Informe técnico

Acceso unificado seguro con switches Cisco Catalyst de la serie 2960-X y 2960-XR

Descripción general

Los switches Cisco® Catalyst® de la serie 2960-X y 2960-XR son las plataformas de switching de acceso líderes de la industria que permiten mayor productividad y dinamismo empresarial, con características diseñadas para abordar las megatendencias en redes corporativas, como transición IPv6, Bring Your Own Device (BYOD) y movilidad. Los switches Cisco Catalyst 2960-X y 2960-XR proporcionan funciones de seguridad que permiten que dichas transiciones en la red se realicen de manera segura y eficiente.

Los switches Cisco Catalyst 2960-X y 2960-XR proporcionan un conjunto completo e integral de funciones de seguridad diseñadas para:

- Asegurar la red de interceptación de tráfico, suplantación de identidad y ataques de denegación de servicio (DoS).
- Controlar el acceso a los recursos en su red con listas de control de acceso (ACL), incluidas ACL por tipo de usuario/dispositivo
- Asegurar el acceso a la red en función de la identidad y el rol del usuario
- Proporcionar políticas basadas en dispositivos a través de la creación de perfiles de dispositivos
- Proteger la confidencialidad e integridad del tráfico de red a través del cifrado* (funcionalidad de hardware)
- Arrancar con seguridad las imágenes de software con firma digital de Cisco IOS®

Como parte de la arquitectura de Acceso unificado de Cisco, los switches Cisco Catalyst 2960-X y 2960-XR representan una infraestructura de red que es compatible con clasificación y aplicación de políticas distribuidas en la capa de acceso, con definiciones de políticas de la plataforma Cisco One Policy, Cisco Identity Services Engine (ISE).

Los switches Cisco Catalyst 2960-X y 2960-XR permiten asegurar las redes y proporcionan acceso seguro a través de las siguientes categorías de funciones primarias:

- **Seguridad de primer salto (FHS) en IPv4:** los switches Cisco Catalyst ofrecen Cisco Integrated Security Features (CISF), una solución líder del sector que proporciona capacidades superiores de defensa ante amenazas de capa 2 a fin de atenuar los ataques por intermediario, tales como la suplantación de identidad de MAC, IP y protocolo de resolución de direcciones (ARP). Esta solución ofrece una seguridad sólida en toda la red a través de herramientas poderosas y fáciles de usar que previenen eficazmente las amenazas de seguridad de capa 2 más comunes y potencialmente dañinas.
- **Seguridad de primer salto en IPv6:** IPv6 plantea un número de preocupaciones FHS que no estaban presentes en IPv4. Dichas preocupaciones emanan de la manera exclusiva con la que el protocolo realiza la detección de routers y vecinos, la asignación de direcciones y la resolución de direcciones mediante el protocolo de detección de vecinos (NDP). Estos mecanismos podrían permitir que un atacante implemente ataques como interceptación de tráfico, DoS o por intermediario.

- **Creación de perfiles de dispositivos:** las tendencias como BYOD requieren que los clientes tengan visibilidad de los diversos tipos de dispositivos que acceden a la red y sean capaces de administrar el control de acceso, las políticas de segmentación y las políticas QoS basadas en el tipo de dispositivo conectado. Los switches Cisco Catalyst tienen funcionalidades integradas de creación de perfiles de dispositivos para identificar el tipo de dispositivo conectado y aplicar políticas basadas en el tipo de dispositivo.
- **Redes basadas en identidades:** Cisco admite una amplia gama de opciones de autenticación, que incluyen 802.1x para dispositivos y usuarios administrados, autenticación web para usuarios temporales o usuarios no 802.1x, y omisión de autenticación MAC para dispositivos no administrados o no 802.1x. Se pueden configurar el orden y la prioridad de los métodos de autenticación, junto con el comportamiento después de los errores de servidor 802.1x o AAA.
- **Cisco TrustSec:** Cisco TrustSec® permite definiciones de políticas basadas en roles en un motor de políticas centralizado (ISE) y la aplicación distribuida de dichas políticas en la infraestructura de red independiente de la arquitectura de la red. Esto proporciona la capacidad de definir políticas granulares basadas en rol de usuario, dispositivo, ubicación, estado, etc., mientras hace que la definición de políticas y la administración de cambios sea eficiente desde el punto de vista operativo.
- Funcionalidad de hardware para cifrar el tráfico mediante MACsec* basado en 802.1AE (hardware compatible en el primer envío a clientes [FCS], soporte de software en plan).

Ahora analizaremos las descripciones detalladas de cada una de estas categorías de funciones.

