

Configure Secure Firewall ASA Devices

- Update ASA connection credentials in Security Cloud Control Firewall Management, on page 1
- ASA interface configuration, on page 2
- ASA system settings policy in Security Cloud Control Firewall Management, on page 15
- ASA routing in Security Cloud Control Firewall Management, on page 26
- API tokens, on page 29
- Manage ASA certificates, on page 30
- ASA file management, on page 38
- Managing ASAs with pre-existing High Availability configuration, on page 42
- Manage ASA configuration files, on page 43
- About System Log Activity , on page 43
- Configure DNS on ASA, on page 44
- ASA command line interface, on page 45
- Network Address Translation, on page 52
- Order of processing NAT rules, on page 53
- Network Address Translation wizard, on page 54
- Common use cases for NAT, on page 55
- Manage security policies in Security Cloud Control Firewall Management, on page 65
- Manage ASA network security policy, on page 65
- Compare ASA network policies, on page 76
- Hit rates, on page 76
- Search and filter ASA network rules in the access list , on page 77
- Shadowed rules, on page 79

Update ASA connection credentials in Security Cloud Control Firewall Management

In the process of onboarding an ASA, you entered the username and password Security Cloud Control Firewall Management must use to connect to the device. If those credentials are changed on the device, use the **Update Credentials** device action to update those credentials on Security Cloud Control Firewall Management as well. This feature allows you to update the credentials on Security Cloud Control Firewall Management without having to re-onboard the device. The username and password combination you switch to must already exist on the ASA or Authentication, Authorization, and Accounting (AAA) server for that user. This process

only affects the Security Cloud Control Firewall Management database; no changes to the ASA configuration are made when using the Update Credentials feature.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab and then click **ASA**.

Step 3 Select the ASAs whose connection credentials it is you want to update. You can update the credentials on one or multiple ASAs at once.

Step 4 In the **Device Actions** pane, click **Update Credentials**.

Step 5 Select the Cloud Connector or the Secure Device Connector (SDC) you use to connect the ASA(s) to Security Cloud Control.

Step 6 Enter the new username and password you want to use to connect to the ASAs.

Step 7 After the credentials are changed, Security Cloud Control syncs the device.

Note
If Security Cloud Control Firewall Management fails to sync the device, the connectivity status in Security Cloud Control Firewall Management may show "Invalid Credentials." If that's the case, you may have tried to use an invalid username and password combination. Make sure the credentials you want to use are stored on your ASA or AAA server, and try again.

Move an ASA from one SDC to Another

Procedure

Step 1 In the left pane, click **Security Devices**

Step 2 In the left pane, click **Inventory**.

Step 3 Select the ASAs you want to move to the other SDC.

Step 4 In the Device Actions pane, click **Update Credentials**.

Step 5 Click the Secure Device Connector button and select the SDC you want to move the device to.

Step 6 Enter the administrator username and password you used to onboard the ASA, and click Update. You do not have to deploy these changes to the device.

ASA interface configuration

Security Cloud Control Firewall Management simplifies ASA interface configuration by providing a user-friendly interface that eliminates the need to use the command line interface. You have complete control over configuring the ASA's physical interfaces, subinterfaces, and EtherChannels. Moreover, you can also view Virtual Tunnel Interfaces that are created during route-based site-to-site VPN, but they are read-only.

You can use Security Cloud Control Firewall Management to configure and edit data interfaces or the management/diagnostic interface on an ASA device.

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for traffic to pass through it. If the interface is a member of a bridge group, naming the interface is sufficient. If the interface is a bridge virtual interface (BVI), you need to assign the BVI an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, or edit an interface, by selecting the interface row and clicking **Edit** in the Actions pane. The list shows the interface characteristics based on your configuration. Expand an interface row to see subinterfaces or bridge group member.

Management interface

You can manage the ASA by connecting to:

- Any through-traffic interface
- A dedicated Management Slot/Port interface (if available for your model)

Use MTU settings

The MTU specifies the maximum frame payload size that the device can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Read-only support for Virtual Tunnel Interface (VTI)

Configuring a route based site-to-site VPN tunnel between two ASA devices creates a Virtual Tunnel Interface (VTI) between the devices. Devices with configured VTI tunnels can be onboarded to Security Cloud Control Firewall Management, which discovers and lists them on the **ASA Interfaces** page but doesn't support their management.

Configure an ASA Physical Interface

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **ASA** tab.

Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 5 Click a physical interface that you want to configure, and click **Edit**.

The **Editing Physical Interface** dialog box appears.

Step 6 In the **Logical Name** field, enter a name for the interface.

