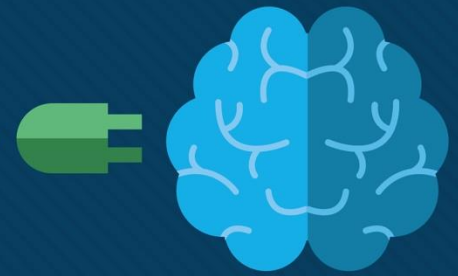

Chapter 25: Secure Network Access Control

Instructor Materials

CCNP Enterprise: Core Networking

Chapter 25 Content

This chapter covers the following content:

- **Network Security Design for Threat Defense -** This section describes a Cisco security framework to protect networks from evolving cybersecurity threats.
- **Next-Generation Endpoint Security -** This section describes security components such as next-generation firewalls, Web Security Appliance (WSA), and Email Security Appliance (ESA) that are part of the Cisco security framework to protect endpoints from threats and attacks.
- **Network Access Control (NAC) -**This section describes technologies such as 802.1x, Web Authentication (WebAuth), MAC Authentication Bypass (MAB), TrustSec and MACsec to enforce network access control.

Network Security Design for Threat Defense

- Endpoints are extremely vulnerable to security threats, and they can become infected. A solid network security design protects the endpoints from these types of security threats and enforces endpoint network access.
- This chapter describes the components of network security design for a campus environment that are used to protect, detect, and remediate security threats and attacks.

Cisco SAFE

To address the evolving cybersecurity threats, Cisco created Cisco SAFE, a security architectural framework that helps design secure solutions for the following places in the network (PINs):

- Branch
- Campus
- Data Center
- Edge
- Cloud
- Wide Area Network (WAN)

Cisco SAFE focuses on the integration of security services within each of the PINs. For information on the underlying networking design and infrastructure see the Cisco Validated Design (CVD) guides, which provide detailed networking design and implementation guidance. CVDs can be found at www.cisco.com/go/cvd.

Cisco SAFE Domains

Cisco SAFE also defines secure domains, which are operational areas used to protect the different PINs. The following security concepts are used to evaluate each PIN:

- Management
- Security Intelligence
- Compliance
- Segmentation
- Threat Defense
- Secure Services

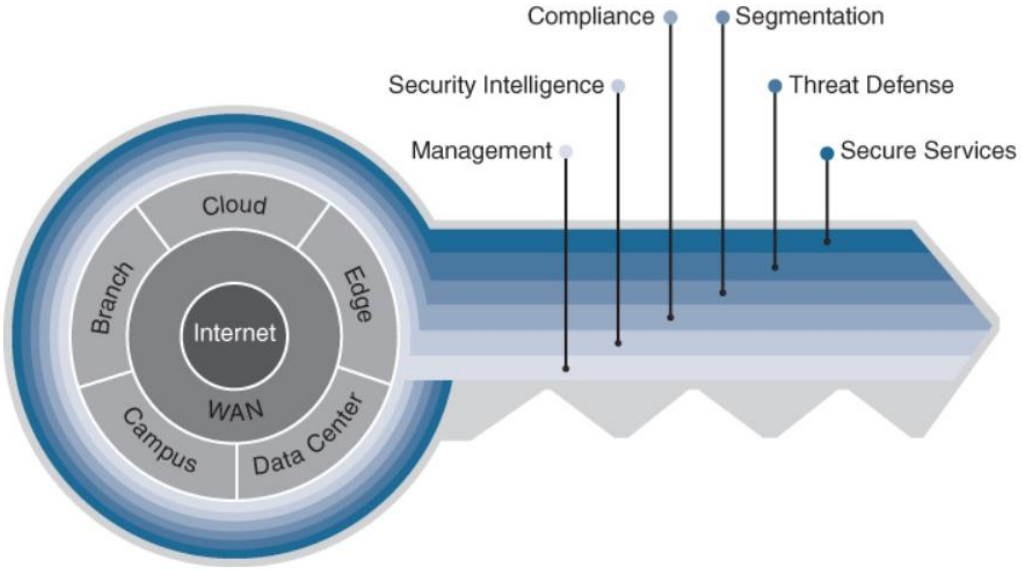

Figure 25-1 *The Key to Cisco SAFE*

Cisco SAFE Implementation

Implementing the Cisco SAFE framework in an organization provides advanced threat defense protection that spans the full attack continuum before, during, and after an attack for all the PINs:

- Before
- During
- After

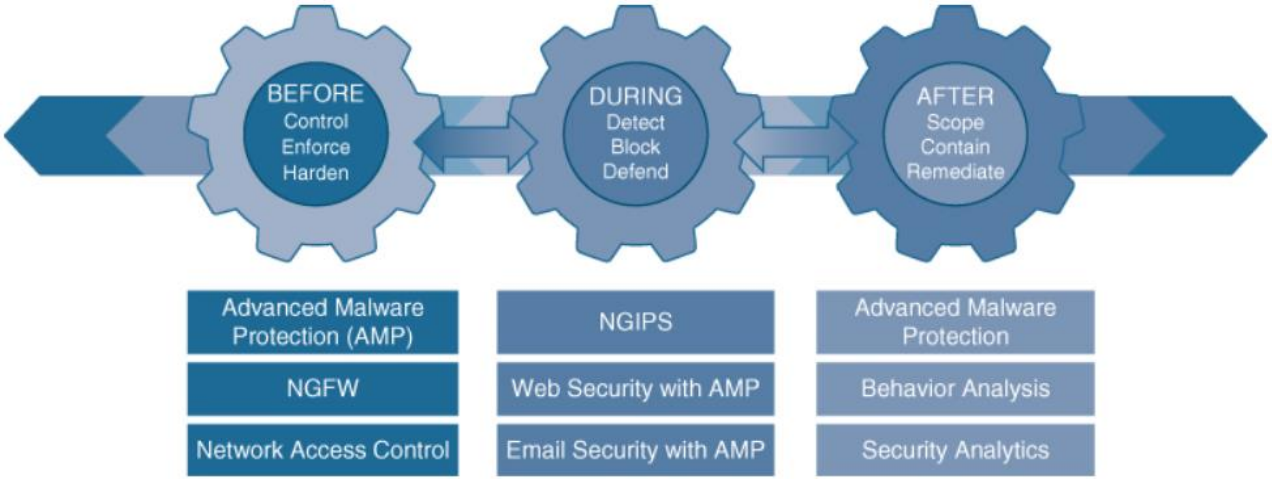

Figure 25-2 *Cisco Products and Solutions Across the Attack Continuum*

Next-Generation Endpoint Security

- To be able to detect the rapidly evolving threats, organizations should design their networks using a security framework such as that provided by Cisco SAFE.
- The following sections describe the most critical components needed to implement the Cisco SAFE framework for a campus environment (or *PIN*, in Cisco SAFE terminology).

Cisco Talos

Talos is the Cisco threat intelligence organization, an elite team of security experts who are supported by sophisticated security systems to create threat intelligence that detects, analyzes, and protects against both known and emerging threats for Cisco products.

Cisco Talos was created from the combination of three security research teams:

- IronPort Security Applications (SecApps)
- The Sourcefire Vulnerability Research Team (VRT)
- The Cisco Threat Research, Analysis, and Communications (TRAC) team

Talos receives valuable intelligence that no other cybersecurity research team can match through the following intelligence feeds:

- Advanced Microsoft and industry disclosures The Advanced Malware Protection (AMP) community
- ClamAV, Snort, Immunet, SpamCop, SenderBase, Threat Grid, and Talos user communities
- Honeypots
- The Sourcefire Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) program
- Private and public threat feeds
- Dynamic analysis

Cisco Threat Grid

Cisco Threat Grid is a solution that can perform static file analysis, as well as dynamic file analysis (also known as behavioral analysis), by running the files in a controlled and monitored sandbox environment.

- Behavioral analysis is combined with threat intelligence feeds from Talos, as well as with existing security technologies to protect against known and unknown attacks.
- It is also possible to upload suspicious files into a sandbox environment called Glovebox to safely interact with them and observe malware behavior directly.
- Threat Grid is available as an appliance and in the cloud, and it is also integrated into existing Cisco security products and third-party solutions.

Automatic submission of suspicious files and samples is available for products and solutions integrated with Threat Grid. When automatic submission is not available, files can also be uploaded manually into Threat Grid for analysis.

Cisco Advanced Malware Protection (AMP)

Cisco Advanced Malware Protection (AMP) (formerly FireAMP) is a malware analysis and protection solution that goes beyond point-in-time detection.

