Secure Unified Access with Cisco Catalyst 2960-X and 2960-XR Series Switches

Overview

The Cisco® Catalyst® 2960-X and 2960-XR Series Switches are the industry's leading access switching platforms, enabling increased business productivity and agility with features designed to address enterprise networking megatrends such as IPv6 transition, Bring Your Own Device (BYOD), and Mobility. The Cisco Catalyst 2960-X and 2960-XR provide security features to enable these transitions in the network in a secure and efficient manner.

Cisco Catalyst 2960-X and 2960-XR switches provide a rich and comprehensive set of security features designed to:

- Secure the network from traffic interception, spoofing, and DoS attacks
- Control access to resources in your network with access control lists (ACLs), including ACLs based on user/device type
- Secure network access based on user identity and user role
- Provision device-based policies through device profiling
- Protect confidentiality and Integrity of network traffic through encryption* (hardware capability)
- Securely boot digitally signed Cisco IOS® Software images

As a part of Cisco's Unified Access architecture, the Cisco Catalyst 2960-X and 2960-XR switches represent a network infrastructure that is capable of distributed policy classification and enforcement at the access layer, with the policy definitions from Cisco's One Policy platform, the Cisco Identity Services Engine (ISE).

The Cisco Catalyst 2960-X and 2960-XR help secure networks and provide secure access through the following primary feature categories:

- **IPv4 First Hop Security (FHS):** Cisco Catalyst switches offer Cisco Integrated Security Features(CISF), an industry-leading solution that provides superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and Address Resolution Protocol [ARP] spoofing). Delivering powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats, CISF provides robust security throughout the network.
- **IPv6 First Hop Security:** IPv6 raises a number of FHS concerns that were not present in IPv4. Those concerns stem from the protocol's unique manner in which it performs router and neighbor discovery, address assignment, and address resolution using Neighbor Discovery Protocol (NDP). These mechanisms could allow an attacker to deploy attacks such as traffic interception, DoS, or man-in-the-middle.
- **Device profiling:** Trends such as BYOD require customers to have visibility into the various types of devices accessing the network and being able to administer access control, segmentation policies, and QoS policies based on the type of device connected. Cisco Catalyst switches have built-in device profiling capabilities to identify the type of device connected and apply policies based on device type.

- **Identity-based networking:** Cisco supports a wide range of authentication options, including 802.1x for managed devices and users, web authentication for guests or non-802.1x users, and MAC authentication bypass for unmanaged or non-802.1x devices. The order and priority of authentication methods can be configured, along with behavior after 802.1x or AAA server failures.
- **Cisco TrustSec:** Cisco TrustSec® enables role-based policy definitions in a centralized policy engine (ISE) and the distributed enforcement of those policies in the network infrastructure independent of network architecture. This provides for ability to define granular policies based on user role, device, location, posture, and so on while making policy definition and change management operationally efficient.
- Hardware capability to encrypt traffic using 802.1AE-based MACsec* (hardware capable at FCS, software support on roadmap).

We will now take a look at the detailed descriptions of each one of these categories of features.

IPv4 First Hop Security

IPv4 First Hop Security, also known as CISF, delivers powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats. CISF includes the following:

- **Port Security:** Prevents MAC address-flooding attacks by limiting the MAC addresses of stations allowed access to the same physical port. Port Security limits the number of learned MAC addresses to deny MAC address flooding.
- **DHCP Snooping:** Prevents DHCP server spoofing and “man-in-the-middle” attacks with the access switch acting much like a small security firewall between users and the legitimate DHCP server. Network attackers can no longer assign themselves as the default gateway or reroute and monitor traffic flow between the two endpoints.
- **Dynamic ARP Inspection:** Prevents ARP spoofing by helping ensure that the access switch relays only “valid” ARP requests and responses. This capability prevents malicious hosts from invisibly eavesdropping on the conversation between the two endpoints to glean passwords or data or to listen to IP phone conversations.
- **IP Source Guard:** Prevents IP host spoofing from attackers and Internet worms assuming a valid user’s IP address. IP Source Guard permits forwarding of only packets with valid source addresses.

IPv6 First Hop Security

Security has become one of the most popular subjects of IPv6 discussions. IPv6 First Hop Security is a suite of features designed specifically to harden IPv6 link operation, as well as help with scale in large L2 domains. The first hop for an end host is very often a Layer 2 switch. The first hop switch is strategically located to learn about all its neighbors, and hence the switch can easily either allow or deny certain types of traffic, end-node roles, and claims. It will inspect the Neighbor Discovery traffic and provide information about Layer 2/Layer 3 binding and monitor the use of Neighbor Discovery by host to spot potentially abnormal behaviors. Ultimately, the switch can block undesired traffic such as rogue Router Advertisement, rogue DHCP server advertisement, and data traffic coming from undesired IP addresses or prefixes.

The core IPv6FHS features available on Cisco Catalyst 2960-X/XR series switches are:

- **RA Guard:** Blocks unauthorized Router Advertisements.
- **DHCP Guard:** Blocks unauthorized DHCP servers.
- **IPv6 Snooping:** Analyzes control/data switch traffic, detects IP address, and stores/updates them in a binding table.

