CHAPTER 48

Configuring the ASA to Integrate with Cisco TrustSec

This chapter includes the following sections:

Information About the ASA Integrated with Cisco TrustSec

This section includes the following topics:

Information about Cisco TrustSec

Traditionally, security features such as firewalls performed access control based on predefined IP addresses, subnets and protocols. However, with enterprises transitioning to borderless networks, both the technology used to connect people and organizations and the security requirements for protecting data and networks have evolved significantly. End points are becoming increasingly nomadic and users often utilize a variety of end points (for example, laptop versus desktop, smart phone, or tablet), which means that a combination of user attributes plus end-point attributes provide the key characteristics, in addition to existing 5-tuple based rules, that enforcement devices, such as switches and routers with firewall features or dedicated firewalls, can reliably use for making access control decisions.

As a result, the availability and propagation of end point attributes or client identity attributes have become increasingly important requirements to enable security solutions across the customers' networks, at the access, distribution, and core layers of the network and in the data center to name but a few examples.

Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security solutions across networks at the access, distribution, and core layers of the network.

Implementing Cisco TrustSec into your environment has the following advantages:

- Provides a growing mobile and complex workforce with appropriate and more secure access from any device
- Lowers security risks by providing comprehensive visibility of who and what is connecting to the wired or wireless network
- Offers exceptional control over activity of network users accessing physical or cloud-based IT resources
- Reduces total cost of ownership through centralized, highly secure access policy management and scalable enforcement mechanisms

For information about Cisco TrustSec, see http://www.cisco.com/go/trustsec.

About SGT and SXP Support in Cisco TrustSec

In the Cisco TrustSec solution, security group access transforms a topology-aware network into a role-based network, thus enabling end-to-end policies enforced on the basis of role-based access-control (RBACL). Device and user credentials acquired during authentication are used to classify packets by security groups. Every packet entering the Cisco TrustSec cloud is tagged with an security group tag (SGT). The tagging helps trusted intermediaries identify the source identity of the packet and enforce security policies along the data path. An SGT can indicate a privilege level across the domain when the SGT is used to define a security group access list.

An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB), which happens with a RADIUS vendor-specific attribute. An SGT can be assigned statically to a particular IP address or to a switch interface. An SGT is passed along dynamically to a switch or access point after successful authentication.

The Security-group eXchange Protocol (SXP) is a protocol developed for Cisco TrustSec to propagate the IP-to-SGT mapping database across network devices that do not have SGT-capable hardware support to hardware that supports SGTs and security group access lists. SXP, a control plane protocol, passes IP-SGT mappings from authentication points (such as legacy access layer switches) to upstream devices in the network.

The SXP connections are point-to-point and use TCP as the underlying transport protocol. SXP uses the well known TCP port number 64999 when initiating a connection. Additionally, an SXP connection is uniquely identified by the source and destination IP addresses.

Roles in the Cisco TrustSec Solution

To provide identity and policy-based access enforcement, the Cisco TrustSec solution includes the functionality:

- **Access Requestor (AR)**: Access requestors are end-point devices that request access to protected resources in the network. They are primary subjects of the architecture and their access privilege depends on their Identity credentials.

  Access requestors include end-point devices such PCs, laptops, mobile phones, printers, cameras, and MACsec-capable IP phones.
- **Policy Decision Point (PDP)**: A policy decision point is responsible for making access control decisions. The PDP provides features such as 802.1x, MAB, and Web authentication. The PDP supports authorization and enforcement through VLAN, DACL, and security group access (SGACL/SXP/SGT).

  In the Cisco TrustSec solution, the Cisco Identity Services Engine (ISE) acts as the PDP. The Cisco ISE provides identity and access control policy functionality.
- **Policy Information Point (PIP)**: A policy information point is a source that provides external information (for example, reputation, location, and LDAP attributes) to policy decision points.

  Policy information points include devices such as Session Directory, Sensors IPS, and Communication Manager.
- **Policy Administration Point (PAP)**: A policy administration point defines and inserts policies into authorization system. The PAP acts as an identity repository, by providing Cisco TrustSec tag to user identity mapping and Cisco Trustsec tag to server resource mapping.

  In the Cisco TrustSec solution, the Cisco Secure Access Control System (a policy server with integrated 802.1x and SGT support) acts as the PAP.
- **Policy Enforcement Point (PEP)**: A policy enforcement point is the entity that carries out the decisions (policy rules and actions) made by the PDP for each AR. PEP devices learn identity information through the primary communication path that exists across networks. PEP devices learn the identity attributes of each AR from many sources, such as end-point agents, authorization servers, peer-enforcement devices, and network flows. In turn, PEP devices use SXP to propagate IP-SGT mappings to mutually-trusted peer devices across the network.

  Policy enforcement points include network devices such as Catalyst switches, routers, firewalls (specifically the ASA), servers, VPN devices, and SAN devices.

The ASA serves the role of the PEP in the identity architecture. Using SXP, the ASA learns identity information directly from authentication points and uses that to enforce identity-based policies.

Security Group Policy Enforcement

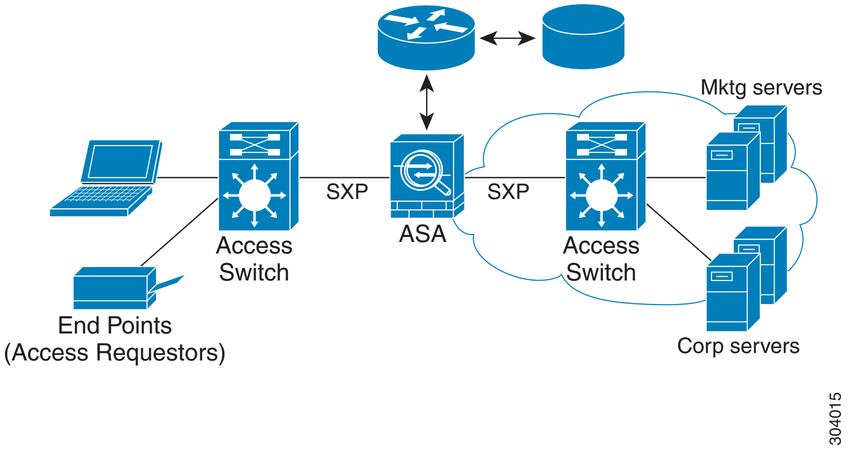
Security policy enforcement is based on security group name. An end-point device attempts to access a resource in the data center. Compared to traditional IP-based policies configured on firewalls, identity-based policies are configured based on user and device identities. For example, mktg-contractor is allowed to access mktg-servers; mktg-corp-users are allowed to access mktg-server and corp-servers.