Cisco AMP provides comprehensive protection for organizations across the full attack continuum:

Attack Time	AMP Processes
Before	Global threat intelligence from Cisco Talos and Cisco Threat Grid feeds into AMP to protect against known and new emerging threats.
During	File reputation to determine whether a file is clean or malicious as well as sandboxing are used to identify threats during an attack.
After	Cisco AMP provides retrospection, indicators of compromise (IoCs), breach detection, tracking, analysis, and surgical remediation after an attack, when advanced malware has slipped past other defenses.

Cisco AMP Components

The architecture of AMP can be broken down into the following components:

- AMP Cloud (private or public)

- AMP connectors
  - AMP for Endpoints (Microsoft Windows, macOS X, Google Android, Apple iOS, and Linux)
  - AMP for Networks (NGFW, NGIPS, ISRs)
  - AMP for Email (ESA)
  - AMP for Web (WSA)
  - AMP for Meraki MX

- Threat intelligence from Cisco Talos and Cisco Threat Grid

Cisco AMP for Endpoints on Apple iOS is known as the Cisco Security Connector (CSC). The CSC incorporates AMP for Endpoints and Cisco Umbrella.

Cisco AMP Components (Cont.)

Figure 25-3 illustrates how all the AMP components come together to form the AMP architecture.

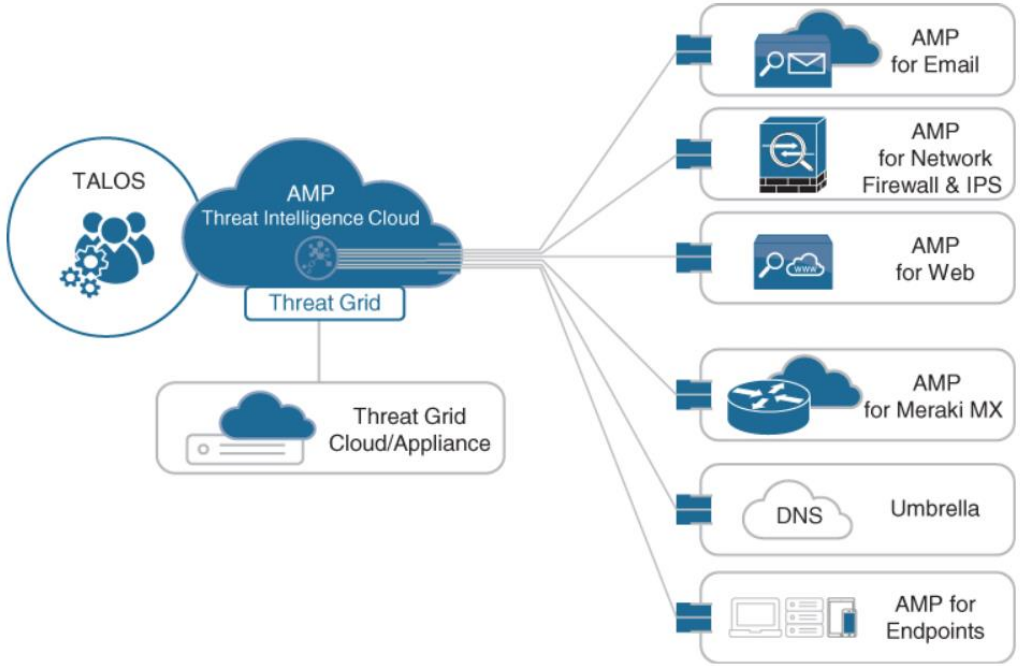

Figure 25-3 *AMP Components*

Cisco AnyConnect

Cisco AnyConnect Secure Mobility Client is a modular endpoint software product that is not only a VPN client that provides VPN access through Transport Layer Security (TLS)/Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules, such as a VPN Posture (HostScan) module and an ISE Posture module.

Cisco AnyConnect also includes web security through Cisco Cloud Web Security, network visibility into endpoint flows within Stealthwatch, and roaming protection with Cisco Umbrella.

AnyConnect is supported across the following platforms:
Windows, macOS, iOS, Linux, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.

TLS/SSL is often used to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so TLS/SSL can be interpreted as referring to TLS only.

Cisco Umbrella

Cisco Umbrella (formerly known as OpenDNS) provides the first line of defense against threats on the internet by blocking requests to malicious internet destinations (domains, IPs, URLs) using the Domain Name System (DNS) before an IP connection is established or a file is downloaded.

- It is 100% cloud delivered, with no hardware to install or software to maintain.
- The Umbrella global network includes 30 data centers around the world using Anycast DNS, which allows it to guarantee 100% uptime.

Figure 25-4 *Cisco Umbrella Blocking Phishing Website*

Cisco Web Security Appliance (WSA)

The Cisco Web Security Appliance (WSA) is an all-in-one web gateway that includes a wide variety of protections that can block hidden malware from both suspicious and legitimate websites.

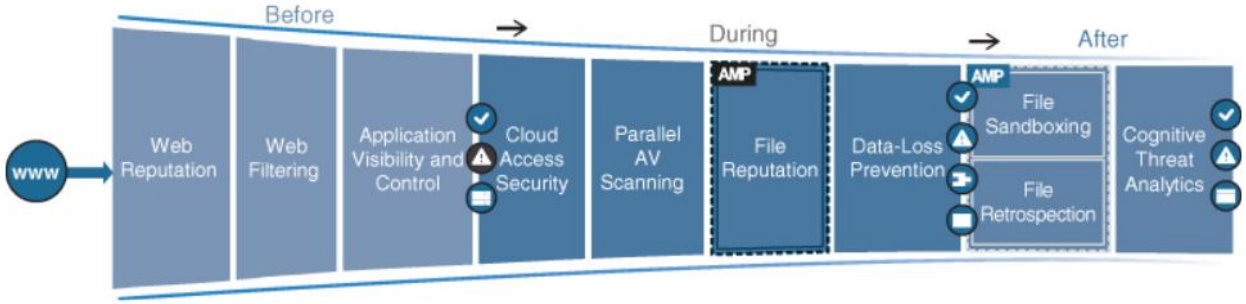

Figure 25-5 *WSA Capabilities Across the Attack Continuum*

Before	During	After
• Web reputation filters • Web filtering • Cisco Application Visibility and Control (AVC)	• Cloud access security • Parallel antivirus (AV) scanning • Layer 4 traffic monitoring • File reputation and analysis with Cisco AMP • Data loss prevention (DLP)	• Continuously inspects for instances of undetected malware and breaches. • Global Threat Analytics (GTA)

Before an Attack

Before an attack, the WSA actively detects and blocks potential threats before they happen by applying web reputation filters and URL filtering and by controlling web application usage:

Terms	Description
Web reputation filters	Cisco WSA detects and correlates threats in real time using Talos. Web reputation filtering prevents client devices from accessing dangerous websites containing malware or phishing links.
Web filtering	Traditional URL filtering is combined with real-time dynamic content analysis. This is used to shut down access to websites known to host malware.
Cisco Application Visibility and Control (AVC)	Cisco AVC identifies and classifies the most relevant and widely used web and mobile applications and more than 150,000 micro-applications.

During an Attack

During an attack, the WSA uses security intelligence from cloud access security broker (CASB) providers, Talos, and AMP for networks to identify and block zero-day threats that managed to infiltrate the network:

Terms	Description
Cloud access security	WSA can protect against hidden threats in cloud apps
Parallel antivirus (AV) scanning	WSA enhances malware defense coverage with multiple anti-malware scanning engines
Layer 4 traffic monitoring	WSA scans all traffic, ports, and protocols to detect and block spyware “phone-home” communications
File reputation and analysis with Cisco AMP	WSA assesses files using the latest threat information from Cisco Talos
Data loss prevention (DLP)	WSA uses Internet Control Adaptation Protocol (ICAP) to integrate with DLP solutions from leading third-party DLP vendors

After an Attack

After an attack, Cisco WSA inspects the network continuously for instances of undetected malware and breaches.

- After an initial detection, using Cisco AMP retrospection capabilities, Cisco WSA continues to scan files over an extended period of time, using the latest threat intelligence from Talos and AMP Thread Grid.

- Alerts are sent when a file disposition changes to provide awareness and visibility into malware that evades initial defenses.

Global Threat Analytics (GTA), formerly Cognitive Threat Analytics (CTA), analyzes web traffic, endpoint data from Cisco AMP for Endpoints, and network data from Cisco Stealthwatch Enterprise. It then identifies malicious activity before it can exfiltrate sensitive data.

WSA can be deployed in the cloud, as a virtual appliance, on-premises, or in a hybrid arrangement. All features are available across any deployment option.

Cisco Email Security Appliance (ESA)

The Cisco Email Security Appliance (ESA) enables users to communicate securely via email and helps organizations combat email security threats with a multilayered approach.