Step 7 Continue with one of the following procedures:

- Configure IPv4 Addressing for the Physical Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA Physical Interface, on page 5 if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv4 Addressing for ASA Physical Interface

Procedure

Step 1 In the **Edit Physical Interface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
  - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

    For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

  DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

  You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Addressing for ASA Physical Interface, on page 5 if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv6 Addressing for ASA Physical Interface

Procedure

Step 1 In the **Editing Physical Interface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note
  Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

- **Address Auto Configuration**:

  Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

  Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

  You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

  Note
  A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.
- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.
- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA Physical Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure Advanced ASA Physical Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

Step 1 In the **Editing Physical Interface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- **Management Only**: Enable to make a data interface management only.

A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **Duplex and Speed (Mbps)**: The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read Limitations for Interface Configuration.
  - **Duplex**: Choose Auto, Half, or Full. Auto is the default when the interface supports it.
  - **Speed**: Choose Auto to have the interface negotiate the speed (this is the default), or pick a specific speed: 10, 100, 1000, 10000 Mbps. You can also select these special options:
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.
- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Interface.

Step 4 Click **Save**.

Enable the ASA Physical Interface

Procedure

Step 1 Select the physical interface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Review and deploy the changes you made.

Add an ASA VLAN Subinterface

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

- Configure ASA VLAN Subinterfaces

  Configure IPv4 Addressing for ASA Subinterface, on page 9
- Configure IPv6 Addressing for ASA Subinterface, on page 9
- Configure Advanced ASA Subinterface Options, on page 11
- Enable the Subinterface, on page 12

Configure ASA VLAN Subinterfaces

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **ASA** tab.

Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 5 You can add a subinterface using one of the following methods:

- Choose  > **Subinterface**
- Click a physical interface that you want to configure and in the **Actions** pane on the right, click **New Subinterface**.

Step 6 In the **VLAN ID** field, enter the VLAN ID between 1 and 4094.

Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.

Step 7 In the **Subinterface ID** field, enter the subinterface ID as an integer between 1 and 4294967293.

The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.

Step 8 Continue with one of the following procedures:

- Configure IPv4 Address for the subinterface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Address for the subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure IPv4 Addressing for ASA Subinterface

Procedure

Step 1 In the **Creating Subinterface** dialog box, configure the following in the **IPv4 Address** tab:

- **Type**: You can use either static IP addressing or DHCP for the interface.

  Static - Choose this option if you want to assign an address that should not change.

  - **IP Address and Subnet Mask**: Enter the interface's IP address and the subnet mask for the network attached to the interface.
  - **Standby IP Address**: If you configured high availability and are monitoring this interface for HA, also configure a standby IP address on the same subnet. This interface on the standby device uses the standby address.

    For each interface, set a standby IP address. Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state.

  DHCP: Choose this option if the address should be obtained from the DHCP server on the network.

  You can check the **Obtain Default Route** check box to get the default route from the DHCP server. You would normally check this option.

Step 2 Click **Save** if you are done or continue with one of these procedures.

- Configure IPv6 Address for the subinterface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the subinterface.

Configure IPv6 Addressing for ASA Subinterface

Procedure

Step 1 In the **Creating Subinterface** dialog box, click the **IPv6 Address** tab.

Step 2 Configure the following:

- **State**: To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

  Note
  Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

- **Address Auto Configuration**:

  Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

  Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

- **Suppress RA**: Check this box if you want to suppress router advertisements. The device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

  You might want to suppress these messages on any interface for which you do not want the device to supply the IPv6 prefix (for example, the outside interface).

- **DAD Attempts** How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **Link-Local Address**: If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

  Note
  A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

- **Standby Link-Local Address**: Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other device, to which this interface is connected.

- **Static Address/Prefix**: If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. You can add another static address.
- **Standby IP Address**: If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 3 Click **Save** if you are done or continue with one of these procedures.

- Configure Advanced ASA subinterface. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the subinterface, and you don't want to continue advanced subinterface options, continue to Enable the Subinterface.

Configure Advanced ASA Subinterface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Procedure

Step 1 In the **Creating Subinterface** dialog box, click the **Advanced** tab.

Step 2 Configure the following advanced settings:

- **HA Monitoring**: Enable to include the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- **Management Only**: Enable to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- **MTU**: The default MTU is 1500 bytes. You can specify a value from 64 - 9198. Set a high value if you typically see jumbo frames on your network.
- **DAD Attempts**: How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation

messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- **MAC Address**: The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)
- **Standby MAC Address**: For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 3 If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Subinterface.

Step 4 Click **Save**.

Enable the Subinterface

Procedure

Step 1 Select the subinterface you want to enable.

Step 2 Move the **State** slider at the top right of the window associated with the interface's logical name.

Step 3 Review and deploy the changes you made.