The benefits of this type of deployment include:

- User group and Resource is defined and enforced using single object (SGT) – simplified policy management.

- User identity and resource identity are retained throughout the Cisco Trustsec capable switch infrastructure.

Figure 48-1 Security Group Name Based Policy Enforcement Deployment



Implementing Cisco TrustSec allows for configuration of security policies supporting server segmentation.

- A pool of servers can be assigned an SGT for simplified policy management.
- The SGT information is retained within the infrastructure of Cisco Trustsec capable switches.
- The ASA can leverage the IP-SGT mapping for policy enforcement across the Cisco TrustSec domain.
- Deployment simplification is possible because 802.1x authorization for servers is mandatory.

How the ASA Enforces Security Group Based Policies

Note User-based security policies and security-group based policies, can coexist on the ASA. Any combination of network, user-based and security-group based attributes can be configured in an security policy. See Chapter 47, "Configuring the Identity Firewall" for information about configuring user-based security policies.

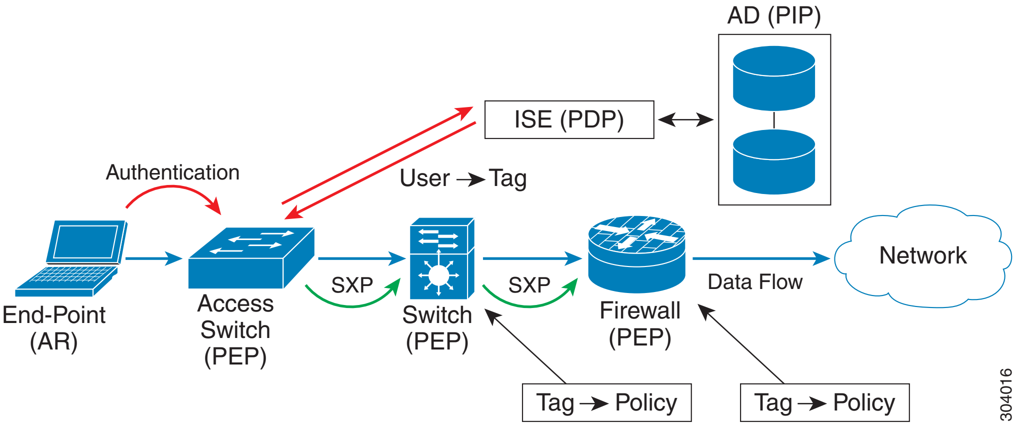
As part of configuring the ASA to function with Cisco TrustSec, you must import a Protected Access Credential (PAC) file from the ISE. Importing a Protected Access Credential (PAC) File, page 48-12.

Importing the PAC file to the ASA establishes a secure communication channel with the ISE. After the channel is established, the ASA initiates a PAC secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data; specifically, the ASA downloads the security group table. The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups.

The first time the ASA downloads the security group table, it walks through all entries in the table and resolves all the security group names contained in security policies configured on the ASA; then, the ASA activates those security policies locally. If the ASA is unable to resolve a security group name, it generates a system log message for the unknown security group name.

The following figure shows how a security policy is enforced in Cisco TrustSec.

Figure 48-2 Security Policy Enforcement



1. An end-point device connects to an access layer device directly or via remote access and authenticates with Cisco TrustSec.
2. The access layer device authenticates the end-point device with the ISE by using authentication methods such as 802.1X or web authentication. The end-point device passes role and group membership to classify the device into the appropriate security group.
3. The access layer device uses SXP to propagate the IP-SGT mapping to the upstream devices.
4. The ASA receives the packet. Using the IP-SGT mapping passed by SXP, the ASA looks up the SGTs for the source and destination IP addresses.

   If the mapping is new, the ASA records it in its local IP-SGT Manager database. The IP-SGT Manager database, which runs in the control plan, tracks IP-SGT mappings for each IPv4 or IPv6 address. The database records the source from which the mapping was learned. The peer IP address of the SXP connection is used as the source of the mapping. Multiple sources can exist for each IP-SGT mapping.

   If the ASA is configured as a Speaker, the ASA transmits all IP-SGT mappings to its SXP peers. See About Speaker and Listener Roles on the ASA, page 48-5.
5. If a security policy is configured on the ASA with that SGT or security group name, the ASA enforces the policy. (You can create security policies on the ASAthat contain SGTs or security group names. To enforce policies based on security group names, the ASA needs the security group table to map security group names to SGTs.)

   If the ASA cannot find a security group name in the security group table and it is included in a security policy, the ASA considers the security group name unknown and generates a system log message. When it becomes know after the ASA refreshes the security group table from the ISE, the ASA generates a system log message indicating that the security group name is known.

About Speaker and Listener Roles on the ASA

The ASA supports SXP to send and receive IP-SGT mappings to and from other network devices. Employing SXP allows security devices and firewalls to learn identity information from access switches without the need for hardware upgrades or changes. SXP can also be used to pass IP-SGT mappings from upstream devices (such as datacenter devices) back to the downstream devices. The ASA can receive information from both upstream and downstream directions.

When configuring an SXP connection on the ASA to an SXP peer, you must designate the ASA as a Speaker or a Listener for that connection so that it can exchange identity information:

- **Speaker mode**—configures the ASA so that it can forward all active IP-SGT mappings collected on the ASA to upstream devices for policy enforcement.
- **Listener mode**—configures the ASA so that it can receive IP-SGT mappings from downstream devices (SGT-capable switches) and use that information in creating policy definitions.

If one end of an SXP connection is configured as Speaker, then the other end must be configured as a Listener, and vice versa. If both devices on each end of an SXP connection are configured with the same role (either both as Speakers or both as Listeners), the SXP connection will fail and the ASA will generate a system log message.

Configuring the ASA to be both a Speaker and a Listener for an SXP connection can cause SXP looping, meanings that SXP data can be received by an SXP peer that originally transmitted it.

