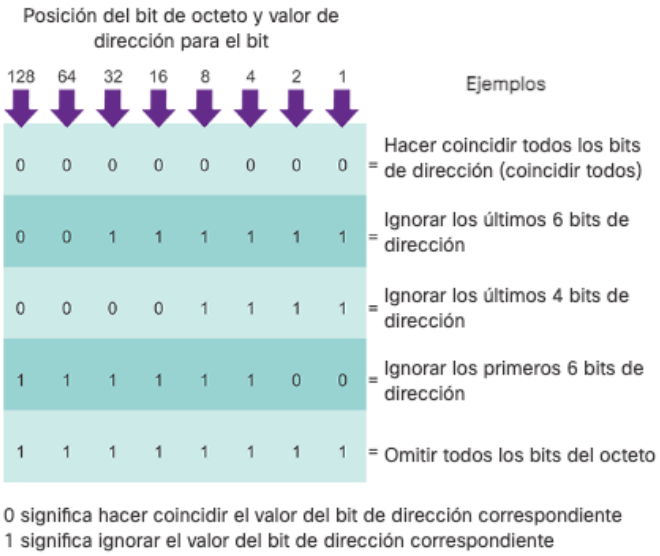


Figura 5: Máscara wildcard.

Fuente: Cisco Networking Academy (2022).

A las máscaras wildcard a menudo se las denomina “máscaras inversas”. La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no es una coincidencia, en las máscaras wildcard es al revés.

2.3.2. Uso de una máscara wildcard

En la tabla de la siguiente tabla, se muestran los resultados de la aplicación de una máscara wildcard 0.0.255.255 a una dirección IPv4 de 32 bits. Recuerde que un 0 binario indica un valor con coincidencia.

Nota: a diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir.

	Dirección decimal	Dirección binaria
Dirección IP para procesar	192.168.10.0	11000000.10101000.00001010.00000000
Mascara wildcard	0.0.255.255	00000000.00000000.11111111.11111111
Dirección IP resultante	192.168.0.0	11000000.10101000.00000000.00000000

Figura 6: Ejemplo máscara wildcard.

Fuente: Cisco Networking Academy (2022).

2.3.3. Ejemplos de máscara wildcard

- Máscaras wildcard para establecer coincidencias con subredes IPv4:

Se necesita práctica para calcular la máscara wildcard. En la siguiente figura, se proporcionan tres ejemplos de máscara wildcard.

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Mascara wildcard	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Mascara wildcard	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Mascara wildcard	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Figura 7: Máscaras wildcard para establecer coincidencias con host y subredes IPv4.

Fuente: Cisco Networking Academy (2022).

En el primer ejemplo, la máscara wildcard estipula que cada bit en la IPv4 192.168.1.1 debe coincidir con exactitud.

En el segundo ejemplo, la máscara wildcard estipula que no habrá coincidencias.

En el tercer ejemplo, la máscara wildcard estipula que cualquier host dentro de la red 192.168.1.0/24 tendrá una coincidencia.

- Máscaras wildcard para establecer coincidencias con rangos:

Los dos ejemplos en la siguiente figura son más complejos. En el ejemplo 1, los primeros dos octetos y los primeros cuatro bits del tercer octeto deben coincidir con exactitud. Los cuatro últimos bits del tercer octeto y el último octeto pueden ser cualquier número válido. Esto genera una máscara que verifica el rango de redes 192.168.16.0 a 192.168.31.0.

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.16.0	11000000.10101000.00010000.00000000
Mascara wildcard	0.0.0.0	00000000.00000000.00001111.11111111
Resultado	De 192.168.16.0 a 192.168.31.255	De 11000000.10101000.00010000.00000000 a 11000000.10101000. 00011111.11111111

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.0	11000000.10101000.00000001.00000000
Mascara wildcard	0.0.254.255	00000000.00000000.11111110.11111111
Resultado	192.168.1.0	11000000.10101000.00000001. 00000000
	Todas las subredes con números impar en la red principal 192.168.0.0	

Figura 8: Máscaras wildcard para establecer coincidencias con rangos.

Fuente: Cisco Networking Academy (2022).

En el ejemplo 2, se muestra una máscara wildcard que coincide con los primeros dos octetos y el bit con menor importancia del tercer octeto. El último octeto y los primeros siete bits en el tercer octeto pueden ser cualquier número válido. Esto genera una máscara que permite o deniega todos los hosts de subredes impares de la red principal 192.168.0.0.