Remove ASA Subinterface

Use the following procedure to remove an subinterface from ASA.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **ASA** tab.

Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, expand the physical interface linked with the subinterface you want to delete and then select that specific subinterface.

Step 6 In the **Actions** pane located to the right, click **Remove**.

Step 7 Confirm you want to delete the EtherChannel interface and click **Delete**.

Step 8 Review and deploy the changes you made.

About ASA EtherChannel Interfaces

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

See the **EtherChannel and Redundant Interfaces** chapter of ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X, Y for more information on ASA EtherChannel interfaces.

Configure ASA EtherChannel

Use this procedure to add a new EtherChannel interface to an ASA.

Before you begin

To configure EtherChannel on ASA interface, the following prerequisites must be met:

- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface, except for the Secure Firewall 3100, which supports different interface capacities as long as the speed is set to Detect SFP; in this case, the lowest common speed is used.
- You cannot add a physical interface to the channel group if you configured a name for it. You must first remove the name.
- You cannot add an interface part of another EtherChannel interface group, Switchport interfaces, and interfaces with subinterfaces.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **ASA** tab.

Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 5 Choose  > **EtherChannel Interface**.

Step 6 In the **Logical Name** field, provide a name for the EtherChannel interface.

Step 7 In the **EtherChannel ID**, enter an integer between 1 and 8.

Step 8 Click the drop-down button for **Link Aggregation Control Protocol** and select one of the two options:

- **Active** —Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On**— The EtherChannel is always on, and LACP is not used. An **on** EtherChannel can only establish a connection with another EtherChannel that is also configured to be **on**.

Step 9 Search for and select the interfaces you want to include in the EtherChannel as members. You **must** include at least one interface.

Warning
If you add an EtherChannel interface as a member and it already has an IP address configured, Security Cloud Control removes the IP address of the member.

Step 10 Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.

- Configure IPv4 Addressing for ASA EtherChannel Interface if you intend to assign an IPv4 address to this interface.
- Configure IPv6 Addressing for ASA EtherChannel Interface if you intend to assign an IPv6 address to this interface.
- Configure Advanced ASA EtherChannel Interface Options. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 11 Move the **State** slider at the top right of the window to enable the EtherChannel interface.

Step 12 Click **Save**.

Step 13 Review and deploy the changes you made.

Edit ASA EtherChannel

Use this procedure to edit an existing EtherChannel on ASA.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 In the left pane, click **Inventory**.

Step 3 Click the **ASA** tab.

Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, select the EtherChannel interface you want to edit.

Step 6 In the **Actions** pane located to the right, click **Edit**.

Step 7 Modify the values you want and click **Save**.

Step 8 Review and deploy the changes you made.

Remove ASA EtherChannel Interface

Use the following procedure to remove an EtherChannel interface from ASA.

Procedure

Step 1 In the left pane, click **Security Devices**.
Step 2 In the left pane, click **Inventory**.
Step 3 Click the **ASA** tab.
Step 4 Select the device you want to modify, and in the **Management** pane on the right, click **Interfaces**.
Step 5 On the **Interfaces** page, select the EtherChannel interface you want to delete.
Step 6 In the **Actions** pane located to the right, click **Remove**.
Step 7 Confirm you want to delete the EtherChannel interface and click **Delete**.
Step 8 Review and deploy the changes you made.

ASA system settings policy in Security Cloud Control Firewall Management

Introduction to ASA system settings policy

Manage your ASA device's operations and functionalities using a System Settings policy. This policy includes essential configurations like domain name services, enabling the secure copy server, message logging, and permitting VPN traffic without checking ACLs. By setting up a policy, you can ensure that your device is properly configured to maintain a secure network environment.

When configuring an ASA device, it's important to note that you have the option to manage multiple devices' settings with a shared system settings policy, or you can individually edit the settings for any single device.

Shared system settings policy

A shared system settings policy applies to multiple ASA devices in your network. It makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes made to a parameter of a shared policy affect the other ASA devices that use the policy.

Choose **Policies** > **ASA System SettingsPolicies** > **ASA** > **System Settings**. See Create an ASA Shared System Settings Policy, on page 15.

You can also modify the device-specific system settings specific to a single ASA device to override the shared system settings policy values. Choose **InventorySecurity Devices** > **ASA device** > **Management** > **Settings**. See Configure or Modify Device Specific System Settings, on page 23.

Create an ASA Shared System Settings Policy

Use this section to create a new shared system settings policy for ASA devices.

Procedure

Step 1 Choose **Policies** > **ASA System Settings**.

Step 2 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 3 Click .

Step 4 In the **Name** field, enter a name for the policy and click **Save**.