As part of configuring SXP on the ASA, you configure an SXP reconcile timer. After an SXP peer terminates its SXP connection, the ASA starts a hold down timer. Only SXP peers designated as Listener devices can terminate a connection. If an SXP peer connects while the hold down timer is running, the ASA starts the reconcile timer; then, the ASA updates the IP-SGT mapping database to learn the latest mappings.

Features of the ASA-Cisco TrustSec Integration

The ASA leverages Cisco TrustSec as part of its identity-based firewall feature. The integrating the ASA with Cisco TrustSec provides the following key features.

Flexibility

- The ASA can be configured as an SXP Speaker or Listener, or both.

  See About Speaker and Listener Roles on the ASA, page 48-5.
- The ASA supports SXP for IPv6 and IPv6 capable network devices.
- The ASA negotiates SXP versions with different SXP-capable network devices. SXP version negotiation eliminates the need for static configuration of versions.
- You can configure the ASA to refresh the security group table when the SXP reconcile timer expires and you can download the security group table on demand. When the security group table on the ASA is updated from the ISE, changes are reflected in the appropriate security policies.
- The ASA supports security policies based on security group names in the source or destination fields, or both. You can configure security policies on the ASA based on combinations of security groups, IP address, Active Directory group/user name, and FQDN.

Availability

- You can configure security group based policies on the ASA in Active/Active and Active/Standby configuration.
- The ASA can communicate with the ISE configured for high availability (HA).
- If the PAC file downloaded from the ISE expires on the ASA and the ASA cannot download an updated security group table, the ASA continues to enforce security policies based on the last downloaded security group table until the ASA downloads an updated table.

Scalability

The ASA supports the following number of IP-SGT mapped entries:

Table 48-1 Capacity Numbers for IP-SGT Mappings

ASA Platform	Number of IP-SGT Mapped Entries
5505	250
5510	1000
5520	2500
5540	5000
5550	7500
5580-20	10,000
5580-40	20,000
5585-X with SSP-10	18,750
5585-X with SSP-20	25,000
5585-X with SSP-40	50,000
5585-X with SSP-60	100,000

The ASA supports the following number of SXP connections:

Table 48-2 SXP Connections

ASA Platform	Number of SXP TCP Connections
5505	10
5510	25
5520	50
5540	100
5550	150
5580-20	250
5580-40	500
5585-X with SSP-10	150
5585-X with SSP-20	250
5585-X with SSP-40	500
5585-X with SSP-60	1000

Licensing Requirements when Integrating the ASA with Cisco TrustSec

Model	License Requirement
All models	Base License.

Prerequisites for Integrating the ASA with Cisco TrustSec

Before configuring the ASA to integrate with Cisco TrustSec, you must perform the following prerequisites:

- Register the ASA with the ISE.
- Create a security group for the ASA on the ISE.
- Generate the PAC file on the ISE to import into the ASA.

Registering the ASA with the ISE

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can successfully import a PAC file.

1. Log into the ISE.
2. Choose **Administration** > **Network Devices** > **Network Devices**.
3. Click **Add**.
4. Enter the IP address of the ASA.
5. When the ISE is being used for user authentication in the Cisco TrustSec solution, enter a shared secret in the Authentication Settings area.

   When you configure the AAA sever on the ASA, provide the shared secret you create here on the ISE. The AAA server on the ASA uses this shared secret to communicate with the ISE.
6. Specify a device name, device ID, password, and a download interval for the ASA. See the ISE documentation for the details to perform these tasks.

Creating a Security Group on the ISE

When configuring the ASA to communicate with the ISE, you specify a AAA server. When configuring the AAA server on the ASA, you must specify a server group.

The security group must be configured to use the RADIUS protocol.

1. Log into the ISE.
2. Choose **Policy** > **Policy Elements** > **Results** > **Security Group Access** > **Security Group**.
3. Add a security group for the ASA. (Security groups are global and not ASA specific.)

   The ISE creates an entry under Security Groups with a tag.
4. Under the Security Group Access section, configure a device ID credentials and password for the ASA.

Generating the PAC File

For information about the PAC file, see Importing a Protected Access Credential (PAC) File, page 48-12.

Before generating the PAC file, you must have registered the ASA with the ISE.

1. Log into the ISE.
2. Choose **Administration** > **Network Resources** > **Network Devices**.
3. From the list of devices, select the ASA device.
4. Under the Security Group Access (SGA), click **Generate PAC**.
5. To encrypt the PAC file, enter a password.

The password (or encryption key) you enter to encrypt the PAC file is independent of the password that was configured on the ISE as part of the device credentials.

The ISE generates the PAC file. The ASA can import the PAC from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC does not have to reside on the ASA flash before you can import it.)

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6

Clustering Guideline

Supported only on the master device in a clustering setting.

High Availability Guideline

Supports a list of servers via configuration. If the first server is unreachable, the ASA will try to contact the second server in the list, and so on. However, the server list downloaded as part of the Cisco TrustSec environment data is ignored.

Limitations

- The ASA can only be configured to interoperate in a single Cisco TrustSec domain.
- The ASA does not support static configuration of SGT-name mappings on the device.
- NAT is not supported in SXP messages.
- SXP conveys IP-SGT mappings to enforcement points in the network. If an access layer switch belongs to a different NAT domain than the enforcing point, the IP-SGT map it uploads is invalid and an IP-SGT mappings database lookup on the enforcement device will not yield valid results; therefore, the ASA cannot apply security group aware security policy on the enforcement device.
- You can configure a default password for the ASA to use for SXP connections, or you can choose not to use a password; however, connection-specific passwords are not supported for SXP peers. The configured default SXP password should be consistent across the deployment network. If you configure a connection-specific password, connections may fail and a warning message will appear. If you configure the connection with the default password, but the default password is not configured, the result is the same as when you have configured the connection with no password.
- SXP connection loops can form when a device has bidirectional connections to a peer, or is part of a unidirectionally connected chain of devices. (The ASA can learn IP-DGT mappings for resources from the access layer in the data center. The ASA might need to propagate these tags to downstream devices.) SXP connection loops can cause unexpected behavior of SXP message transport. In cases where the ASA is configured to be a Speaker and Listener, an SXP connection loop can occur causing SXP data to be received by the peer that originally transmitted it.