Cisco ESA includes the following advanced threat protection capabilities that allow it to detect, block, and remediate threats across the attack continuum:

- **Global threat intelligence -** It leverages real-time threat intelligence from Talos and AMP.
- **Reputation filtering -** ESA blocks unwanted email with reputation filtering.
- **Spam protection -** ESA uses the Cisco Context Adaptive Scanning Engine (CASE) to block spam emails.
- **Forged email detection -** Forged email detection protects high-value targets such as executives against business email compromise (BEC) attacks.

Cisco Email Security Appliance (ESA) (Cont.)

- **Cisco Advanced Phishing Protection (CAPP) -** CAPP combines Cisco Talos with local email intelligence and advanced machine learning techniques to model trusted email behaviors.

- **Cisco Domain Protection (CDP) -** CDP for external email helps prevent phishing emails from being sent using a customer domains.

- **Malware defense -** ESA protects against malware with Cisco AMP for email.

- **Graymail detection and Safe Unsubscribe -** ESA detects and classifies graymail for an administrator to take action on it if necessary. Graymail consists of marketing, social networking, and bulk messages (that is, mailing list emails).

- **URL-related protection and control -** ESA protects against malicious URLs with URL filtering and scanning of URLs in attachments and shortened URLs.

Cisco Email Security Appliance (ESA) (Cont.)

- **Outbreak filters -** Outbreak filters defend against emerging threats and blended attacks by leveraging Cisco Talos.

- **Web interaction tracking -** ESA generates reports that track the end users who click on URLs that have been rewritten by the outbreak filters. The reports include the following information:
  - Top users who clicked on malicious URLs
  - The top malicious URLs clicked by end users
  - Date and time, rewrite reason, and action taken on the URLs

- **Data security for sensitive content in outgoing emails -** Confidential outbound messages that match one of the more than 100 expert policies included with ESA are automatically protected.

Next-Generation Intrusion Prevention System (NGIPS)

A system that passively monitors and analyzes network traffic for potential network intrusion attacks and logs the intrusion attack data for security analysis is known as an intrusion detection system (IDS). A system that provides IDS functions and also automatically blocks intrusion attacks is known as an intrusion prevention system (IPS).

A next-generation IPS (NGIPS) should include IPS functionality as well as the following capabilities:

- Real-time contextual awareness
- Advanced threat protection
- Intelligent security automation
- Unparalleled performance and scalability
- Application visibility and control (AVC) and URL filtering

Next-Generation Intrusion Prevention System (Cont.)

With the acquisition of Sourcefire in 2013, Cisco added the Firepower NGIPS to its portfolio. Following are some of the most important capabilities included with the Cisco Firepower NGIPS:

Features	Advanced Features
Real-time contextual awareness	Centralized management
Advanced threat protection and remediation	Global threat intelligence from the Cisco Talos
Intelligent security automation	Snort IPS detection engine
Unparalleled performance and scalability	High availability and clustering
AVC	Third-party and open-source ecosystem
URL filtering	Integration with Cisco ISE: Quarantine, Unquarantine, Shutdown

Next-Generation Firewall (NGFW)

A firewall is a network security device that monitors incoming and outgoing network traffic and allows or blocks traffic by performing simple packet filtering and stateful inspection based on ports and protocols.

A next-generation firewall (NGFW) can block threats such as advanced malware and application-layer attacks. A NGFW firewall must include:

- Standard firewall capabilities such as stateful inspection
- An integrated IPS
- Application-level inspection (to block malicious or risky apps)
- The ability to leverage external security intelligence to address evolving security threats

NGFW: Management Options

The following management options are available for NGFWs:

- For FTD or Firepower Services software:
  - Firepower Management Center (FMC)
  - Firepower Device Manager (FDM) for small appliances

- For ASA software:
  - The command-line interface (CLI)
  - Cisco Security Manager (CSM)
  - Adaptive Security Device Manager (ASDM)
  - Cisco Defense Orchestrator

FTD or Firepower Services software CLI configuration is not supported. CLI is only available for initial setup and troubleshooting purposes.

Cisco Firepower Management Center (FMC)

The Cisco FMC is a centralized management platform that aggregates and correlates threat events, contextual information, and network device performance data.

The FMC performs event and policy management for the following Firepower security solutions:

- Cisco Firepower NGFW and NGFWv
- Cisco Firepower NGIPS and NGIPSv
- Cisco Firepower Threat Defense for ISR
- Cisco ASA with Firepower Services
- Cisco Advanced Malware Protection (AMP)

Cisco Stealthwatch

Cisco Stealthwatch is a collector and aggregator of network telemetry data that performs network security analysis and monitoring to automatically detect threats that manage to infiltrate a network as well as the ones that originate from within a network.

There are currently two offerings available for Stealthwatch:

- Stealthwatch Enterprise
- Stealthwatch Cloud

Cisco Stealthwatch Enterprise

Stealthwatch Enterprise provides real-time visibility into activities occurring within the network.

- At the core of Stealthwatch Enterprise are the Flow Rate License, the Flow Collector, Management Console, and Flow Sensor. Optional but recommended components include the following:
  - Cisco Stealthwatch Threat Intelligence
  - Cisco Stealthwatch Endpoint
  - Cisco Stealthwatch Cloud

- Stealthwatch Enterprise offers the following benefits:
  - Real-time threat detection
  - Incident response and forensics
  - Network segmentation
  - Network performance and capacity planning
  - Ability to satisfy regulatory requirements

Cisco Stealthwatch Enterprise (Cont.)

Stealthwatch Enterprise requires the following components:

- **Flow Rate License -** The Flow Rate License is required for the collection, management, and analysis of flow telemetry data and aggregates flows at the Stealthwatch Management Console, as well as to define the volume of flows that can be collected
- **Flow Collector -** The Flow Collector collects and analyzes enterprise telemetry data and other types of flow data.
- **Stealthwatch Management Console (SMC) -** The SMC is the control center that aggregates, organizes, and presents analysis from up to 25 Flow Collectors, Cisco ISE, and other sources.

Optional Stealthwatch Enterprise components include the following:

- Flow Sensor
- UDP Director

Cisco Stealthwatch Cloud

Stealthwatch Cloud provides the visibility and continuous threat detection required to secure the on-premises, hybrid, and multicloud environments.

Cisco Stealthwatch Cloud consists of two primary offerings:

- **Public Cloud Monitoring -** Cisco Stealthwatch Cloud Public Cloud Monitoring provides visibility and threat detection in AWS, GCP, and Microsoft Azure cloud infrastructures. It is a SaaS-based solution that can be deployed easily and quickly.

- **Private Network Monitoring -** Cisco Stealthwatch Cloud Private Network Monitoring provides visibility and threat detection for the on-premises network, delivered from a cloud-based SaaS solution.

Stealthwatch Cloud consumes metadata only. The actual packet payloads are never retained or transferred outside the network.

Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is a security policy management platform that provides highly secure network access control (NAC) to users and devices across wired, wireless, and VPN connections.

Some of the most important features ISE include the following:

ISE Features	
Streamlined network visibility	Streamlined device onboarding
Cisco Digital Network Architecture (DNA) Center integration	Internal certificate authority
Centralized secure network access control	Device profiling:
Centralized device access control	Endpoint posture service
Cisco TrustSec	Active Directory support
Guest lifecycle management	Cisco Platform Exchange Grid (pxGrid)

Cisco Identity Services Engine (ISE) Example

Example 25-1 shows the type of contextual information Cisco ISE can share with devices integrated with it through pxGrid.

Example 25-1 *Contextual Information from Cisco ISE Session Directory*

```
Session={ip=[192.168.1.2]
Audit Session Id=0A0000010000000120001C0AC
UserName=dewey.hyde@corelab.com
ADUserDNSDomain=corelab.com
ADUserNetBIOSName=corelab,
ADUserResolvedIdentities=dewey.hyde@corelab.com
ADUserResolvedDNs=CN=Dewey Hyde
CN=Users
DC=corelab
DC=com
MacAddresses=[00:0C:C1:31:54:69]
State=STARTED
ANCstatus=ANC_Quarantine
SecurityGroup=Quarantined_Systems
EndpointProfile=VMWare-Device
EndpointProfile=VMWare-Device
NAS IP=192.168.1.1
NAS Port=GigabitEthernet0/0/1
RADIUSAVPairs=[ Acct-Session-Id=0000002F]
Posture Status=null
Posture Timestamp=
LastUpdateTime=Sat Aug 21 11:49:50 CST 2019
Session attributeName=Authorization_Profiles
Session attributeValue=Quarantined_Systems
Providers=[None]
EndpointCheckResult=none
IdentitySourceFirstPort=0
IdentitySourcePortStart=0
```

Network Access Control (NAC)

This section describes multiple network access control (NAC) technologies, such as 802.1x, MAC Authentication Bypass (MAB), and Web Authentication (WebAuth), as well as nextgeneration NAC technologies such as TrustSec and MACsec.