2.3.4. Cálculo de la máscara wildcard

El cálculo de máscaras wildcard puede ser difícil. Un método abreviado es restar la máscara de subred a 255.255.255.255.

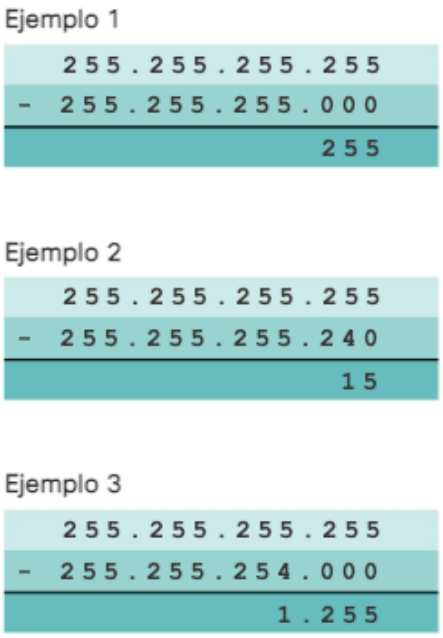


Figura 9: Cálculo de máscara wildcard.

Cisco Networking Academy (2022).

Cálculo de máscara wildcard: ejemplo 1

En el primer ejemplo en la figura anterior, suponga que desea permitir el acceso a todos los usuarios en la red 192.168.3.0. Dado que la máscara de subred es 255.255.255.0, podría tomar 255.255.255.255 y restarle la máscara de subred 255.255.255.0. El resultado genera la máscara wildcard 0.0.0.255.

Cálculo de máscara wildcard: ejemplo 2

En el segundo ejemplo en la figura anterior, suponga que desea permitir el acceso a la red a los 14 usuarios en la subred 192.168.3.32/28. La máscara de subred para la subred IPv4 es 255.255.255.240; por lo tanto, tome 255.255.255.255 y réstele la máscara de subred 255.255.255.240. Esta vez, el resultado genera la máscara wildcard 0.0.0.15.

Cálculo de máscara wildcard: ejemplo 3

En el tercer ejemplo en la figura anterior, suponga que solo quiere establecer la coincidencia con las redes 192.168.10.0 y 192.168.11.0. Una vez más, tome 255.255.255.255 y reste la máscara de subred regular que, en este caso, es 255.255.254.0. El resultado es 0.0.1.255.

Puede lograr el mismo resultado con instrucciones como las dos que se muestran a continuación:

R1(config)# **access-list 10 permit 192.168.10.0**

R1(config)# **access-list 10 permit 192.168.11.0**

Resulta mucho más eficaz configurar la máscara wildcard de la siguiente manera:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.1.255**

Considere un ejemplo en el cual se deben hacer coincidir las redes en el rango de 192.168.16.0/24 a 192.168.31.0/24. Estas redes resumirán en 192.168.16.0/20. En este caso, 0.0.15.255 es la máscara wildcard correcta para configurar una declaración eficaz de ACL, como se muestra a continuación:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**

2.3.5. Palabras clave de las máscaras wildcard

Trabajar con representaciones decimales de los bits binarios de máscaras wildcard puede ser tedioso. Para simplificar esta tarea, las palabras clave *host y any* ayudan a identificar los usos más comunes de las máscaras wildcard. Estas palabras clave eliminan la necesidad de introducir máscaras wildcard para identificar un host específico o toda una red. También facilitan la lectura de una ACL, ya que proporcionan pistas visuales en cuanto al origen o el destino de los criterios.

La palabra clave host reemplaza la máscara 0.0.0.0. Esta máscara indica que todos los bits de direcciones IPv4 deben coincidir para filtrar solo una dirección de host.

La opción any sustituye la dirección IP y la máscara 255.255.255.255. Esta máscara establece que se omita la dirección IPv4 completa o que se acepte cualquier dirección, como se puede apreciar en la siguiente figura.