Seguridad de primer salto en IPv4

La seguridad de primer salto en IPv4, también conocida como CISF, ofrece herramientas poderosas y fáciles de usar para impedir con eficacia las amenazas de seguridad de capa 2 más frecuentes y potencialmente peligrosas. CISF incluye lo siguiente:

- **Seguridad de puerto:** impide los ataques de desbordamiento de direcciones MAC ya que limita las direcciones MAC de las estaciones que tienen permitido acceder al mismo puerto físico. La seguridad de puerto limita la cantidad de direcciones MAC conocidas para denegar el desbordamiento de direcciones MAC.
- **Snooping DHCP:** impide la falsificación del servidor DHCP y los ataques por intermediario con el switch de acceso actuando como un pequeño firewall de seguridad entre los usuarios y el servidor DHCP legítimo. Los atacantes de la red ya no pueden asignarse como como gateway predeterminado ni redistribuir o supervisar el flujo de tráfico entre los dos terminales.
- **Inspección ARP dinámica:** impide la suplantación de identidad ARP ya que permite garantizar que el switch de acceso transmita solamente solicitudes y respuestas ARP “válidas”. Esta funcionalidad impide que hosts maliciosos intercepten (sin ser detectados) la conversación entre los dos terminales para recoger contraseñas o datos o para escuchar conversaciones telefónicas por IP.
- **Protección de IP de origen:** impide la falsificación de hosts IP de atacantes y gusanos de Internet suponiendo una dirección IP de usuario válido. La protección de IP de origen permite reenviar solamente paquetes con direcciones de origen válidas.

Seguridad de primer salto en IPv6

La seguridad se ha convertido en uno de los temas más frecuentes de los debates sobre IPv6. La seguridad de primer salto en IPv6 es un conjunto de características diseñadas específicamente para proteger la operación de enlaces IPv6, además de ayudar con la escalablilidad en grandes dominios de capa 2. El primer salto de un host final suele ser un switch de capa 2. El switch de primer salto se encuentra ubicado estratégicamente para para tener información de todos sus vecinos; por tanto, el switch puede permitir o denegar con facilidad ciertos tipos de tráfico, roles de nodo final y notificaciones. Inspeccionará el tráfico de detección de vecinos y proporcionará información sobre enlaces de capa 2/capa 3, además de supervisar el uso de la detección de vecinos por el host para identificar comportamientos potencialmente anormales. En última instancia, el switch puede bloquear el tráfico no deseado, como un anuncio de router dudoso, un anuncio de servidor DHCP dudoso y tráfico de datos provenientes de direcciones IP o prefijos no deseados.

Las características básicas de IPv6FHS disponibles en los switches Cisco Catalyst de la serie 2960-X/XR son:

- **Protección RA:** bloquea los anuncios de router (RA) no autorizados.
- **Protección DHCP:** bloquea los servidores DHCP no autorizados.
- **Snooping IPv6:** analiza el tráfico de switches de control/datos, detecta direcciones IP y las almacena/actualiza en una tabla de enlaces.

Creación de perfiles de dispositivos

Los switches Cisco Catalyst 2960-X y 2960-XR admiten la funcionalidad de sensor de dispositivos integrada en el software Cisco IOS. El sensor de dispositivos captura los paquetes de protocolo, como Cisco Discovery Protocol, LLDP (protocolo de detección de capa de enlace), DHCP, H.323 y mDNS (DNS de multidifusión), además de información MAC OUI (identificador único organizacional) de los hosts y clasifica el dispositivo en función de una base de datos de dispositivos que está integrada en el software Cisco IOS. La funcionalidad del sensor de dispositivos también se admite junto con Cisco Identity Service Engine (ISE). En esta característica, el switch crea perfiles del host final mediante la captura de la información del protocolo y el envío de la información de atributos del protocolo a ISE mediante RADIUS. Esto permite que los dispositivos se clasifiquen y se supervisen en forma central en ISE de una manera escalable. Las políticas de autorización como la asignación VLAN (LAN virtual) o las listas de control de acceso descargables (dACL) basadas en el tipo de dispositivo se pueden definir en ISE. Además, las macros AutoSmartPort para configurar ajustes adicionales en el puerto se pueden activar en función del tipo de dispositivo determinado a través del sensor de dispositivos. Estas macros AutoSmartPort también pueden transferirse al puerto de switch desde ISE.

Redes basadas en identidades

Cisco Identity-Based Networking Services (IBNS) permite la aplicación de políticas empresariales de todos los usuarios y hosts, ya sean administrados o no administrados. La solución promueve la autenticación para acceder a la red; esta autenticación también sirve como la base para diferenciar usuarios y/o hosts, lo que proporciona diversos niveles de acceso a recursos en la red basados en la política de acceso corporativa. Cisco IBNS en switches Cisco Catalyst proporciona un conjunto completo de características de 802.1X y funcionalidad asociada, diseñada para reducir la sobrecarga operativa en relación con la implementación de IEEE 802.1X, al tiempo que proporciona la flexibilidad para implementar las políticas de autenticación y autorización requeridas para mantener el acceso seguro. Estas nuevas funciones incluyen:

- Autenticación flexible compatible con diversos mecanismos de autenticación, como 802.1X, omisión de autenticación MAC y autenticación web, controlados mediante una única configuración uniforme.
- Funcionalidades de acceso de usuarios temporales integradas con Cisco ISE.