Step 5 In the edit ASA shared system settings page, configure the parameters you want:

- Configure Basic DNS Settings, on page 16
- Configure HTTP Settings, on page 17
- Set the Date and Time Using an NTP Server, on page 18
- Configure SSH Access, on page 19
- Configure System Logging, on page 20
- Enable Sysopt Settings, on page 22

Note

- An orange dot () on the corresponding parameter highlights unsaved changes.
- The denied symbol () highlights parameters that use existing local values from the device.

Configure Basic DNS Settings

You need to configure a DNS server so that the ASA can resolve host names to IP addresses. You also must configure a DNS server to use fully qualified domain names (FQDN) network objects in access rules.

Procedure

Step 1 In the edit ASA system settings page, click **DNS** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 In the **DNS** section, click  to configure servers.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify DNS server's IP address.
- **Interface Name**: Specify the interface where the DNS lookup should be enabled.

Note
Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

Step 4 Click **Save**.

Step 5 In the **Domain name** field, specify the domain name for the ASA.

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Step 6 In the **DNS Lookup** section, click + and specify the interface name.

If you do not enable DNS lookup on an interface, then the ASA will not communicate with the DNS server on that interface. Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

Note
To remove a configured interface, you can click the delete icon under **Actions**.

Step 7 Click **Save**.

Configure HTTP Settings

To access the ASA interface for management access, you must specify the addresses of all hosts/networks which are allowed to access the ASA using HTTP. If you configure HTTP redirect to redirect HTTP connections to HTTPS automatically, you must enable an access rule to allow HTTP; otherwise, the interface cannot listen to the HTTP port.

Procedure

Step 1 In the edit ASA system settings page, click **HTTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4 In the **Port Number** field, set the port number. The port identifies the port from which the interface redirects HTTP connections.

Warning
If you change the HTTP port on your device, it may cause some problems with its connection to Security Cloud Control. It's important to remember this if you plan to alter any settings related to your device's network connection.

Step 5 Click  to add HTTP information.

- **Interface**: Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using HTTP.
- **Netmask**: Specify the subnet mask for the network.

Note
To remove a host, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Set the Date and Time Using an NTP Server

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Time derived from an NTP server overrides any time set manually.

The ASA supports NTPv4.

Procedure

Step 1 In the edit ASA system settings page, click **NTP** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Click  to add NTP server details.

- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the NTP server's IP address.

  You cannot enter a hostname for the server; the ASA does not support DNS lookup for the NTP server.

- **Key Id**: Enter a number between 1 and 4294967295.

  This setting specifies the key ID for this authentication key, which enables you to use authentication to communicate with the NTP server. The NTP server packets must also use this key ID.

- **Interface Name**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.

  NTP uses an algorithm to determine which server is the most accurate and synchronizes to it. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one.

- **Prefer**: (optional) Check the **Preferred** check box to set this server as a preferred server.

Note
To remove an NTP server, you can click the delete icon under **Actions**.

Step 4 Click **Save**.

Configure SSH Access

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

Procedure

Step 1 In the edit ASA settings policy page, click **SSH** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Enable Scopy SSH** (secure copy SSH).

Step 4 In the **Timeout in Minutes** field, set the timeout from 1 to 60 minutes. The default is 5 minutes. The default duration is too short in most cases, and should be increased until all pre-production testing and troubleshooting have been completed.

Step 5 Click  and configure the following:

- **Interface**: Specify the interface name. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the addresses of all hosts/networks that can access the ASA using SSH.
- **Netmask**: Specify the subnet mask for the network.

Note
To remove SSH details, you can click the delete icon under **Actions**.

Step 6 Click **Save**.

Configure System Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Security Levels

The following table lists the syslog message severity levels.

Table 1: Syslog Message Severity Levels

Level Number	Security Level	Description
0	**emergencies**	System is unusable
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only. Log at this level only temporarily, when debugging issues. This log level can potentially generate so many messages that system performance can be affected.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

Procedure

Step 1 In the edit ASA system settings page, click **Syslog** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Configure the following:

- **Logging Enabled**: Enable secure logging.
- **Timestamp Enabled**: Enable to include the date and time in syslog messages.
- **Permit host down**: (Optional) Disable the feature to block new connections when a TCP-connected syslog server is down.
- **Buffer Size**: Specify the size of the internal log buffer. The allowed range is 4096 to 1048576 bytes.
- **Buffered Logging Level**: Specify which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location.
- **Console Logging Level**: Specify which syslog messages should be sent to the console port.
- **Trap Logging Level**: Specify which syslog messages should be sent to the syslog server.

Step 4 Click  to add Syslog server details.