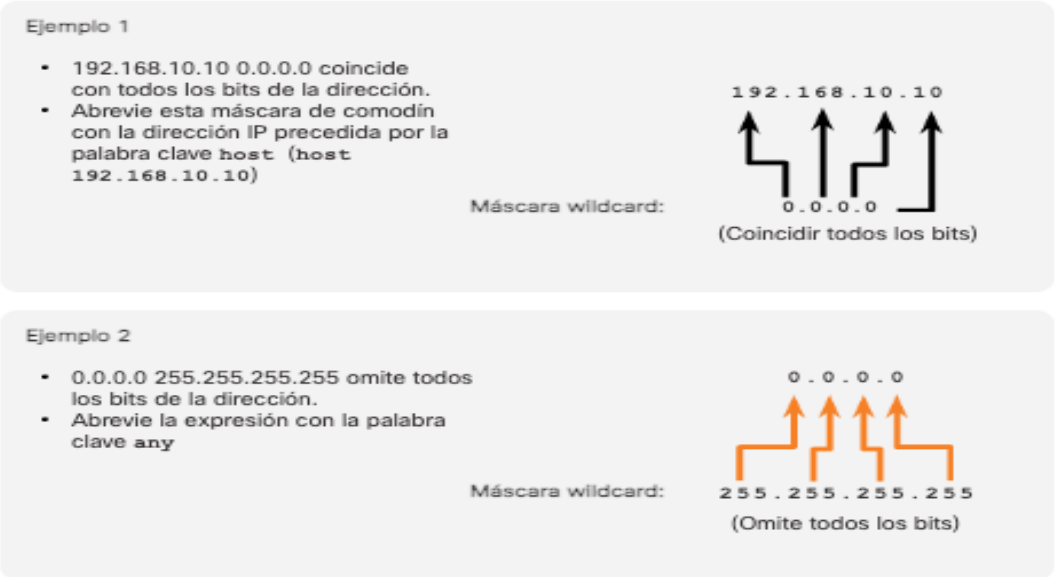


Figura 10: Abreviatura de la máscara de bits wildcard.

Fuente: Cisco Networking Academy (2022).

- **Ejemplo 1: proceso de máscara wildcard con una única dirección IPv4**

En el ejemplo 1 en la figura 10, en vez de introducir **192.168.10.10 0.0.0.0**, puede utilizar **host 192.168.10.10**.

- **Ejemplo 2: proceso de máscara wildcard con coincidencia con cualquier dirección IPv4**

En el ejemplo 2 en la figura 10, en vez de introducir **0.0.0.0 255.255.255.255**, puede utilizar la palabra clave **any** (cualquier) sola.

2.3.6. Ejemplos de palabras claves de máscara wildcard

En el ejemplo 1 de la siguiente figura, se muestra cómo utilizar la palabra clave any para sustituir la dirección IPv4 0.0.0.0 por una máscara wildcard 255.255.255.255.

En el ejemplo 2 de la siguiente figura, se muestra cómo utilizar la palabra clave host para sustituir la máscara wildcard para identificar un único host.

Figura 11: Palabras claves any y host.

Fuente: Cisco Networking Academy (2022).

2.4. Una conversación TCP

Los administradores pueden controlar el tráfico de red basándose en varias características, incluido el puerto TCP que se solicita. Es más fácil comprender cómo filtra el tráfico una ACL si se examina el diálogo que se produce durante una conversación TCP, por ejemplo, cuando se solicita una página web.

Cuando un cliente solicita datos a un servidor web, IP administra la comunicación entre la computadora (origen) y el servidor (destino). TCP administra la comunicación entre el navegador web (aplicación) y el software del servidor de red.

En la animación que se muestra en la siguiente figura, se ilustra cómo se lleva a cabo una conversación TCP/IP. Los segmentos TCP se marcan con indicadores que denotan

su objetivo: la sesión comienza (se sincroniza) con un indicador SYN, el indicador ACK es un acuse de recibo de un segmento esperado, y un indicador FIN finaliza la sesión. Un indicador SYN/ACK confirma que la transferencia está sincronizada. Los segmentos de datos TCP incluyen el protocolo del nivel más alto necesario para dirigir los datos de aplicación a la aplicación correcta.