- When changing the ASA local IP address, you must ensure that all SXP peers have updated their peer list. Likewise, if an SXP peers changes its IP addresses, you must ensure those changes are reflected on the ASA.
- Automatic PAC file provisioning is not supported. The ASA administrator must request the PAC file from the ISE administrative interface and import it to the ASA. For information about the PAC file, see Generating the PAC File, page 48-8 and Importing a Protected Access Credential (PAC) File, page 48-12.
- PAC files have expiration dates. You must import the updated PAC file before the current PAC file expires; otherwise, the ASA will not be able to retrieve environment data updates.
- When a security group changes on the ISE (for example, it is renamed or deleted), the ASA does not change the status of any ASA security policies that contain an SGT or security group name associated with the changed security group; however, the ASA generates a system log message to indicate that those security policies changed.

  See Refreshing Environment Data, page 48-16 for information about manually updating the security group table on the ASA to pick up changes from the ISE.
- The multicast types are not supported in ISE 1.0.
- An SXP connection stays in the initializing state among two SXP peers interconnected by the ASA; as shown in the following example:

  (SXP peer A) - - - - (ASA) - - - (SXP peer B)

  Therefore, when configuring the ASA to integrate with Cisco TrustSec, you must enable the no-NAT, no-SEQ-RAND, and MD5-AUTHENTICATION TCP options on the ASA for SXP connections. Create a TCP-state-bypass policy for traffic destined to SXP port TCP 64999 among the SXP peers. Apply the policy on the appropriate interfaces.

  For example, configure the ASA as shown in this sample configuration for a TCP-state-bypass policy:

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

Configuring the ASA for Cisco TrustSec Integration

This section contains the following topics:

- Task Flow for Configuring the ASA to Integrate with Cisco TrustSec, page 48-11

- Configuring the AAA Server for Cisco TrustSec Integration, page 48-11
- Importing a Protected Access Credential (PAC) File, page 48-12
- Configuring the Security Exchange Protocol (SXP), page 48-14
- Adding an SXP Connection Peer, page 48-15
- Refreshing Environment Data, page 48-16
- Configuring the Security Policy, page 48-17

Task Flow for Configuring the ASA to Integrate with Cisco TrustSec

Prerequisite

Before configuring the ASA to integrate with Cisco TrustSec, you must meet the following prerequisites:

- Register the ASA with the ISE.
- Generate the PAC file on the ISE to import into the ASA.

See the "Prerequisites for Integrating the ASA with Cisco TrustSec" section on page 48-8 for information.

Task Flow in the ASA

To configure the ASA to integrate with Cisco TrustSec, perform the following tasks:

Step 1 Configure the AAA server.

See Configuring the AAA Server for Cisco TrustSec Integration, page 48-11.

Step 2 Import the PAC file from the ISE.

See Importing a Protected Access Credential (PAC) File, page 48-12.

Step 3 Enable and set the default values for SXP.

See Configuring the Security Exchange Protocol (SXP), page 48-14.

Step 4 Add SXP connection peers for the Cisco TrustSec architecture.

See Adding an SXP Connection Peer, page 48-15.

Step 5 As necessary, refresh environment data for the ASA integrated with Cisco TrustSec.

See Refreshing Environment Data, page 48-16.

Step 6 Configure the Security Policy.

See Configuring the Security Policy, page 48-17.

Configuring the AAA Server for Cisco TrustSec Integration

As part of configuring the ASA to integrate with Cisco TrustSec, you must configure the ASA so that it can communicate with the ISE.

See also the "Configuring AAA Server Groups" section on page 46-11 and the "Adding a Server to a Group" section on page 46-12 for more information.

Prerequisites

- The referenced server group must be configured to use the RADIUS protocol. If you add a non-RADIUS server group to the ASA, the feature configuration will fail.
- If the ISE is also used for user authentication, obtain the shared secret that was entered on the ISE when you registered the ASA with the ISE. Contact your ISE administrator if you do not have this information.

To configure the ASA to communicate with the ISE for Cisco TrustSec integration, perform the following steps:

Step 1 In the main ASDM application window, choose **Configuration** > **Firewall** > **Identity By TrustSec**. The Identity By TrustSec pane appears.

Step 2 To add a server group to the ASA, click **Manage** in the Server Group Setup area, The Configure AAA Server Group dialog box appears.

Step 3 In the AAA Server Group field, enter the name of the security group created on the ISE for the ASA.

The server group name you specify here must match the name of the security group created on the ISE for the ASA. If these two group names do not match, the ASA will not be able to communicate with the ISE. Contact your ISE administrator if you do not have this information.

Step 4 In the Protocol drop-down list, select RADIUS.

For information about completing the remaining fields in the AAA Server Group dialog box, see Configuring AAA Server Groups, page 46-11

Step 5 Click **OK**. The ASA adds the group to the list of AAA Server Groups.

Step 6 To add a server to a group, select the AAA sever group you just created and click **Add** in the Servers in the Selected Group area (lower pane). The Add AAA Server dialog box appears.

Step 7 In the Interface Name field, select the network interface where the ISE server resides.

Step 8 In the Server Name or IP Address field, enter the IP address of the ISE server.

For information about completing the remaining fields in the AAA Server dialog box, see See Adding a Server to a Group, page 46-12.

Step 9 Click **OK**. The ASA adds the ISE server to the list of AAA servers.

Step 10 Click **OK** to save the addition of the ISE server and server group for the integration with Cisco TrustSec.

The changes are saved to the running configuration.

Importing a Protected Access Credential (PAC) File

Importing the PAC file to the ASA establishes the connection with the ISE. After the channel is established, the ASA initiates a secure RADIUS transaction with the ISE and downloads Cisco TrustSec environment data; specifically, the ASA downloads the security group table. The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups.

More specifically, no channel is established prior to the radius transaction. The ASA simply initiates a radius transaction with the ISE using the PAC for authentication

Tip The PAC file contains a shared key that allows the ASA and ISE to secure the RADIUS transactions that occur between them. Given the sensitive nature of this key, it must be stored securely on the ASA.