Device Profiling

Cisco Catalyst 2960-X and 2960-XR switches support Device Sensor functionality built into Cisco IOS Software. Device Sensor captures protocol packets such as Cisco Discovery Protocol, LLDP, DHCP, H.323, and mDNS as well as MAC OUI information from the end hosts and classifies the device based on a device database that is built into Cisco IOS Software. Device Sensor functionality is also supported in conjunction with the Cisco Identity Service Engine (ISE).In this feature the switch profiles the end host by capturing the protocol information and sending the protocol attribute information to ISE using RADIUS. This enables devices to be centrally classified and monitored in ISE in a scalable manner. Authorization policies such as VLAN assignment or dACLs based on device type can be defined in ISE. Also, AutoSmartPort macros to configure additional configurations to the port can be triggered based on the device type determined via Device Sensor. These AutoSmartPort macros can also be pushed to the switch port from ISE.

Identity-Based Networking

Cisco Identity-Based Networking Services (IBNS) enable enterprise policy enforcement of all users and hosts, whether managed or unmanaged. The solution promotes authentication to access the network; this authentication also serves as the basis for differentiating users and/or hosts, providing varying levels of access to networked resources based on corporate access policy. Cisco IBNS on Cisco Catalyst switches provides a very rich feature set of 802.1X and associated functionality designed to reduce the operational overhead associated with deploying IEEE 802.1X, while providing the flexibility to implement to authentication and authorization policies required to maintain secure access. These new capabilities include:

- Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC authentication bypass, and web authentication, using a single, consistent configuration
- Guest Access capabilities integrated with Cisco ISE
- Open mode that enables a user-friendly environment for 802.1X operations
- Integration of device-profiling technology and guest access handling with Cisco switching to significantly improve security while reducing deployment and operational challenges
- Comprehensive policy management capabilities such as RADIUS Change of Authorization and downloadable access control lists (ACLs)
- End-to-end system troubleshooting, monitoring, and reporting capabilities

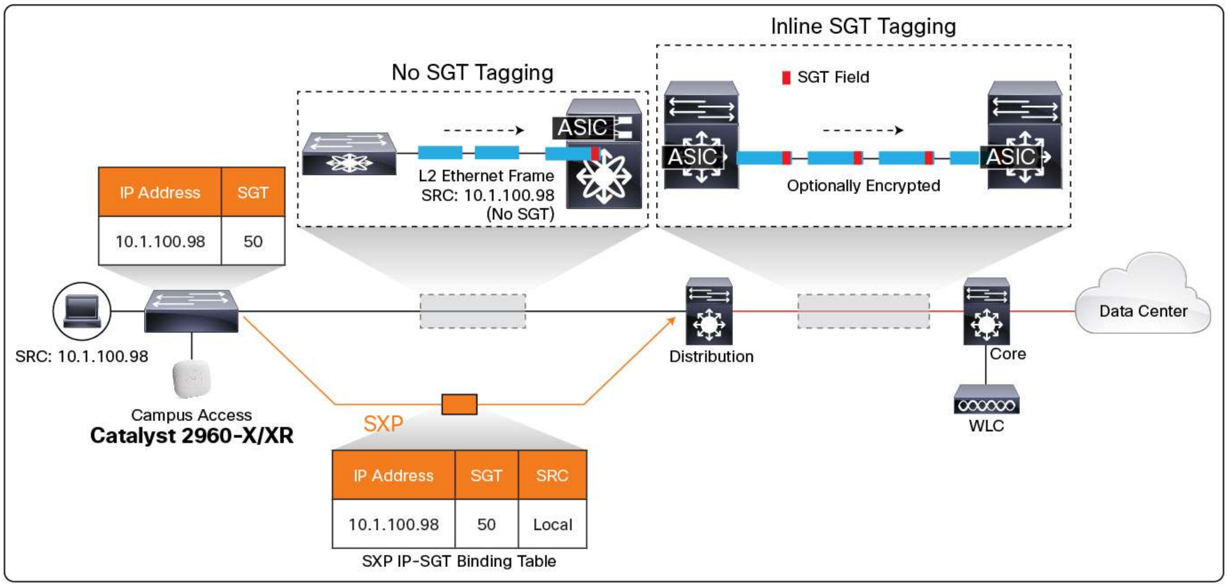
Cisco TrustSec

Cisco TrustSec simplifies network security by defining security and access control permissions in terms of roles or “security group tags” rather than IP-based access control lists. The traffic from the end host is tagged with the identity information of the end host via a Security Group Tag (SGT). As the traffic flows through the network, the identity context of the traffic is carried throughout the network via the SGT tag, and appropriate security permissions can be applied to the traffic based on the SGT tag. These policies, called Security Group Access Control Lists (SGACLs), are based on identity information of the traffic derived from the SGT tag.

The Cisco Catalyst 2960-X and 2960-XR currently do not support tagging packets with SGT. By using the SGT Exchange Protocol (SXP), Cisco Catalyst 2960-X and 2960-XR switches can pass IP-address-to-SGT mappings to a Cisco TrustSec peer device that has hardware capable of using Cisco TrustSec.

The Cisco Catalyst 2960-X and 2960-XR in the access layer perform802.1X/MAB/web-based authentication of the end host to determine the appropriate SGTs for ingress packets. The access layer switch learns the IP addresses of the source devices using IP device tracking and (optionally) DHCP snooping, then uses SXP to pass the IP addresses of the source devices along with their SGTs to the distribution switches. Distribution switches with hardware capable of using Cisco TrustSec can use this IP-to-SGT mapping information to tag packets appropriately and to enforce SGACL policies (see Figure 1).

Figure 1. SXP Protocol to Propagate SGT Information



IP Address	SGT
10.1.100.98	50

IP Address	SGT	SRC
10.1.100.98	50	Local

For More Information

IPv4 First Hop Security

http://www.cisco.com/web/strategy/docs/gov/turniton_cisf.pdf

IPv6 First Hop Security

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

Device Sensor

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

Identity-Based Networking

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-728742-00 06/13