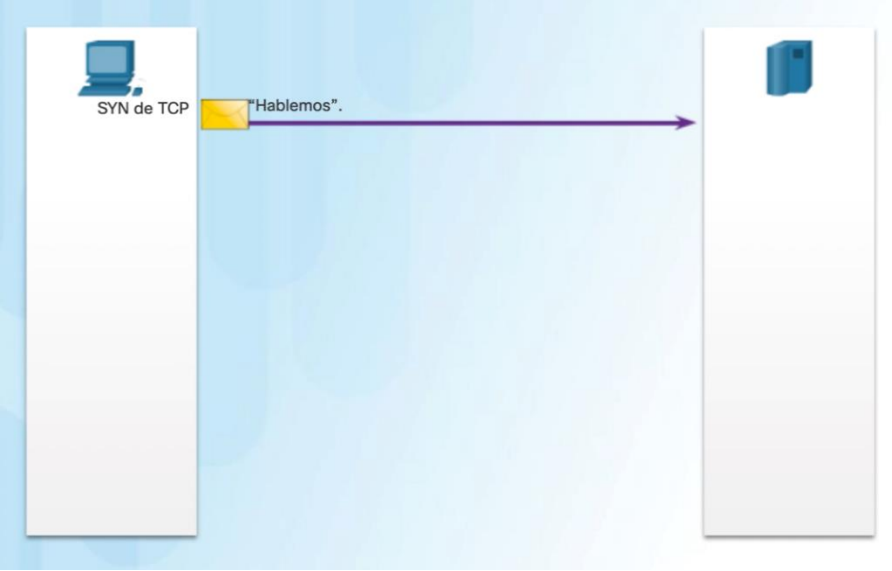


Figura 12: Una conversación TCP.

Fuente: Cisco Networking Academy (2022).

Los segmentos de datos TCP también identifican el puerto que coincide con el servicio solicitado. En la siguiente figura, se muestran los rangos de puertos UDP y TCP.

Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Entre 0 y 1023
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Figura 13: Números de puerto.

Fuente: Cisco Networking Academy (2022)

La siguiente figura muestra una lista de números de puertos conocidos.

Número de puerto	Protocolo	Aplicación	Acrónimo
20	TCP	Protocolo de transferencia de archivos (datos)	FTP
21	TCP	Protocolo de transferencia de archivos (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Protocolo simple de transferencia de correo	SMTP
53	UDP, TCP	Servicio de nombres de dominios	DNS
67	UDP	Protocolo de configuración dinámica de host (servidor)	DHCP
68	UDP	Protocolo de configuración dinámica de host (cliente)	DHCP
69	UDP	Protocolo trivial de transferencia de archivos	TFTP
80	TCP	Protocolo de transferencia de hipertexto	HTTP
110	TCP	Protocolo de oficina de correos versión 3	POP3
143	TCP	Protocolo de acceso a mensajes de Internet	IMAP
161	UDP	Protocolo simple de administración de redes	SNMP
443	TCP	Protocolo seguro de transferencia de hipertexto	HTTPS

Figura 14: Números de puertos reconocidos.

Fuente: Cisco Networking Academy (2022).

3. Configuración básica de un dispositivo Cisco en un entorno gráfico

Una de las formas más sencillas de configurar los parámetros y realizar cambios en un switch es acceder a su interfaz de usuario web. La interfaz de usuario web también se denomina interfaz basada en web, guía basada en web, utilidad basada en web, página de configuración web o utilidad de configuración web.

Al configurar un switch nuevo, Cisco Business le recomienda que realice las configuraciones del switch antes de conectarlo a la red. Esto puede ayudar a evitar posibles problemas y conflictos.

Lista de switches que pueden configurarse de esta forma:

SF300	**SF500**	**SG550X**
SG300	**SG500**	**SG550XG**
SF350	**SG500X**	**CBS220**
SG350	**SG500XG**	**CBS250**
SG350X	**SF550**	**CBS350**
SG350XG	**SF550X**	

Tabla 2: Lista de switches

Fuente: Elaboración propia

Todos los switches enumerados a continuación son un switch administrado y vienen con una interfaz de usuario web. Este tipo de interfaz, que se muestra en la pantalla, muestra opciones para la selección. No necesita saber ningún comando para navegar por estas pantallas. La interfaz de usuario web proporciona al administrador una herramienta que contiene todas las características posibles que se pueden cambiar para modificar el rendimiento de un switch. Además, la interfaz de usuario web puede proporcionar acceso a una cuenta de invitado, lo que permite al usuario ver la configuración sin permitir ningún cambio.

3.1. Conectar al switch

Dado que el switch no está en una red, se debe conectar un extremo de un cable Ethernet a un puerto numerado del switch y el otro extremo al computador. Asegurándose de que el switch está conectado a la corriente.

3.2. Determinar la dirección IP

Para acceder a la interfaz de usuario web, de debe conocer la dirección IP del switch. Como, por ejemplo, se puede realizar una de las siguientes opciones:

- Si su switch Cisco Business es nuevo, la dirección IP predeterminada es 192.168.1.254.
- Si no puede recordar la dirección IP o no tiene una configuración especial, utilice un clip abierto para presionar el botón de reinicio del switch durante al menos 10 segundos mientras está encendido. Esto restablecerá el switch a la configuración predeterminada y a la dirección IP predeterminada 192.168.1.254.