When you import the PAC file, the file is converted to ASCII HEX format and sent to the ASA in non-interactive mode. After successfully importing the file, the ASA download Cisco TrustSec environment data from the ISE without requiring the device password configured in the ISE.

Prerequisites

- The ASA must be configured as a recognized Cisco TrustSec network device in the ISE before the ASA can generate a PAC file. The ASA can import any PAC file but it will only work on the ASA when the file was generated by a properly configured ISE. See Registering the ASA with the ISE, page 48-8.
- Obtain the password used to encrypt the PAC file when generating it on the ISE.

  The ASA requires this password to import and decrypt the PAC file.
- Access to the PAC file generated by the ISE. The ASA can import the PAC from flash or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB. (The PAC does not have to reside on the ASA flash before you can import it.)
- The server group has been configured for the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must import the PAC file to the primary ASA device.
- When the ASA is part of a clustering configuration, you must import the PAC to the master device.

To import a PAC file, perform the following steps:

Step 1 In the main ASDM application window, choose **Configuration** > **Firewall** > **Identity By TrustSec**. The Identity By TrustSec pane appears.

Step 2 Check the Enable Security Exchange Protocol checkbox to enable SXP.

Step 3 In the Server Group Setup area, click Import PAC. The Import PAC dialog box appears.

Step 4 In the Filename field, enter the path and filename for the PAC file by using one of the following formats:

- disk0: Path and filename on disk0
- disk1: Path and filename on disk1
- flash: Path and filename on flash

Step 5 In the Password field, enter the password used to encrypt the PAC file. The password is independent of the password that was configured on the ISE as part of the device credentials.

Step 6 In the Confirm Password field, re-enter the password to confirm it.

Step 7 Click **Import**. The Identity By TrustSec pane reappears.

Step 8 Click **Apply** to save the changes.

The changes are saved to the running configuration.

Configuring the Security Exchange Protocol (SXP)

Configuring the Security Exchange Protocol (SXP) involves enabling the protocol in the ASA and setting the following default values for SXP:

- The source IP address of SXP connections
- The authentication password between SXP peers
- The retry interval for SXP connections
- The Cisco TrustSec SXP reconcile period

To configure the default settings for the ASA integration with Cisco TrustSec, perform the following steps:

Step 1 In the main ASDM application window, choose **Configuration > Firewall > Identity By TrustSec**. The Identity By TrustSec pane appears.

Step 2 Check the Enable Security Exchange Protocol checkbox to enable SXP. By default, SXP is disabled.

In multi-context mode, enabling SXP is done in the user context.

Step 3 In the Default Source field, enter the default local IP address for SXP connections. The IP address can be an IPv4 or IPv6 address.

Note The ASA determines the local IP address for an SXP connection as the outgoing interface IP address that is reachable by the peer IP address. If the configured local address is different from the outgoing interface IP address, the ASA cannot connect to the SXP peer and generates a system log message.

Step 4 In the Default Password field, enter the default password for TCP MD5 authentication with SXP peers. By default, SXP connections do not have a password set.

You can specify the password as an encrypted string up to 162 characters or an ASCII key string up to 80 characters. Configuring an encryption level for the password is optional. If you configure an encryption level, you can only set one level:

- Level 0—unencrypted cleartext
- Level 8—encrypted text

Step 5 In the Retry Timer field, enter the default time interval between ASA attempts to set up new SXP connections between SXP peers.

The ASA will continue to attempt to connect to new SXP peers until a successful connection is made. The retry timer is triggered as long as there is one SXP connection on the ASA that is not up.

Enter the retry timer value as a number of seconds in the range of 0 to 64000 seconds. If you specify 0 seconds, the timer never expires and the ASA will not attempt to connect to SXP peers. By default, the *timervalue* is 120 seconds.

When the retry timer expires, the ASA goes through the connection database and if the database contains any connections that are off or in a “pending on” state, the ASA restarts the retry timer.

Step 6 In the Reconcile Timer field, enter the default reconcile timer.

After an SXP peer terminates its SXP connection, the ASA starts a hold down timer. If an SXP peer connects while the hold down timer is running, the ASA starts the reconcile timer; then, the ASA updates the SXP mapping database to learn the latest mappings.

When the reconcile timer expires, the ASA scans the SXP mapping database to identify stale mapping entries (entries that were learned in a previous connection session). The ASA marks these connections as obsolete. When the reconcile timer expires, the ASA removes the obsolete entries from the SXP mapping database.

Enter the reconcile timer value as a number of seconds in the range of 1 to 64000 seconds. By default, the *timervalue* is 120 seconds.

Note You cannot specify 0 for the timer because specifying 0 would prevent the reconcile timer from starting. Not allowing the reconcile timer to run would keep stale entries for an undefined time and cause unexpected results from the policy enforcement.

Step 7 Click **Apply** to save the default settings.

The changes are saved to the running configuration.

Adding an SXP Connection Peer

SXP connections between peers are point-to-point and use TCP as the underlying transport protocol.

To add an SXP connection peer, perform the following steps:

Step 1 In the main ASDM application window, choose **Configuration** > **Firewall** > **Identity By TrustSec**. The Identity By TrustSec pane appears.

Step 2 If necessary, check the Enable Security Exchange Protocol checkbox to enable SXP.

Step 3 Click **Add**. The Add Connection dialog box appears.

Step 4 In the Peer IP Address field, enter the IPv4 or IPv6 address of the SXP peer. The peer IP address must be reachable from the ASA outgoing interface.

Step 5 **(Optional)** In the Source IP Address field, enter the local IPv4 or IPv6 address of the SXP connection. Specifying the source IP address is optional, however, specifying it safeguards misconfiguration.

Step 6 From the Password drop-down list, specify whether to use the authentication key for the SXP connection by selecting the following values:

- Default—Use the default password configured for SXP connections.

  See Configuring the Security Exchange Protocol (SXP), page 48-14.

- None—Do not use a password for the SXP connection.

Step 7 **(Optional)** From the Mode drop-down list, specify the mode of the SXP connection by selecting one of the following values:

- Local—Use the local SXP device.
- Peer—Use the peer SXP device.

Step 8 From the Role drop-down list, specify whether the ASA functions as a Speaker or Listener for the SXP connection:

- Speaker—The ASA can forward IP-SGT mappings to upstream devices.
- Listener—The ASA can receive IP-SGT mappings from downstream devices.