802.1x

IEEE 802.1x (referred to as Dot1x) is a standard for port-based network access control (PNAC) that provides an authentication mechanism for local area networks (LANs) and wireless local area networks (WLANs).

802.1x comprises the following components:

- **Extensible Authentication Protocol (EAP) -** This message format and framework defined by RFC provides an encapsulated transport for authentication parameters.
- **EAP method (also referred to as EAP type) -** Different authentication methods can be used with EAP.
- **EAP over LAN (EAPoL) -** This Layer 2 encapsulation protocol is defined by 802.1x for the transport of EAP messages over IEEE 802 wired and wireless networks.
- **RADIUS protocol -** This is the AAA protocol used by EAP.

802.1x Roles

802.1x network devices have the following roles:

- **Supplicant -** Software on the endpoint communicates and provides identity credentials through EAPoL with the authenticator.
- **Authenticator -** A network access device (NAD) such as a switch or wireless LAN controller (WLC) controls access to the network based on the authentication status of the user or endpoint.
- **Authentication server -** RADIUS server performs authentication of the client.

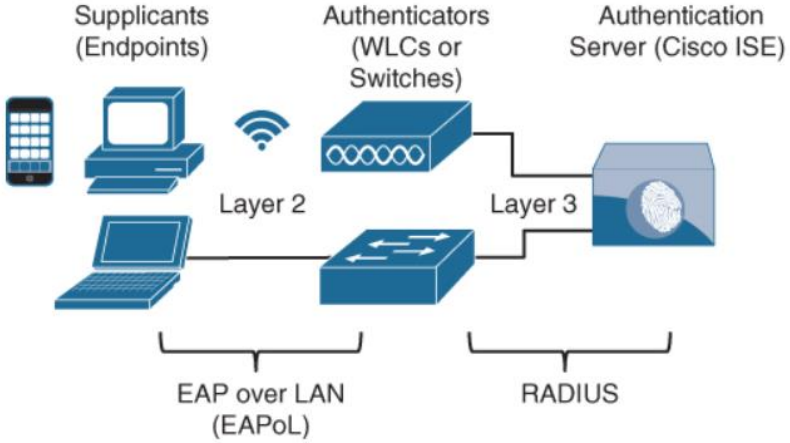

Figure 25-6 *802.1x Roles and Components*

802.1x Authentication

The EAP identity exchange and authentication occur between the supplicant and the authentication server.

Step 1. When the authenticator notices a port coming up, it starts the authentication process by sending periodic EAP-request/identify frames.

Step 2. The authenticator relays EAP messages between the supplicant and the authentication server.

Step 3. If authentication is successful, the authentication server returns a RADIUS access-accept message.

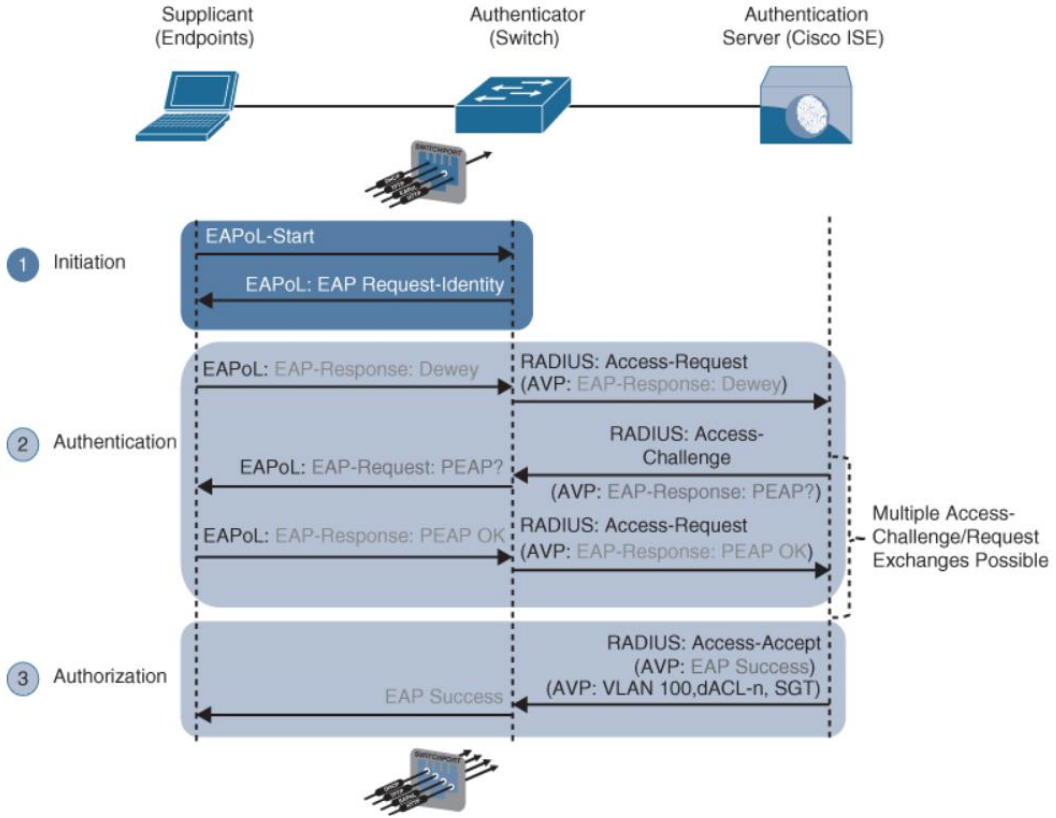

Figure 25-7 *Successful 802.1x Authentication Process Flow*

EAP Methods

There are many different EAP authentication methods available, most of them based on Transport Layer Security (TLS). The following are the most commonly used EAP methods, which are described in this section:

- EAP challenge-based authentication method
  - Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- EAP TLS authentication method
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- EAP tunneled TLS authentication methods
  - Extensible Authentication Protocol Flexible Authentication via Secure Tunneling (EAP-FAST)
  - Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLS)
  - Protected Extensible Authentication Protocol (PEAP)
- EAP inner authentication methods
  - EAP Generic Token Card (EAP-GTC)
  - EAP Microsoft Challenge Handshake Authentication Protocol Version 2 (EAP-MSCHAPv2)
  - EAP TLS.

EAP Methods (Cont.)

Following is a description of each of the EAP authentication methods:

- **EAP-MD5 –** This uses the MD5 message-digest algorithm to hide the credentials in a hash.
- **EAP-TLS –** This uses the TLS Public Key Infrastructure (PKI) certificate authentication mechanism to provide mutual authentication of supplicant to authentication server and authentication server to supplicant.
- **PEAP -** In PEAP, only the authentication server requires a certificate. PEAP forms an encrypted TLS tunnel between the supplicant and the authentication server

After the tunnel has been established, PEAP uses one of the following EAP authentication inner methods to authenticate the supplicant through the outer PEAP TLS tunnel:

PEAP Authentication		
EAP-MSCHAPv2 (PEAPv0)	**EAP-TLS**	**EAP-TTLS**
EAP-GTC (PEAPv1)	**EAP-FAST**	

EAP Chaining

EAP-FAST includes the option of EAP chaining:

- Supports machine and user authentication inside a single outer TLS tunnel
- Enables machine and user authentication to be combined into a single overall authentication result
- Allows the assignment of greater privileges or posture assessments to users who connect to the network using corporate managed devices

MAC Authentication Bypass (MAB)

MAC Authentication Bypass (MAB) is an access control technique that enables port-based access control using the MAC address of an endpoint.

Step 1. The switch initiates authentication by sending an EAPoL identity request message to the endpoint every 30 seconds by default.

Step 2. The switch begins MAB by opening the port to accept a single packet from which it will learn the source MAC address of the endpoint.