- Si establece una dirección IP estática del switch, puede introducir esa dirección IP en lugar de la predeterminada. Esto no se recomienda, ya que puede haber configuraciones en conflicto que pueden crear problemas en su red existente.

3.3. Acceso a la interfaz de usuario web del switch

Ahora que conoce la dirección IP del switch, puede acceder a la interfaz de usuario web.

Paso 1

Abra un navegador web.

Figura 15: Paso 1A – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Si no ve el explorador Web que desea utilizar, puede acceder a él en la barra de búsqueda inferior izquierda de un equipo con Windows. Comience a escribir el nombre de la aplicación y selecciónelo cuando aparezca como una opción.

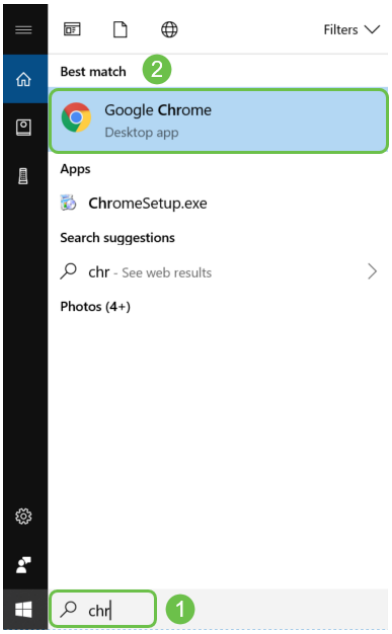


Figura 16: Paso 1B – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Paso 2

Ingrese 192.168.1.254, o la dirección IP estática si está configurada, y haga clic en **Enter** en el teclado. Esto debería abrir la interfaz de usuario Web, mostrando primero la pantalla de inicio de sesión.

Al acceder a un switch, esta dirección IP predeterminada sólo se aplica en situaciones en las que el switch no está conectado a un router y el ordenador está conectado directamente al switch. Si el switch está conectado a un router, el protocolo de configuración dinámica de host (DHCP) asignará de forma predeterminada una dirección IP y puede ser diferente.

Figura 17: Paso 2 – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Paso 3

Si ve una pantalla de inicio de sesión, vaya directamente al **Paso 7**.

Si recibe una advertencia de que no es seguro. Esto se debe a que no tiene un certificado registrado para el switch. Puede elegir *Proceed*, *Add Exception* o *Advanced*. Esto variará según el navegador web.

Si dispone de un bloqueador de ventanas emergentes, deberá hacer clic para permitir la ventana emergente antes de continuar. La notificación suele aparecer en la parte superior derecha de la pantalla.

En este ejemplo, Chrome se utilizó para un navegador web. Aparece este mensaje, haga clic en **Avanzadas**.

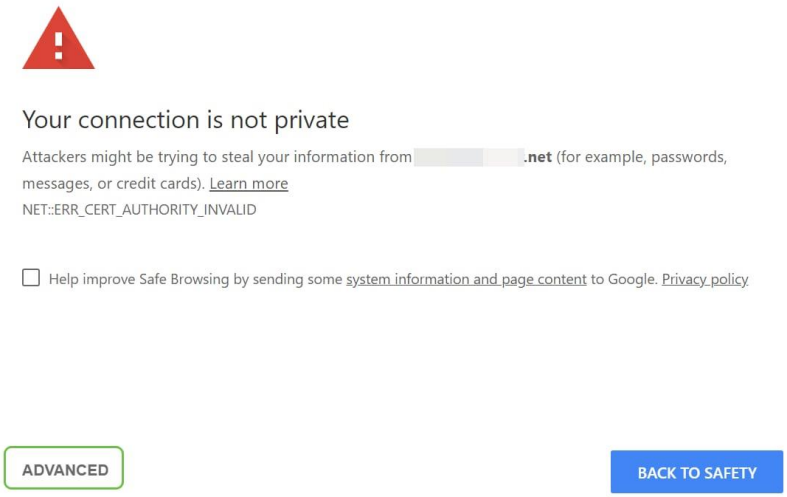


Figura 18: Paso 3 – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022).*https://bit.ly/3vIYSX6*

Paso 4

Se abrirá una nueva pantalla y tendrá que hacer clic en *Proceed to* (dirección IP utilizada para acceder al switch) (no seguro).