See About Speaker and Listener Roles on the ASA, page 48-5.

Step 9 Click **OK**. The peer appears in the Connection Peers list.

Step 10 Click **Apply** to save SXP peer settings.

The changes are saved to the running configuration.

Refreshing Environment Data

The ASA downloads environment data from the ISE, which includes the Security Group Tag (SGT) name table. The ASA automatically refreshes its environment data obtained from the ISE when you complete the following tasks on the ASA:

- Configure a AAA server to communicate with the ISE.
- Import a PAC file from the ISE.
- Identify the AAA server group that the ASA will use for retrieval of Cisco TrustSec environment data.

Normally, you will not need to manually refresh the environment data from the ISE; however, security groups can change on the ISE. These changes are not reflected on the ASA until you refresh the data in the ASA security group table. Refresh the data on the ASA to make sure any security group made on the ISE are reflected on the ASA.

Tip We recommend that you schedule policy configuration changes on the ISE and the manual data refresh on the ASA during a maintenance window. Handling policy configuration changes in this way maximizes the chances of security group names getting resolved and security policies becoming active immediately on the ASA.

Prerequisites

The ASA must be configured as a recognized Cisco TrustSec network device in the ISE and the ASA must have successfully imported a PAC file, so that the changes made for Cisco TrustSec are applied to the ASA.

Restrictions

- When the ASA is part of an HA configuration, you must refresh the environment data on the primary ASA device.
- When the ASA is part of a clustering configuration, you must refresh the environment data on the master device.

To Refresh Environment Data

In the main ASDM application window, choose **Configuration** > **Firewall** > **Identity By TrustSec**. The Identity By TrustSec pane appears. In the Server Group Setup area, click **Refresh Environment Data**.

The ASA refreshes the Cisco TrustSec environment data from the ISE and resets the reconcile timer to the configured default value.

Configuring the Security Policy

You can incorporate TrustSec policy in many ASA features. Any feature that uses extended ACLs (unless listed in this chapter as unsupported) can take advantage of TrustSec. You can now add security group arguments to extended ACLs, as well as traditional network-based parameters.

- To configure an extended ACL, see Chapter 19, "Adding an Extended Access Control List."
- To configure security group object groups, which can be used in the ACL, see the "Configuring Local User Groups" section on page 25-7.

For example, an access rule permits or denies traffic on an interface using network information. With TrustSec, you can now control access based on security group. See Chapter 51, "Configuring Access Rules." For example, you could create an access rule for sample_securitygroup1 10.0.0.0 255.0.0.0, meaning the security group could have any IP address on subnet 10.0.0.0/8.

You can configure security policies based on combinations of security group names (servers, users, unmanaged devices, etc.), user-based attributes, and traditional IP-address-based objects (IP address, Active Directory object, and FQDN). Security-group membership can extend beyond roles to include device and location attributes and is independent of user-group membership.

Monitoring the ASA Integrated with Cisco TrustSec

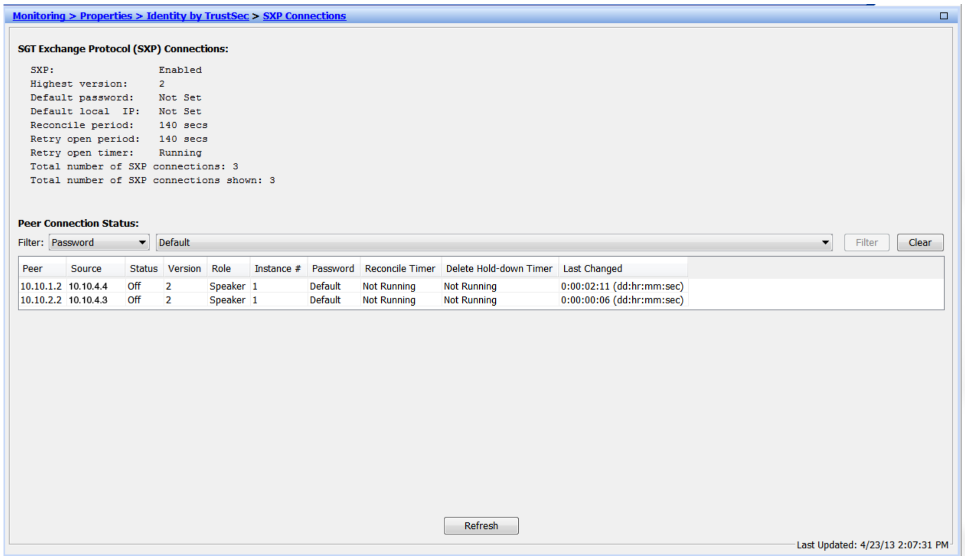
This section contains the following topics:

- Monitoring SXP Connections, page 48-17
- Monitoring Environment Data, page 48-18
- Monitoring Cisco TrustSec IP-SGT Mappings, page 48-19
- Monitoring the PAC File, page 48-20

Monitoring SXP Connections

To verify which SXP connections are up and running, you can view the Security Exchange Protocol monitoring panel in ASDM. This panel displays the SXP connections on the ASA for a particular user context when multi-context mode is used.

In the main ASDM application window, choose **Monitoring** > **Properties** > **Identity By TrustSec** > **SXP Connections**. The following monitoring panel appears.