- Modo abierto, que permite un entorno intuitivo para realizar operaciones 802.1X.
- Integración de tecnología de creación de perfiles de dispositivos y gestión de acceso de usuarios temporales con switching de Cisco, para aumentar considerablemente la seguridad y, a la vez, reducir los desafíos de implementación y funcionamiento.
- Funcionalidades integrales de administración de políticas, como cambio de autorización RADIUS y dACL.
- Funcionalidades integrales de solución de problemas, supervisión e informes del sistema.

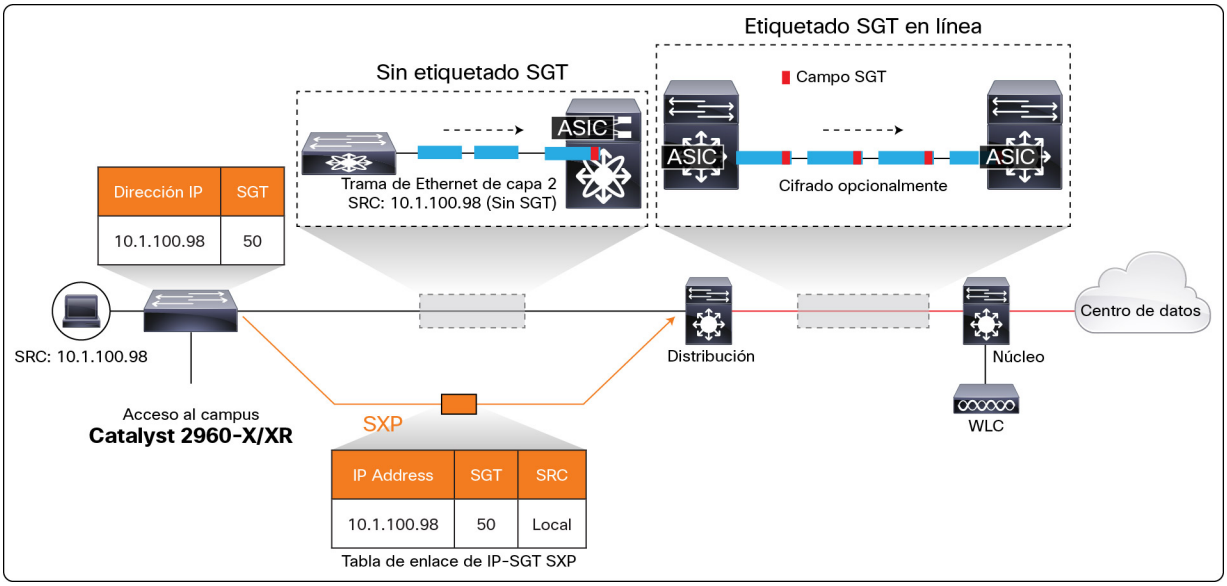
Cisco TrustSec

Cisco TrustSec simplifica la seguridad de la red mediante la definición de permisos de control de acceso y seguridad en términos de roles o “etiquetas de grupos de seguridad” en lugar de listas de control de acceso basadas en IP. El tráfico del host final se etiqueta con la información de identidad del host final mediante una etiqueta de grupo de seguridad (SGT). A medida que el tráfico fluye a través de la red, el contexto de identidad del tráfico se transfiere a toda la red a través de la etiqueta SGT, y se pueden aplicar permisos de seguridad adecuados al tráfico en función de la etiqueta SGT. Estas políticas, denominadas listas de control de acceso de grupo de seguridad (SGACL), están basadas en información de identidad del tráfico derivada de la etiqueta SGT.

Los switches Cisco Catalyst 2960-X y 2960-XR actualmente no admiten paquetes de etiquetado con SGT. Mediante el uso del protocolo de intercambio SGT (SXP), los switches Cisco Catalyst 2960-X y 2960-XR pueden pasar asignaciones de dirección-IP-a-SGT a un dispositivo del mismo nivel de Cisco TrustSec que tiene hardware compatible con Cisco TrustSec.

Los switches Cisco Catalyst 2960-X y 2960-XR en la capa de acceso realizan la autenticación basada en 802.1X/MAB/web del host final para determinar las SGT adecuadas para los paquetes de ingreso. El switch de capa de acceso aprende las direcciones IP de los dispositivos de origen mediante el seguimiento de dispositivos IP y (opcionalmente) snooping DHCP; a continuación, usa SXP para pasar las direcciones IP de los dispositivos de origen junto con sus SGT a los switches de distribución. Los switches de distribución con hardware compatible con Cisco TrustSec pueden usar esta información de asignación IP-a-SGT para etiquetar paquetes en forma adecuada y aplicar las políticas SGACL (ver Figura 1).

Figure 1. Protocolo SXP para propagar información de SGT



Para más información

Seguridad de primer salto en IPv4
http://www.cisco.com/web/strategy/docs/gov/turniton_cisf.pdf

Seguridad de primer salto en IPv6
http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-602135.html
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html

Sensor de dispositivos
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-1sg/sec-dev-sensor.html

AutoSmartPorts
http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/15.0_1_se/configuration/guide/asp_cg.html

Redes basadas en identidades
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html
http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-overview.html

Cisco TrustSec
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: **www.cisco.com/go/offices**.

Impreso en EE. UU. C11-728742-00 06/13