Step 3. The RADIUS server determines whether the device should be granted access to the network

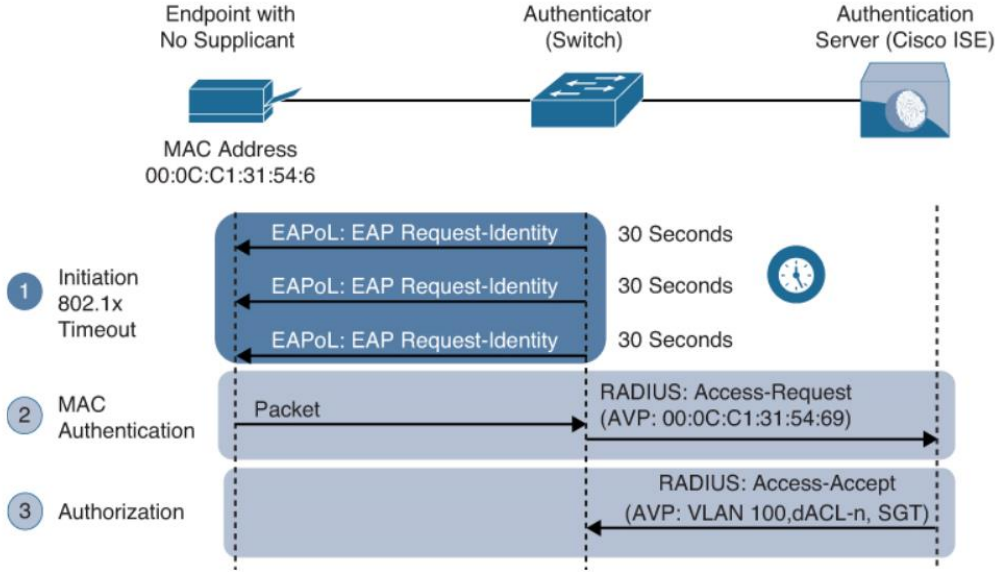

Figure 25-8 *Successful MAB Authentication Process Flow*

MAC Authentication Bypass (Cont.)

MAC addresses are easily spoofed. For this reason, MAB authenticated endpoints should be given very restricted access and should only be allowed to communicate to the networks and services that the endpoints are required to speak to.

If the authenticator is a Cisco switch, then many authorization options can be applied as part of the authorization result from the authentication server, including the following:

- Downloadable ACLs (dACLs)
- Dynamic VLAN assignment (dVLAN)
- Security Group Tags (SGT) tags

Web Authentication (WebAuth)

Web Authentication (WebAuth) can be used for endpoints that try to connect to the network might not have 802.1x supplicants and might not know the MAC address to perform MAB.

- WebAuth, like MAB, can be used as a fallback authentication mechanism for 802.1x.
- If both MAB and WebAuth are configured as fallbacks for 802.1x, when 802.1x times out a switch first attempts to authenticate through MAB, and if it fails, the switch attempts to authenticate with WebAuth.
- Unlike MAB, WebAuth is only for users and not devices since it requires a web browser and manual username and password entry.

There are two types of WebAuth:

- Local Web Authentication
- Centralized Web Authentication with Cisco ISE

Local Web Authentication

Local Web Authentication (LWA) is the first form of Web Authentication that was created.

The switch (or wireless controller) redirects web traffic (HTTP and/or HTTPS) to a locally hosted web portal running in the switch where an end user can enter a username and a password.

- When the switch sends the login credentials on behalf of the user, it is considered to be LWA.
- The LWA web portals are not customizable.
- With Cisco switches, there is no native support for advanced services such as acceptable use policy (AUP), acceptance pages, password changing capabilities, device registration, and self-registration. For those advanced capabilities, a centralized web portal is required.
- LWA does not support VLAN assignment; it supports only ACL assignment.
- LWA doesn't support the change of authorization (CoA) feature to apply new policies. Therefore, access policies cannot be changed based on posture or profiling state, and even administrative changes cannot be made as a result of malware to quarantine the endpoint.

Central Web Authentication with Cisco ISE

Cisco created Centralized Web Authentication (CWA) to overcome LWA's deficiencies.

CWA supports the following:

- CoA for posture profiling, as well as dACL and VLAN authorization options.
- All the advanced services: client provisioning, posture assessments, acceptable use policies, password changing, self-registration, and device registration.

Just like LWA, CWA is only for endpoints that have a web browser, where the user can manually enter a username and a password.

With CWA, WebAuth and guest VLAN functions remain mutually exclusive.

Central Web Authentication with Cisco ISE (Cont.)

Authentication for CWA is different from authentication for LWA. The following steps detail how CWA authentication takes place:

Step 1. The endpoint entering the network does not have a configured supplicant or the supplicant is misconfigured.

Step 2. The switch performs MAB, sending the RADIUS access-request to Cisco ISE (the authentication server).

Step 3. The authentication server (ISE) sends the RADIUS result, including a URL redirection, to the centralized portal on the ISE server itself.

Step 4. The endpoint is assigned and IP address, DNS server, and default gateway using DHCP.

Step 5. The end user opens a browser and enters credentials into the centralized web portal.

Step 6. ISE sends a re-authentication change of authorization (CoA-reauth) to the switch.

Step 7. The switch sends a new MAB request with the same session ID to ISE. ISE sends the final authorization result to the switch for the end user.

Enhanced Flexible Authentication (FlexAuth)

By default, a Cisco switch configured with 802.1x, MAB, and WebAuth always attempts 802.1x authentication first, followed by MAB, and finally WebAuth.

If an endpoint that does not support 802.1x tries to connect to the network, it needs to wait for a considerable amount of time before WebAuth is offered as an authentication option.

- Enhanced FlexAuth (also referred to as Access Session Manager) addresses this problem by allowing multiple authentication methods concurrently (for example, 802.1x and MAB) so that endpoints can be authenticated and brought online more quickly.
- Enhanced FlexAuth is a key component of the Cisco Identity-Based Networking Services (IBNS) 2.0 integrated solution, which offers authentication, access control, and user policy enforcement.

Cisco Identity-Based Networking Services (IBNS) 2.0

Cisco IBNS 2.0 is an integrated solution that offers authentication, access control, and user policy enforcement with a common end-to-end access policy that applies to both wired and wireless networks.

It is a combination of the following existing features and products:

- Enhanced FlexAuth (Access Session Manager)
- Cisco Common Classification Policy Language (C3PL)
- Cisco ISE

Cisco TrustSec

TrustSec is a next-generation access control enforcement solution developed by Cisco to address the growing operational challenges related to maintaining firewall rules and ACLs by using Security Group Tag (SGT) tags.

- TrustSec uses SGT tags to perform ingress tagging and egress filtering to enforce access control policy.
- Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated and authorized through 802.1x, MAB, or WebAuth.
- The SGT tag assignment is delivered to the authenticator as an authorization option (in the same way as a dACL). After the SGT tag is assigned, an access enforcement policy (allow or drop) based on the SGT tag can be applied at any egress point of the TrustSec network.
- SGT tags represent the context of the user, device, use case, or function. This means SGT tags are often named after particular roles or business use cases.

SGT tags are referred to as scalable group tags in Cisco Software-Defined Access (SD-Access).

Cisco TrustSec (Cont.)

Figure 25-9 illustrates a list of default SGT tags on Cisco ISE. The SGT tags all have business-relevant names and descriptions.

The SGT name is available on ISE and network devices to create policies; what is actually inserted into a Layer 2 frame SGT tag is a numeric value like the ones shown in the SGT column in decimal and hexadecimal notation.

TrustSec configuration occurs in three phases:

- Ingress classification
- Propagation
- Egress enforcement

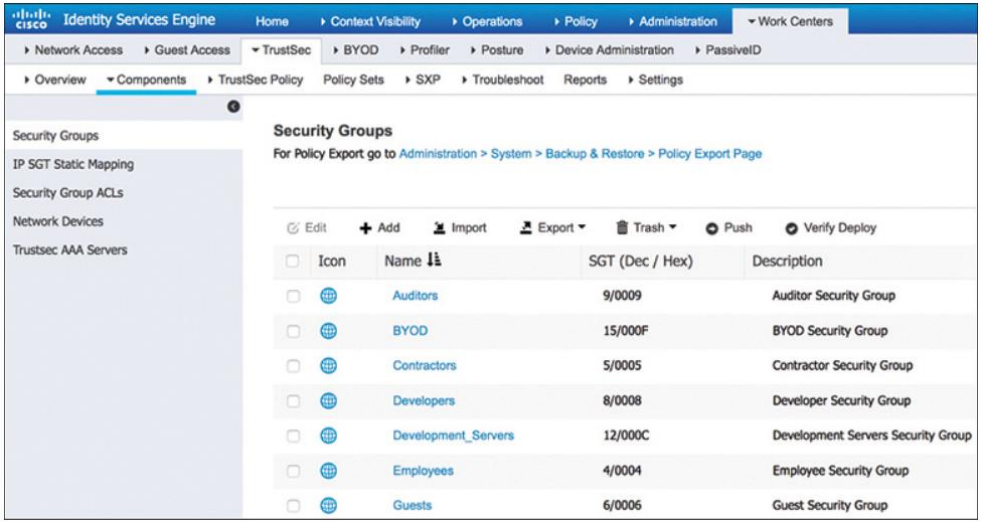

Figure 25-9 *Default SGT Tags in Cisco ISE*

Ingress Classification

Ingress classification is the process of assigning SGT tags to users, endpoints, or other resources as they ingress the TrustSec network, and it can happen in one of two ways:

- **Dynamic assignment -** The SGT is assigned dynamically and can be downloaded as an authorization option from ISE when authenticating using 802.1x, MAB, or WebAuth.
- **Static assignment -** In environments such as a data center that do not require 802.1x, MAB, or WebAuth authentication, dynamic SGT assignment is not possible. Static assignment on a device can be one of the following:
  - IP to SGT tag
  - Subnet to SGT tag
  - VLAN to SGT tag
  - Layer 2 interface to SGT tag
  - Layer 3 logical interface to SGT tag
  - Port to SGT tag
  - Port profile to SGT tag

As an alternative to assigning an SGT tag to a port, Cisco ISE added the ability to centrally configure a database of IP addresses and their corresponding SGT tags. Network devices that are SGT capable can download the list from Cisco ISE.