Monitoring > Properties > Identity by TrustSec > SXP Connections

SGT Exchange Protocol (SXP) Connections:

```
  SXP:                Enabled
  Highest version:    2
  Default password:   Not Set
  Default local  IP:  Not Set
  Reconcile period:   140 secs
  Retry open period:  140 secs
  Retry open timer:   Running
  Total number of SXP connections: 3
  Total number of SXP connections shown: 3
```

Peer Connection Status:

Filter: Password ▾ Default ▾ Filter Clear

Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
10.10.1.2	10.10.4.4	Off	2	Speaker	1	Default	Not Running	Not Running	0:00:02:11 (dd:hr:mm:sec)
10.10.2.2	10.10.4.3	Off	2	Speaker	1	Default	Not Running	Not Running	0:00:00:06 (dd:hr:mm:sec)

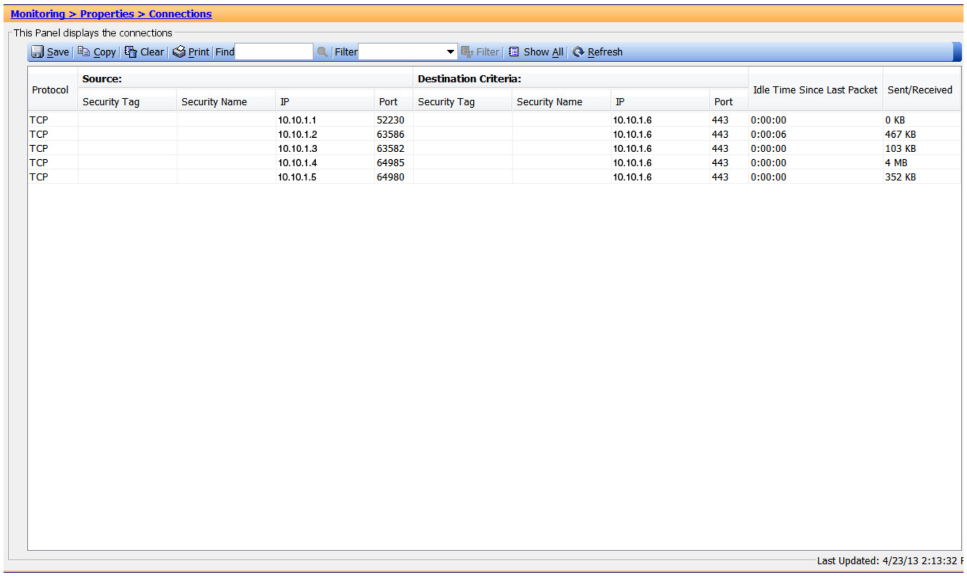
Refresh

Last Updated: 4/23/13 2:07:31 PM

304017

Alternatively, you can view the Connections monitoring panel in ASDM to display all connections configured for the ASA including the SXP connections. In the main ASDM application window, choose **Monitoring** > **Properties** > **Connections**. The following monitoring panel appears.

You can filter the IP-SGT mappings so that you view the data by SGT value, security group name, or IP address.



Monitoring > Properties > Connections

This Panel displays the connections

Save | Copy | Clear | Print | Find | Filter ▾ | Filter | Show All | Refresh

Protocol	Source:				Destination Criteria:				Idle Time Since Last Packet	Sent/Received
	Security Tag	Security Name	IP	Port	Security Tag	Security Name	IP	Port		
TCP			10.10.1.1	52230			10.10.1.6	443	0:00:00	0 KB
TCP			10.10.1.2	63586			10.10.1.6	443	0:00:06	467 KB
TCP			10.10.1.3	63582			10.10.1.6	443	0:00:00	103 KB
TCP			10.10.1.4	64985			10.10.1.6	443	0:00:00	4 MB
TCP			10.10.1.5	64980			10.10.1.6	443	0:00:00	352 KB

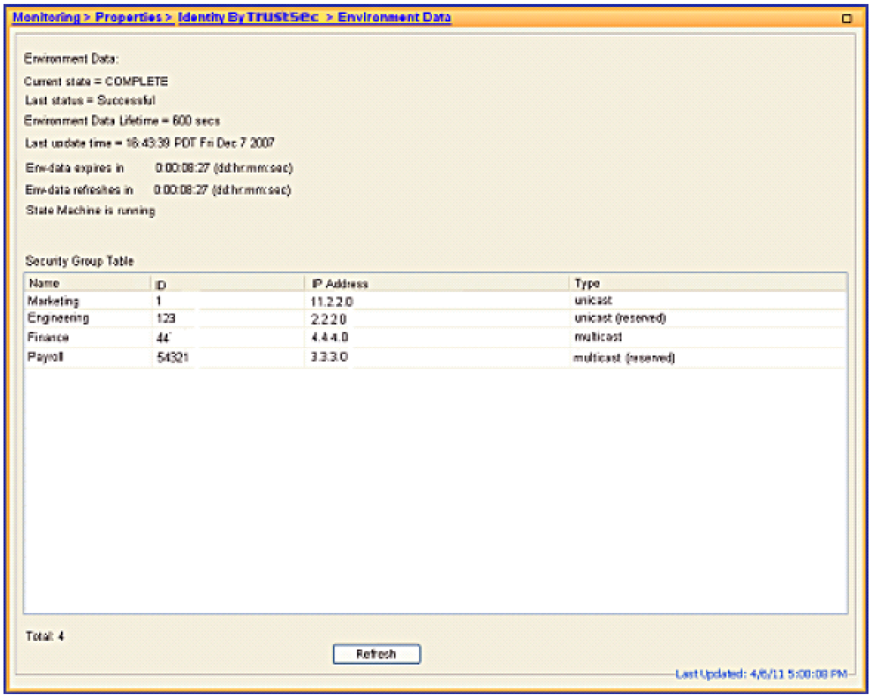
Last Updated: 4/23/13 2:13:32 F

304011

Monitoring Environment Data

To display the Cisco TrustSec environment information contained in security group table on the ASA, you can view the Environment Data monitoring panel in ASDM. The information in this panel includes the expiry timeout and security group name table. The security group table is populated with data from the ISE when you import the PAC file.

In the main ASDM application window, choose **Monitoring** > **Properties** > **Identity By TrustSec** > **Environment Data**. The following monitoring panel appears.