- **Interface Name**: Specify the interface name on which the syslog server resides. Ensure the interface name specified here is the same on the ASA devices associated with this shared system settings policy.
- **IP Version**: Select the IP address version you want to use.
- **IP Address**: Specify the IP address of the syslog server.
- **Protocol**: Choose the protocol (**TCP** or **UDP**) the ASA should use to send syslog messages to the syslog server.
  - **Port**: Specify the port that the syslog server listens to for syslog messages. The allowed TCP port range is 1 to 65535, and the UDP port range is 1025 to 65535.
  - **Log messages in Cisco EMBLEM format (UDP only)**: Enables EMBLEM format logging for the syslog server with UDP only.
  - **Enable secure syslog using SSL?**: Specifies that the connection to the remote logging host should use SSL/TLS for TCP only.
- **Reference Identity**: Specify the reference identity type to enable RFC 6125 reference identity checks on the certificate based on the previously configured reference identity object. See Configure Reference Identities for details on the reference identity object.

Note
To remove a Syslog server, you can click the delete icon under **Actions**.

Step 5 Click **Save**.

Enable Sysopt Settings

The crypto map ACL bound to the outgoing interface either permits or denies IPsec packets through the VPN tunnel. IPsec authenticates and deciphers packets that arrive from an IPsec tunnel, and subjects them to evaluation against the ACL associated with the tunnel.

ACLs define which IP traffic to protect. For example, you can create ACLs to protect all IP traffic between two subnets or two hosts.

Procedure

Step 1 In the edit ASA system settings page, click **Sysopt** in the left pane.

Step 2 Uncheck the **Retain existing values** checkbox to configure the values for the shared ASA system settings policy.

Important
If the **Retain existing values** check box is selected, you can't configure the values as the fields are hidden. Security Cloud Control uses the existing local values of the ASA device for this setting and doesn't inherit from the shared policy.

Step 3 Enable **Allow VPN traffic to bypass interface access lists** bypasses the ACL inspection.

Step 4 Click **Save**.

Assign a Policy from the Shared System Settings Page

After configuring a shared system settings policy, assign onboarded ASA devices and deploy the settings to the devices for the changes to take effect. Any change made to the policy affects the devices that are associated with the policy.

You can also assign a policy from the device-specific settings page.

Note You can associate an ASA device to only one shared system settings policy.

Procedure

Step 1 Choose **Policies** > **ASA System Settings**.

Step 2 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 3 Select a shared policy and click **Edit**.

Step 4 Click the filter appearing beside the policy name to assign devices.

Step 5 Select the ASA devices you want to associate with the selected policy and click **OK**.

Note
The checkboxes are ticked for devices that are already associated with the selected policy.

If you see a red icon , it means that an error has occurred while applying the shared system settings policy to your devices. To troubleshoot the issue, click the policy on the **ASA System Settings** page and in the **Error Detected** pane, click the **Device Workflows** to get more information.

Configure or Modify Device Specific System Settings

A device-specific system settings are existing values specific to an ASA device that can be modified using Security Cloud Control. You can override the shared system settings policy values with existing device-specific values for parameters you want.

This topic describes configuring an onboarded ASA device's system settings.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab.

Step 4 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific system settings of the selected ASA device.

Note
If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. You can also assign a policy from the device-specific settings page. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 5 Configure or modify the values of the system settings you want and click **Save**.

Note
The field descriptions for a shared and device-specific system settings remain the same. You can click the corresponding link below for more information.

- Configure Basic DNS Settings, on page 16
- Configure HTTP Settings, on page 17
- Set the Date and Time Using an NTP Server, on page 18
- Configure SSH Access, on page 19
- Configure System Logging, on page 20
- Enable Sysopt Settings, on page 22

You can click **Return to Security Devices** to navigate to the **Security Devices** page.

Step 6 Click **Save** after making the changes.

Note

An orange dot ( ) on the corresponding parameter highlights unsaved changes.

Assign a Policy from Device-Specific Settings Page

You can also assign a policy from the device-specific settings page of an onboarded ASA device.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab.

Step 4 Select the ASA device you want and in the **Management** pane on the right, click **Settings**.

You will see the device-specific settings of the selected ASA device.

Note
If the selected device is assigned with a shared system settings policy, the **Parent Policy** provides a link to open the policy. Select the ASA devices you want to associate with the selected policy and click **OK**

Step 5 Click the **Parent Policy** button to assign a shared system settings policy.

Step 6 Select a policy and click **Apply**.

Auto Assignment of ASA Devices to a Shared System Settings Policy

When onboarding a new ASA device, or checking for changes or handing out-of-band changes for existing devices, Security Cloud Control verifies whether:

- The device-specific settings match a pre-existing shared system settings policy. If there is a match, the device gets assigned to the shared system settings policy.
- The device-specific settings of the onboarded devices match each other. If they do, a new shared system settings policy gets created automatically, and devices with the same local settings are assigned to this shared policy.