Propagation

Propagation is the process of communicating the mappings to the TrustSec network devices that will enforce policy based on SGT tags.

There are two methods available for propagating an SGT tag—inline tagging (also referred to as native tagging) and the Cisco-created protocol SGT Exchange Protocol (SXP):

- **Inline tagging -** With inline tagging, a switch inserts the SGT tag inside a frame to allow upstream devices to read and apply policy.

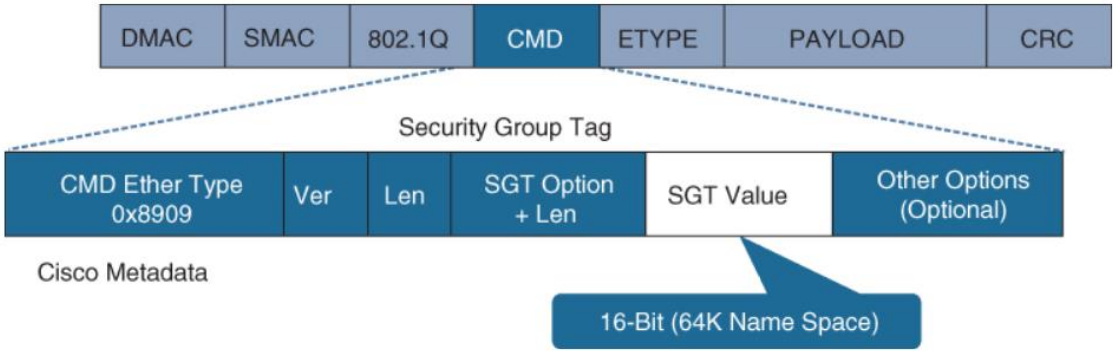

Figure 25-10 *Layer 2 Ethernet Frame with an SGT Tag*

Propagation (Cont.)

- **SXP propagation -** SXP is a TCP-based peer-to-peer protocol used for network devices that do not support SGT inline tagging in hardware.
  - Non-inline tagging switches also have an SGT mapping database to check packets against and enforce policy.
  - The SXP peer that sends IP-to-SGT bindings is called a speaker.
  - The IP-to-SGT binding receiver is called a listener.
  - SXP connections can be single-hop or multi-hop, as shown in Figure 25-11.

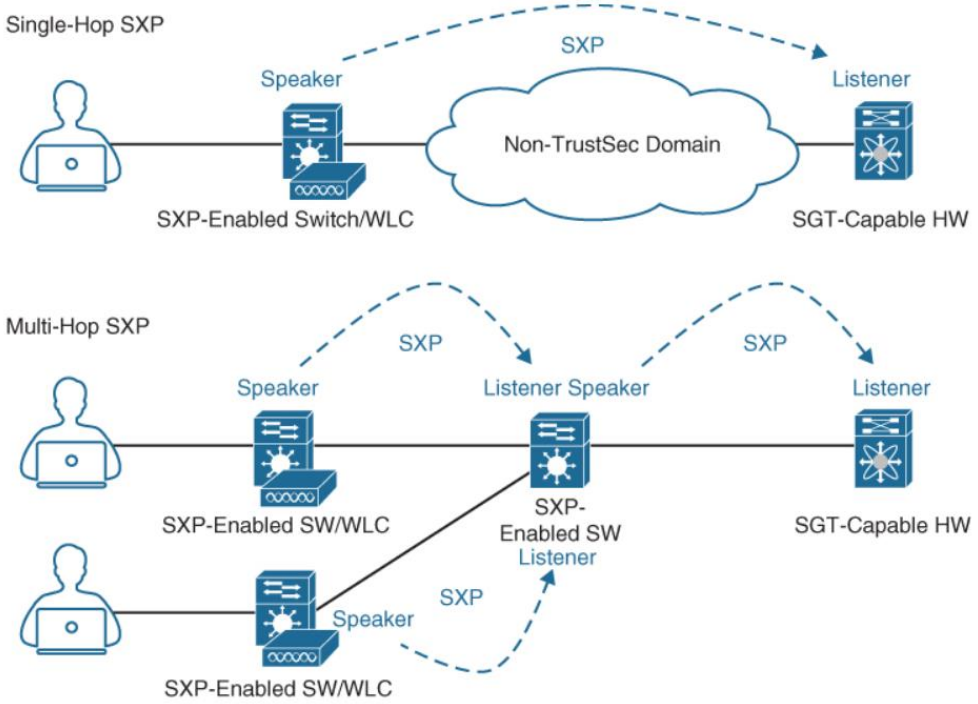

Figure 25-11 *Single-Hop and Multi-Hop SXP Connections*

Propagation: SPX Example

- Figure 25-12 shows an example of one access switch that supports native tagging. The packets get tagged on the uplink port and through the infrastructure.
- It also shows a switch that is not capable of inline tagging and that uses SXP to update the upstream switch.
- In both cases, the upstream switch continues to tag the traffic throughout the infrastructure.

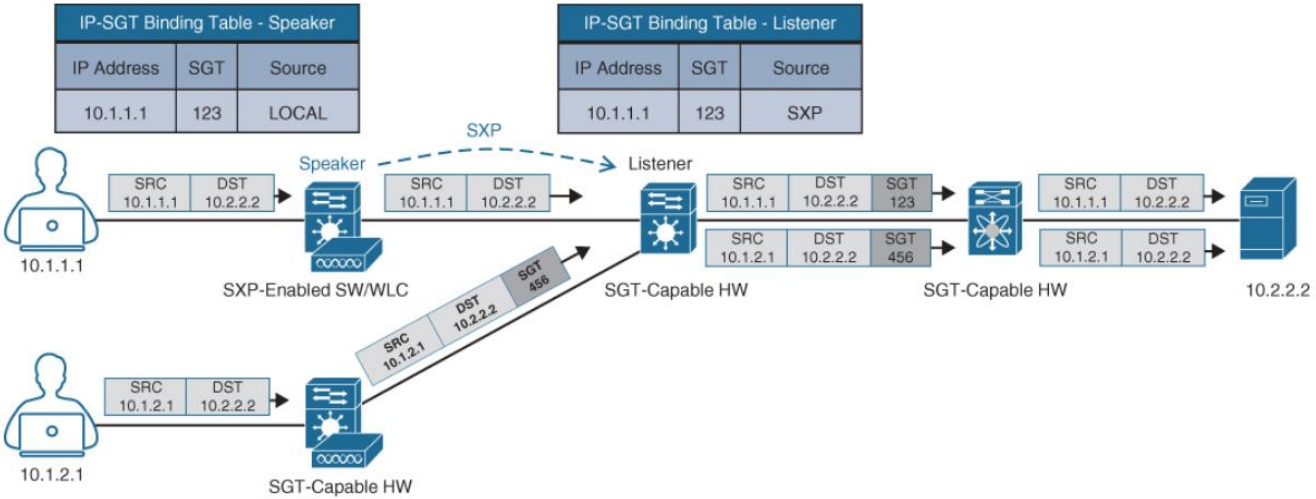

Figure 25-12 *Inline Tagging and SXP Propagation*

Propagation: SPX Peering

Figure 25-13 illustrates an example where a user authenticates to ISE via 802.1x.

The user is connected to a switch that does not support inline tagging or SXP. This means an SGT-to-IP binding cannot be assigned to the user on the switch. The solution is for ISE to assign an SGT to the user by sending a mapping through SXP to an upstream device that supports TrustSec.

Cisco ISE also supports assigning the SGT mapping information to an upstream device through pxGrid.