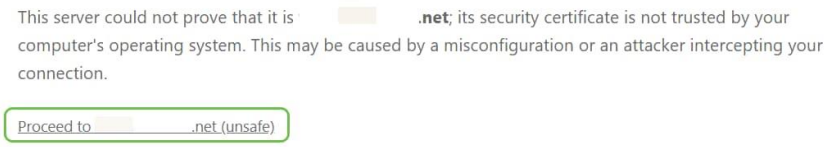


Figura 19: Paso 4A – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Si utiliza Firefox como navegador web, haría clic en **Avanzado**.

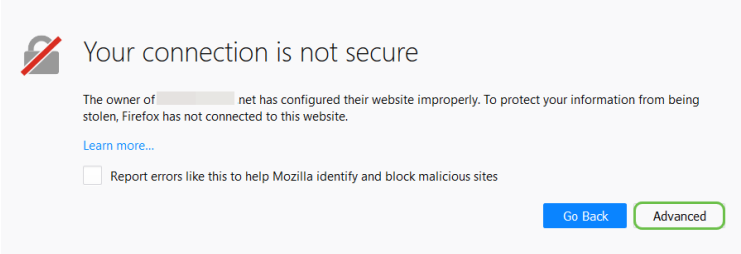


Figura 20: Paso 4B – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Paso 5

Haga clic en **Agregar excepción.**

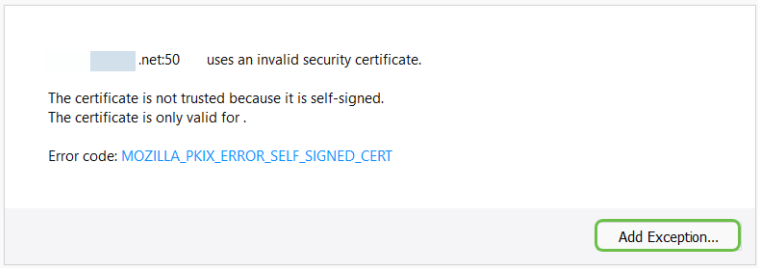


Figura 21: Paso 5 – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Paso 6

Haga clic en **Confirmar excepción de seguridad.**

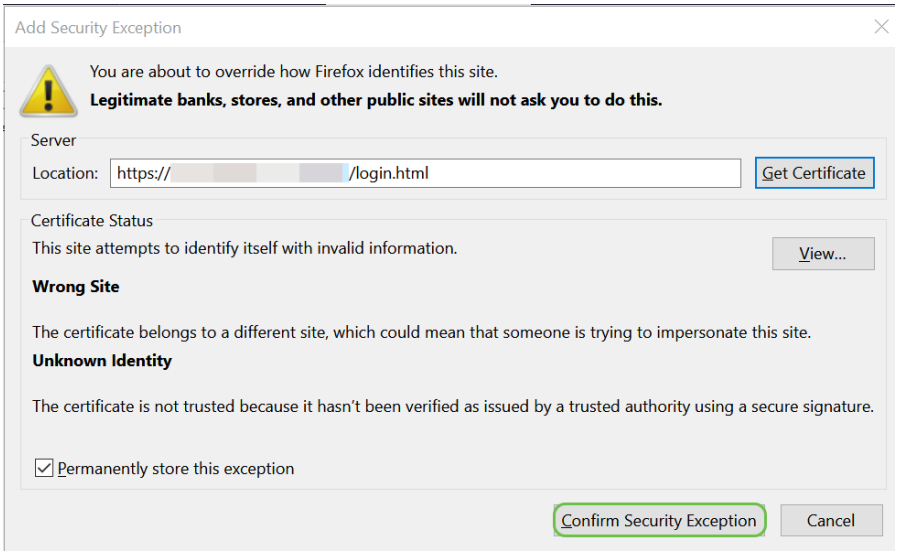


Figura 22: Paso 6 – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022.)*https://bit.ly/3vIYSX6*

Paso 7

Luego debe ingresar un **nombre de usuario** y **contraseña**. Las credenciales predeterminadas son *cisco* para el nombre de usuario y la contraseña la primera vez. Los switches más antiguos pueden utilizar *admin* como nombre de usuario y contraseña predeterminados. Se recomienda encarecidamente cambiar la contraseña para que sea más compleja por motivos de seguridad.