Note You can rename the Shared Settings policy whether it was created by the user or the system.

Filter ASA Shared System Settings Policy

If you're searching for specific shared system settings policies on the ASA System Setting page, you can use filters based on issues and usage to narrow down your search and find what you're looking for more easily.

Choose **Policies** > **ASA System Settings**Click **Policies** > **ASA** > **System Settings** >  .

- **Issues**:
  - **Issue Detected**: Displays only the policies that have issues when applying devices to them.
  - **No issue**: Displays only the policies that are successfully applied to devices.
- **Usage**:
  - **In Use**: Displays policies that have are assigned to devices.
  - **Unused**: Displays policies that have not been assigned to any devices yet.

Disassociate Devices from Shared System Settings Policy

If an ASA device is no longer needed in the shared system settings policy, you can easily dissociate it. The device detaches from the policy when:

- Changes are made to the device-specific settings, where the corresponding setting on the shared policy is not configured to retain existing values from the device.
- Devices are detached manually from the shared system settings policy.
- Shared system settings policy is deleted from Security Cloud Control. However, this doesn't delete the device. See Delete Shared Settings Policy, on page 25.

Procedure

Step 1 Choose **Policies** > **ASA System Settings**.

Step 2 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 3 Select a shared policy and click **Edit**.

Step 4 Click the filter appearing beside the policy name to detach devices.

Step 5 Uncheck the devices you want to detach from the selected shared system settings policy and click **OK**.

Note
The changes are saved automatically and don't require any manual deployment.

Delete Shared Settings Policy

If you want to remove some shared settings policies, you have the option to select one or more of them and delete them. However, it's important to note that you can only delete them if they haven't been applied or committed to any devices yet.

Before you begin

Ensure the devices are dissociated from the shared settings policy you wish to delete. See Disassociate Devices from Shared System Settings Policy for more information.

Procedure

Step 1 In the left pane, choose **Policies** > **ASA System Settings**.

Step 2 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 3 Select a shared policy and click **Delete**.

Step 4 Click **OK** to confirm your action.

Note
If you delete an ASA from Security Cloud Control, the device-specific settings and configurations will also be deleted, and the device references will be removed from the shared settings policy.

ASA routing in Security Cloud Control Firewall Management

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which include route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with various information. Destination or next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the next hop on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables can also include other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of various messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message that is sent between routers, informs other routers of the state of the sender links. Link information can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

About ASA Static Route

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

For general information on how ASA routing concepts and CLI commands, see the following documents:

- *Static and Default Routes* chapter from ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, X,Y.
- *Static and Default Routes* chapter from CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, X,Y.

Default Route

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

You should always define a default route.

Static Route

You might want to use static routes in the following cases:

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.
- You are using a feature that does not support dynamic routing protocols.

Static Route Tracking

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements static route tracking by associating a static route with a monitoring target host on the destination network that the ASA monitors using ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address.
- The next hop gateway address (if you are concerned about the availability of the gateway).
- A server on the target network, such as a syslog server, that the ASA needs to communicate with.
- A persistent network object on the destination network.

Configure ASA Static Route

A static route defines where to send traffic for specific destination networks.

This section describes the steps to add a static route to an ASA device.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab.

Step 4 Select a device you want to configure a static route.

Step 5 In the **Management** pane on the right, click **Routing**.

Step 6 Click  to add a static route.

Step 7 You can enter a **Description** for the route.

Step 8 Select whether the route is for an **IPv4** or **IPv6** address.

Step 9 Configure the route properties:

- **Interface**: Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.

  You can use a **Null0** route to forward unwanted or undesirable traffic so the traffic is dropped. Static Null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops.

  The ASA CLI accepts both Null0 or null0 strings.
- **Gateway IP**: (Not applicable to a **Null0** route) Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
- **Metric**: The administrative distance for the route, between 1 and 254. The default for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

  Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.
- **Destination IP**: Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.
- **Destination Mask** (only for IPv4 addressing): Enter the subnet mask for the destination IP.
- **Tracking** (only for IPv4 addressing): Enter a unique identifier for the route tracking process.

Step 10 Click **Save**.

Edit ASA Static Route

You can edit the static route parameters associated with an ASA device.

Note However, you cannot select a different IP version while modifying the static route. Alternatively, you can create a new static route based on your requirement.

Procedure

Step 1 Select an ASA device you want to edit the static route.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Edit**.

Step 4 Modify the values you want and click **Save**. See Configure ASA Static Route, on page 28 for information on the routing parameters.