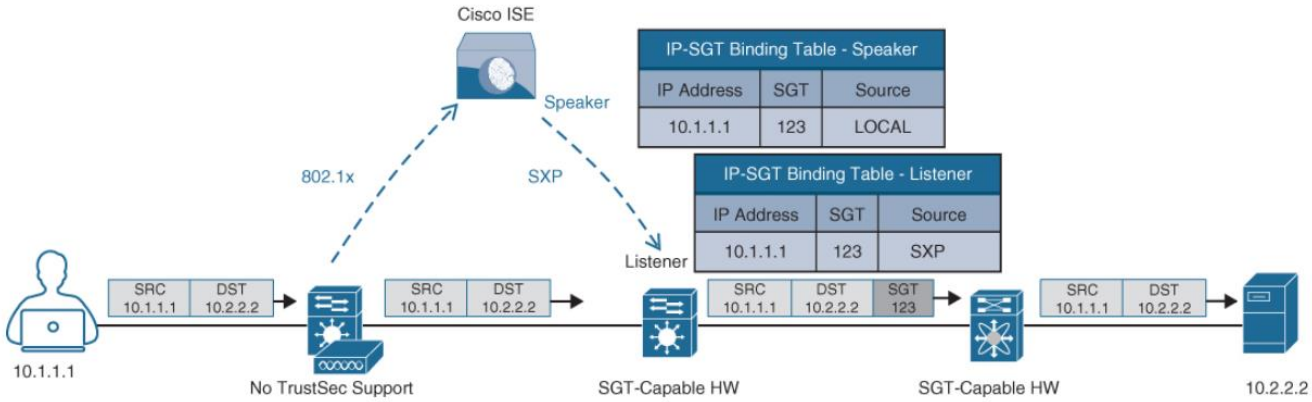

Figure 25-13 *SXP Peering Between Cisco ISE and TrustSec-Capable Devices*

Egress Enforcement

After the SGT tags have been assigned (classification) and are being transmitted across the network (propagation), policies can be enforced at the egress point of the TrustSec network.

- There are multiple ways to enforce traffic based on the SGT tag, and they can be divided into two major types:
- Security Group ACL (SGACL) - Provides enforcement on routers and switches. Access lists provide filtering based on source and destination SGT tags.
- Security Group Firewall (SGFW) - Provides enforcement on firewalls (such as Cisco ASA and NGFW). Requires tag-based rules to be defined locally on the firewall.

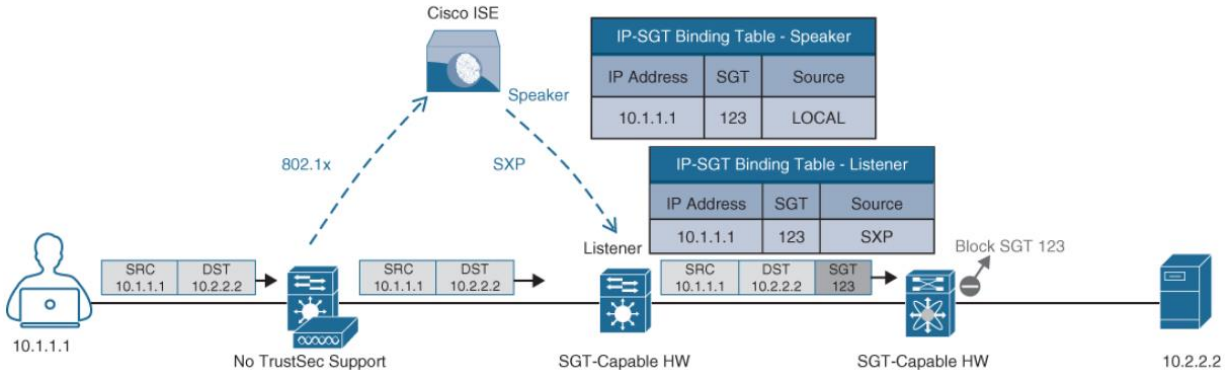

Figure 25-14 *TrustSec Enforcement with SGACL*

Egress Enforcement: SGACL

Figure 25-15 illustrates an SGACL egress policy production matrix from Cisco ISE that allows the defined SGACL enforcements to be visualized.

Figure 25-16 shows the SGACL Permit_FTP configuration on Cisco ISE, which is only allowing FTP traffic (TCP port 21) and denying all other traffic.

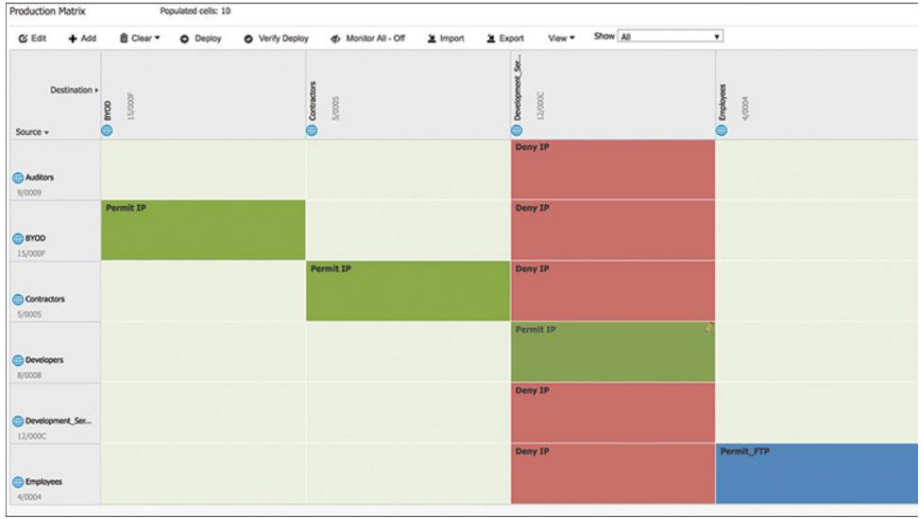

Figure 25-15 *SGACL Production Matrix View*

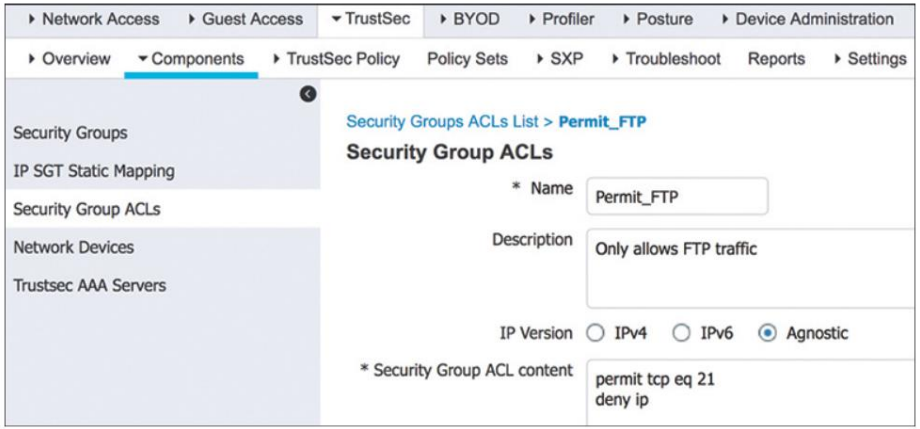

Figure 25-16 *Permit FTP SGACL Contents*

Egress Enforcement Example

Figure 25-17 illustrates a scenario where only developers have access to the development servers, and any employee trying to access them is blocked.

Traffic is blocked on egress and not on ingress.

This example also illustrates that FTP is the only protocol allowed between employees, while any other type of traffic is blocked. For the employees connected to the same switch, the switch is acting as the ingress and egress point.