Si no ve una pantalla de inicio de sesión, consulte la sección **Consejos para la resolución de problemas** a continuación.

Figura 23: Paso 7 – Acceso a interfaz de usuario web.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Ahora debe tener acceso a la interfaz de usuario web del switch que incluye un panel de navegación en el lado izquierdo. Contiene una lista de las funciones de nivel superior del switch.

Los colores de esta página pueden variar, así como las funciones de nivel superior, según el equipo y la versión del firmware. Las categorías y opciones varían entre los switches.

Este es un ejemplo del panel de navegación en un switch SG550.

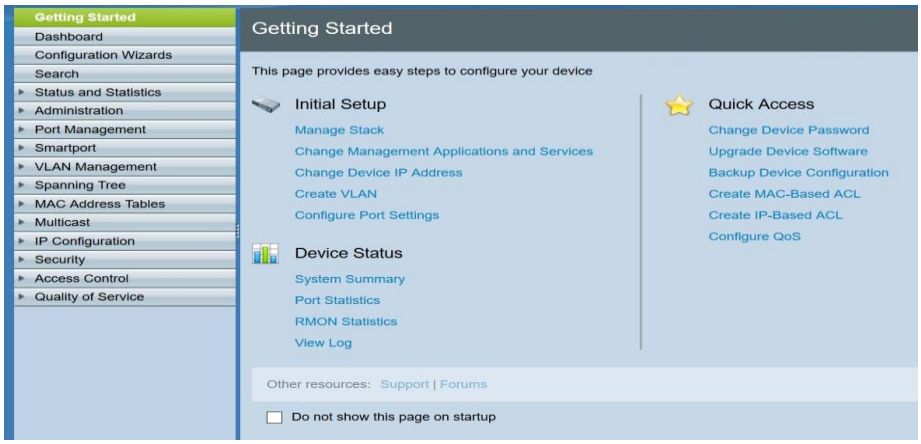


Figura 24: Ejemplo de panel de navegación 1.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Este es un ejemplo del panel de navegación en un switch CBS350.

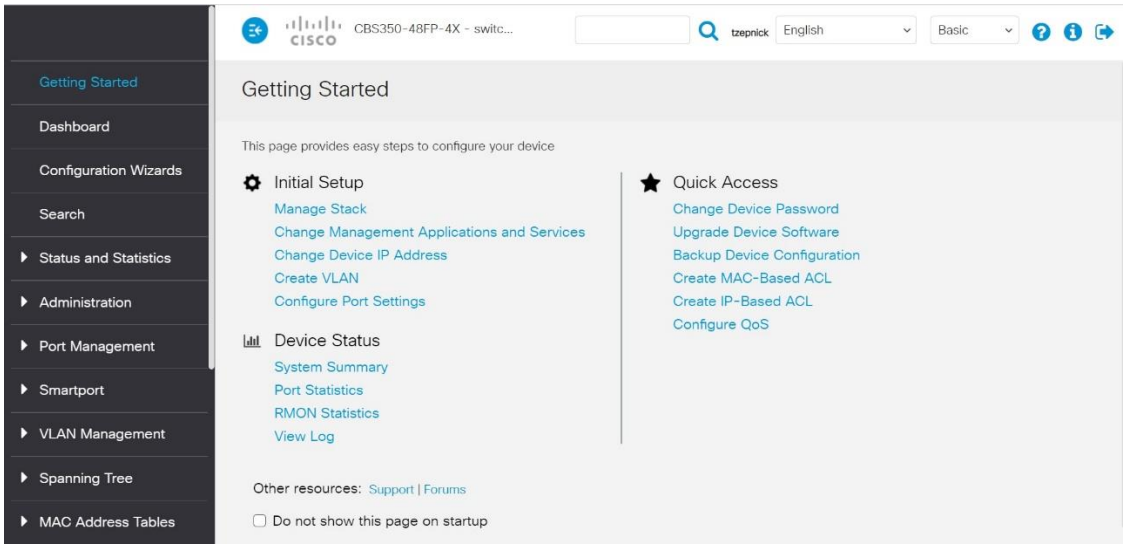
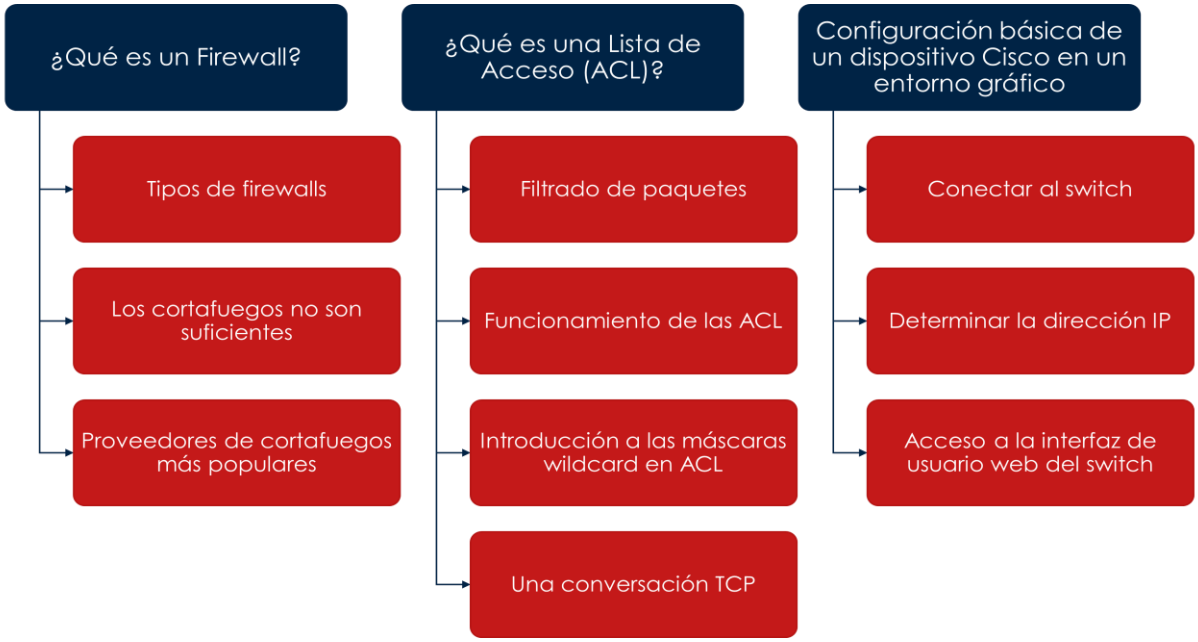