Delete a Static Route

Before you begin

Deleting a static route may impact the connectivity to your device's local SDC or Security Cloud Control. Ensure a proper disaster recovery procedure is in place for any connectivity loss.

Procedure

Step 1 Select an ASA device you want to delete.

Step 2 In the **Management** pane on the right, click **Routing**.

Step 3 In the routing listing page, select a route you want to modify and in the **Actions** pane on the right, click **Delete**.

Step 4 Click OK to confirm the changes.

API tokens

Developers use Security Cloud Control API tokens when making Security Cloud Control REST API calls. The API token must be inserted in the REST API authorization header for a call to succeed. API tokens are "long-lived" access tokens which do not expire; however, you can renew and revoke them.

You can generate API tokens from within Security Cloud Control. These tokens are only visible immediately after they're generated and for as long as the General Settings page is open. If you open a different page in Security Cloud Control and return to the General Settings page, the token is no longer visible, although it is clear that a token has been issued.

Individual users can create their own tokens for a particular tenant. One user cannot generate a token on behalf of another. Tokens are specific to an account-tenant pair and cannot be used for other user-tenant combinations.

API Token Format and Claims

The API token is a JSON Web Token (JWT). To learn more about the JWT token format, read the Introduction to JSON Web Tokens.

The Security Cloud Control API token provides the following set of claims:

- **id** - user/device uid
- **parentId** - tenant uid
- **ver** - the version of the public key (initial version is 0, for example, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - Security Services Exchange subscriptions (optional)
- **client_id** - "**api-client**"
- **jti** - token id

Manage ASA certificates

Digital certificates provide digital identification for authenticating devices and individual users. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. For more information on digital certificates, see the "Digital Certificates" chapter in the "Basic Settings" book of the Cisco ASA Series General Operations ASDM Configuration, X.Y document.

Certificate Authorities (CAs) are trusted authorities that “sign” certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs also issue identity certificates.

- **Identity Certificate** — Identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate. CAs issue identity certificates, which are certificates for specific systems or hosts.
- **Trusted CA Certificate** — Trusted CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. A trusted CA certificate is self-signed and called a root certificate.

The Remote Access VPN uses digital certificates for authenticating secure gateways and AnyConnect clients (endpoints) to establish a secure VPN connection.

For more information, see Remote Access VPN Certificate-Based Authentication.

Guidelines for Certificate Installation

Read the following guidelines for certificate installation on ASA:

- Certificate can be installed on a single or multiple ASA devices simultaneously.
- Only one certificate can be installed at a time.
- Certificate can be installed only on a live ASA device and not on a modal device.

Install ASA Certificates

Note Ensure that the ASA device has no out-of-band changes, and all staged changes have been deployed.

The following lists the digital certificates and formats supported by Security Cloud Control:

- Identity Certificate can be installed using the following methods:
  - PKCS12 file import.
  - Self-Signed certificate
  - Certificate Signing Request (CSR) import.
- Trusted CA Certificate can be installed using PEM or DER format.

Watch the screencast demonstrates the steps for installing certificates on ASA using Security Cloud Control. It also shows steps for modifying, exporting, and deleting installed certificates.

Supported Certificate Formats

- PKCS12: PKCS#12, P12, or PFX format is a binary format for storing the server certificate, any intermediate certificates, and the private key in one encryptable file. PFX files usually have extensions such as **.pfx** and **.p12**.
- PEM: PEM (originally “Privacy Enhanced Mail”) files contain ASCII (or Base64) encoding data and the certificate files can be in .pem, .crt, .cer, or .key formats. They are Base64 encoded ASCII files and contain "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" statements.
- DER: DER (Distinguished Encoding Rules) format is simply a binary form of a certificate instead of the ASCII PEM format. It sometimes has a file extension of **.der**, but it often has a file extension of **.cer**, so the only way to tell the difference between a DER .cer file and a PEM .cer file is to open it in a text editor and look for the BEGIN/END statements. Unlike PEM, DER-encoded files do not contain plain text statements such as -----BEGIN CERTIFICATE-----.

Trustpoints Screen

After onboarding the ASA device into Security Cloud Control, on the **Security Devices** tab, select the ASA device and in the **Management** pane on the left, click **Trustpoints**.

In the **Trustpoints** tab, you'll see the certificates that are already installed on the device.

- The "Installed" status indicates that the corresponding certificate is installed successfully on the device.
- The "Unknown" status indicates that the corresponding certificate doesn't contain any information. You need to remove and upload it again with the correct details. Security Cloud Control discovers all the unknown certificates as trusted CA certificates.
- Click the row that shows "Installed" to view certificate details on the right pane. Click **more** to see additional details of the selected certificate.
- An installed Identity Certificate can be exported in PKCS12 or PEM format and imported into other ASA devices. See Exporting an Identity Certificate.