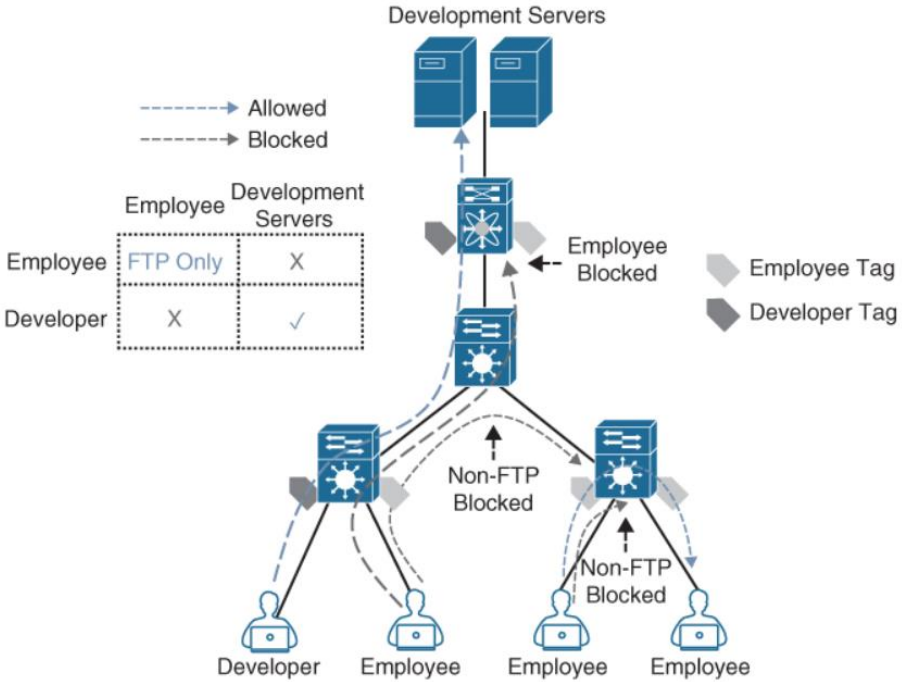

Figure 25-17 *SGACL Enforcement Scenario*

MACsec

MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption method.

- The traffic is encrypted only on the wire between two MACsec peers and is unencrypted as it is processed internally within the switch. This allows the switch to look into the inner packets for things like SGT tags to perform packet enforcement or QoS prioritization.
- MACsec also leverages onboard ASICs to perform the encryption and decryption rather than having to offload to a crypto engine, as with IPsec.
- MACsec is based on the Ethernet frame format; however, an additional 16-byte MACsec Security Tag field (802.1AE header) and a 16-byte Integrity Check Value (ICV) field are added.
- MACsec provides authentication using Galois Method Authentication Code (GMAC) or authenticated encryption using Galois/Counter Mode Advanced Encryption Standard (AES-GCM).

MACsec Illustrated

Figure 25-18 illustrates the MACsec frame format and how it encrypts the TrustSec SGT tag.

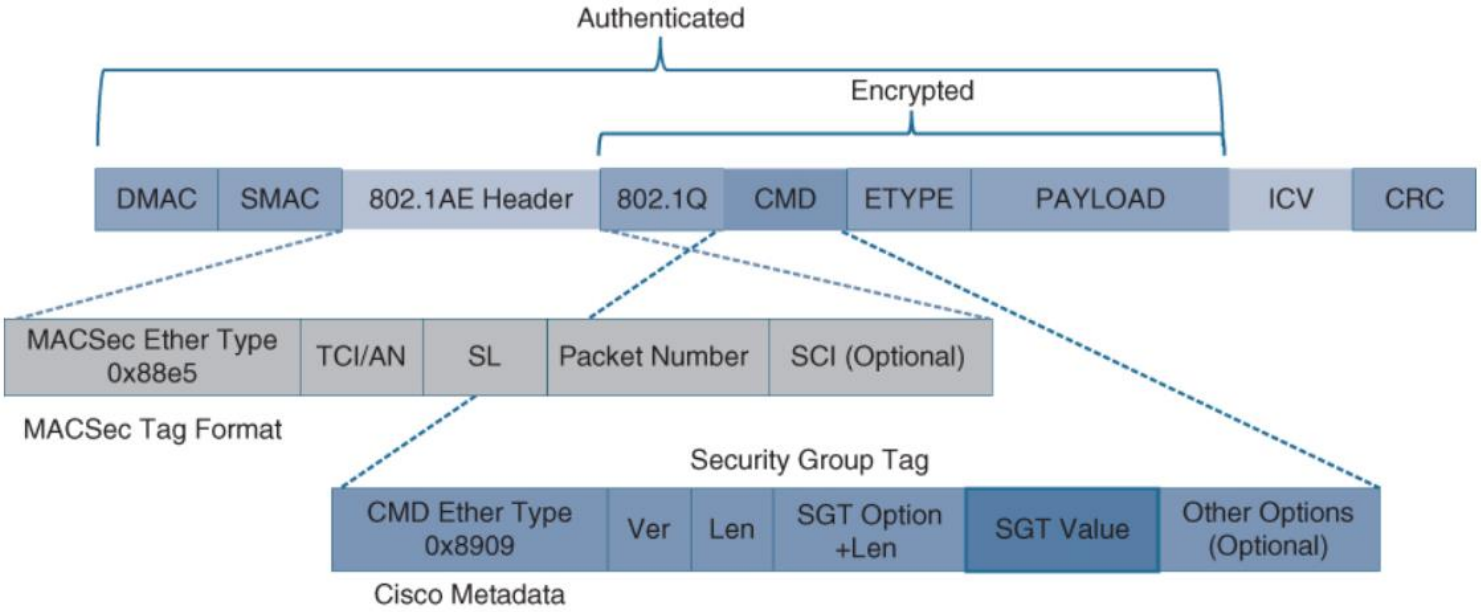

Figure 25-18 *MACsec Ethernet Frame with SGT*

MACsec Tags

The MACsec Security Tag fields are as follows:

- **MACsec EtherType (first two octets) -** Set to 0x88e5, designating the frame as a MACsec frame
- **TCI/AN (third octet) -** Tag Control Information/Association Number field, designating the version number if confidentiality or integrity is used on its own
- **SL (fourth octet) -** Short Length field, designating the length of the encrypted data
- **Packet Number (octets 5–8) -** The packet number for replay protection and building of the initialization vector
- **SCI (octets 9–16) -** Secure Channel Identifier, for classifying the connection to the virtual port

Two MACsec keying mechanisms are available:

- **Security Association Protocol (SAP) -** This is a proprietary Cisco keying protocol used between Cisco switches.
- **MACsec Key Agreement (MKA) protocol -** MKA provides the required session keys and manages the required encryption keys.

Downlink MACsec

Downlink MACsec is the term used to describe the encrypted link between an endpoint and a switch.

- The encryption between the endpoint and the switch is handled by the MKA keying protocol. This requires a MACsec-capable switch and a MACsec-capable supplicant on the endpoint (such as Cisco AnyConnect). The encryption on the endpoint may be handled in hardware or in software, using the main CPU for encryption and decryption.
- The Cisco switch has the ability to force encryption, make encryption optional, or force non-encryption.
- This setting may be configured manually per port (which is not very common) or dynamically as an authorization option from Cisco ISE.
- If ISE returns an encryption policy with the authorization result, the policy issued by ISE overrides anything set using the switch CLI.

Uplink MACsec

Uplink MACsec is the term for encrypting a link between switches with 802.1AE.

- By default, uplink MACsec uses Cisco proprietary SAP encryption. The encryption is the same AES-GCM-128 encryption used with both uplink and downlink MACsec.
- Uplink MACsec may be achieved manually or dynamically. Dynamic MACsec requires 802.1x authentication between the switches.

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 25

Description	
Cisco SAFE places in the network (PINs)	Cisco Web Security Appliance (WSA)
Full attack continuum	Cisco Email Security Appliance (ESA)
Cisco Talos	Intrusion Prevention System (IPS)
Cisco Threat Grid	Next-Generation Intrusion Prevention System (NGIPS)
Cisco Advanced Malware Protection (AMP)	Standard Firewall
Cisco AMP components	Next-Generation Firewall (NGFW)
Cisco AnyConnect	Cisco Stealthwatch
Cisco Umbrella	

Key Topics for Chapter 25 (Cont.)

Description	
Cisco Stealthwatch Offerings	Web Authentication (WebAuth)
Cisco Stealthwatch Required Components	WebAuth Types
Cisco Stealthwatch Cloud Offerings	Cisco TrustSec
Cisco Identity Services Engine (ISE)	Cisco TrustSec Phases
802.1x	Cisco TrustSec Propogation Methods
802.1x Components	Cisco TrustSec Types of Enforcement
802.1x Roles	MACsec
EAP Methods	MACsec Keying Mechanism
EAP Chaining	Downlink MACsec
MAC Authentication Bypass (MAB)	Uplink MACsec

Key Terms for Chapter 25

Terms	
802.1x	Cisco TrustSec
Cisco Advanced Malware Protection (AMP)	Cisco Umbrella
Cisco AnyConnect Secure Mobility Client	Cisco Web Security Appliance (WSA)
Cisco Email Security Appliance (ESA)	Endpoint
Cisco Identity Services Engine (ISE)	Extensible Authentication Protocol (EAP)
Cisco SAFE	MAC Authentication Bypass (MAB)
Cisco Stealthwatch	MACsec
Cisco Talos	next-generation firewall(NGFW)
Cisco Threat Grid	Web Authentication (WebAuth)


CISCO