Figura 25: Ejemplo de panel de navegación 2.

Fuente: Cisco. (2022). *https://bit.ly/3vIYSX6*

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



Los *routers* no filtran tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de *routing*.

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete. Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte.

Una ACL es una lista secuencial de instrucciones *permit* o deny. La última instrucción de una ACL siempre es una instrucción deny implícita que bloquea todo el tráfico. Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, es posible agregar la instrucción **permit any**.

Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada entrada, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente.

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. La regla básica para la colocación de una ACL estándar es colocarla cerca del destino.

Las ACL extendidas filtran paquetes según varios atributos: el tipo de protocolo, la dirección IPv4 de origen o de destino y los puertos de origen o de destino. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen.

El comando de configuración *global* ***access-list*** define una ACL estándar con un número entre 1 y 99. El nombre ***ip access-list standard*** se utiliza para crear una ACL con nombre estándar.

Después de que se configura una ACL, se vincula a una interfaz mediante el comando ***ip access-group*** del modo de configuración de interfaz. Recuerde estas reglas: una ACL por protocolo, una ACL por dirección, una ACL por interfaz.

Para eliminar una ACL de una interfaz, primero introduzca el comando **no *ip access-group*** en la interfaz y, a continuación, introduzca el comando global ***no access-list*** para eliminar la ACL completa.

Los comandos ***show running-config*** y ***show access-lists*** se utilizan para verificar la configuración de la ACL. El comando ***show ip interface*** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.

El comando ***access-class*** configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada y las direcciones en una lista de acceso.

Referencias bibliográficas

- CCNA desde cero. (2022). *¿Qué es un Firewall? Cómo funcionan y cómo encajan en la seguridad*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3zH2XO6

- Tecnozero Soluciones Informaticas. (s. f.). *Cuadrante mágico de Gartner para firewalls de red 2021*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3cVdmwP

- Cisco Networking Academy (2022). *Conexión de redes. Capítulo 4 – Listas de Control de acceso*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3vzi7lQ

- Cisco Networking Academy (2022). *Principios básicos de routing y switching. Capítulo 7 – Listas de Control de acceso*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3vzi7lQ

- Cisco (2022). *Cómo iniciar sesión en la interfaz de usuario web de un switch empresarial de Cisco*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3vIYSX6