Monitoring > Properties > Identity By TrustSec > Environment Data
Refresh
304012

Environment Data:

Current state = COMPLETE

Last status = Successful

Environment Data Lifetime = 600 secs

Last update time = 16:43:39 PDT Fri Dec 7 2007

Env-data expires in 0:00:08:27 (dd:hr:mm:sec)

Env-data refreshes in 0:00:08:27 (dd:hr:mm:sec)

State Machine is running

Security Group Table

Name	ID	IP Address	Type
Marketing	1	11.2.2.0	unicast
Engineering	123	2.2.2.0	unicast (reserved)
Finance	44	4.4.4.0	multicast
Payroll	54321	3.3.3.0	multicast (reserved)

Total: 4

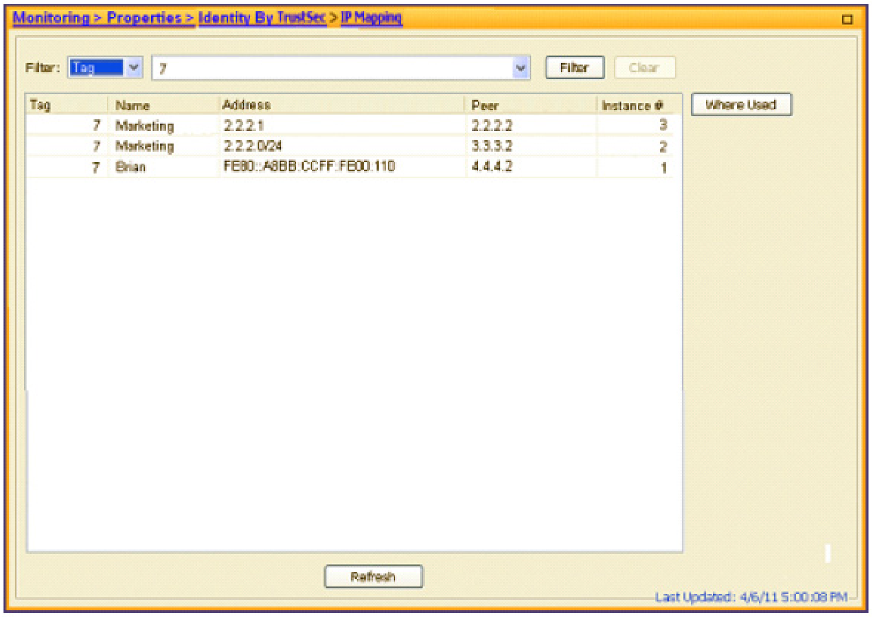
Last Updated: 4/6/11 5:00:08 PM

Monitoring Cisco TrustSec IP-SGT Mappings

To display the active IP-SGT mappings on the ASA consolidated from SXP, you can view the IP Mappings monitoring panel in ASDM.

In the main ASDM application window, choose **Monitoring** > **Properties** > **Identity By TrustSec** > **IP Mapping**. The following monitoring panel appears. You can filter the IP-SGT mappings so that you view the data by SGT value, security group name, or IP address.

Tip: Click **Where Used** to display where the selected security group object is used in an access list or nested in another security group object.



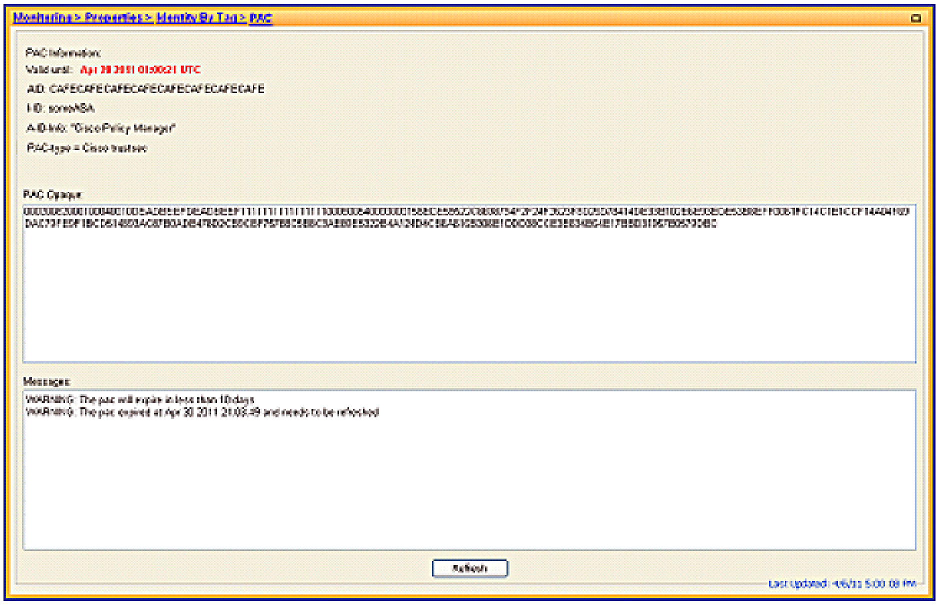
Monitoring > Properties > Identity By TrustSec > IP Mapping
Filter: Tag
7
Filter
Clear
Where Used
Refresh
Last Updated: 4/6/11 5:00:08 PM
304013

Tag	Name	Address	Peer	Instance #
7	Marketing	2.2.2.1	2.2.2.2	3
7	Marketing	2.2.2.0/24	3.3.3.2	2
7	Brian	FE80::A8BB:CCFF:FE00:110	4.4.4.2	1

Monitoring the PAC File

To display the active PAC file imported into the ASA, you can view the PAC File monitoring panel in ASDM.

In the main ASDM application window, choose **Monitoring** > **Properties** > **Identity By TrustSec** > **PAC**. The following monitoring panel appears.



Monitoring > Properties > Identity By Tag > PAC
Refresh
Last updated: 4/6/11 5:00:08 PM
304014

PAC Information:
Valid until: Apr 30 2011 01:00:21 UTC
AID: CAFECAFECAFECAFECAFECAFECAFECAFE
I-ID: someASA
A-ID-Info: "Cisco Policy Manager"
PAC-type = Cisco trustsec

PAC Opaque:

[illegible]

Messages:

WARNING: The pac will expire in less than 10 days
WARNING: The pac expired at Apr 30 2011 21:03:49 and needs to be refreshed

Feature History for the ASA-Cisco TrustSec Integration

Table 48-3 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 48-3 Feature History for the ASA-Cisco TrustSec Integration

Feature Name	Platform Releases	Feature Information
Cisco TrustSec Integration	9.0(1)	Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions. In this release, the ASA integrates with Cisco TrustSec to provide security group based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses. The ASA can utilize the Cisco TrustSec solution for other types of security group based policies, such as application inspection; for example, you can configure a class map containing an access policy based on a security group. We introduced or modified the following screens: Configuration > Firewall > Identity By TrustSec Configuration > Firewall > Objects > Security Groups Object Groups Configuration > Firewall > Access Rules > Add Access Rules Monitoring > Properties > Identity By Tag