- Only the advanced settings can be modified on an installed certificate.
  - Click **Edit** to modify the advanced settings.
  - After making the changes, click **Send** to install the updated certificate.

Install an Identity Certificate Using PKCS12

You can select an existing trustpoint object created for PKCS12 format and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the guidelines for certificate installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note
You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

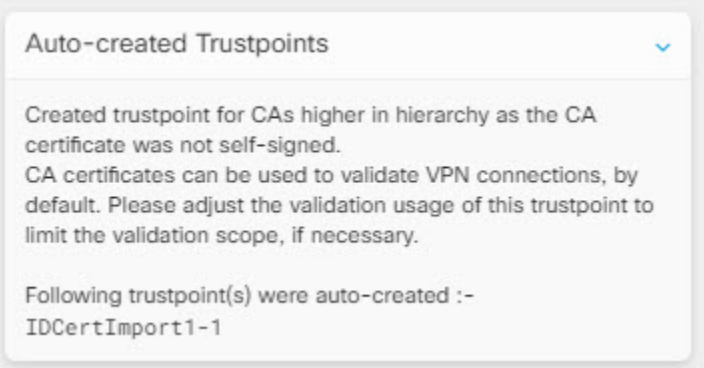
Step 4 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object.
- **Choose** to select Certificate Enrollment Object of the PKCS type.

Step 5 Click **Send**.

This installs the certificate on the ASA device

Note
If you are importing a PKCS12 certificate that has intermediate CAs installed on it, ASA automatically creates and installs trustpoint objects on the device for every intermediate CA certificate that is not installed already. When you click on the identity certificate, you'll see a message on the right pane, as shown in the following example.



Install a Certificate Using Self-Signed Enrollment

You can select an existing trustpoint object created for a self-signed certificate and install it on the ASA device. You can also create a new trustpoint object from the installation wizard and install the certificate on the ASA device.

Before you begin

- Read the guidelines for certificate installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 To install an identity certificate on a single ASA device, do the following:

a) Click the **Devices** tab.
b) Click the **ASA** tab and select an ASA device.
c) In the **Management** pane on the right, click **Trustpoints**.
d) Click **Install**.

Note
You can also install a signed certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 4 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object.
- **Choose** to select a Certificate Enrollment Object of the type Self-Signed..

Step 5 Click **Send**.

For self signed enrollment type trustpoints, the Issuer Common Name status will always be the ASA device since the managed device is acting as its own CA and does not need a CA certificate to generate its own Identity Certificate.

Manage a Certificate Signing Request (CSR)

You must first generate a CSR request and then get this request signed by a trusted Certificate Authority (CA). Then, you can install the signed identity certificate issued by the CA on the ASA device.

- Read the guidelines for certificate installation.
- ASA must be “Synced” state and “Online”.

The following diagram depicts the workflow for generating CSR and installing a certified issued certificate in ASA:

Generate a CSR Request

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select an ASA device.

Step 5 To install an identity certificate on a single ASA device, do the following:

Step 6 Click **Install**.

Step 7 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint CSR object.
- **Choose**to select the CSR request trustpoint that is already created..

Step 8 Click **Send**.

This generates an unsigned Certificate Signing Request (CSR).

Step 9 Click the copy icon copy_icon.png to copy the CSR details. You can also download the CSR request in ".csr" file format.

Step 10 Click **OK**.

Step 11 Submit the certificate signing request (CSR) to the Certificate Authority to sign the certificate.

Install a Signed Identity Certificate Issued by a Certificate Authority

Once the CA issues the signed certificate, install it on the ASA device

Procedure

Step 1 In the **Trustpoint** screen, click the CSR request with the **Status** as "Awaiting Signed Certificate Install" and in the **Actions** pane on the right, click **Install Certified ID Certificate**.

Step 2 Upload the signed certificate received from the CA. You can drag and drop the file or paste its contents in the provided field. The trustpoint commands are generated based on the trustpoint you selected.

Step 3 Click **Send**.

This installs the signed identity certificate to the ASA device. Installing certificates will immediately deploy changes to the device.

Note
You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Install a Trusted CA Certificate in ASA

Before you begin

- Read the guidelines for certificate installation.
- ASA must be “Synced” state and “Online”.

Procedure

Step 1 In the navigation menu, click **Inventory**.

Step 2 In the navigation menu, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select an ASA device.

Step 5 To install an identity certificate on a single ASA device, do the following:

a) Select an ASA device and in the **Management** pane on the right, click **Trustpoints**.

b) Click **Install**.

Note
You can also install a certificate on multiple ASA devices. Select multiple ASA devices and in the **Devices Action** on the right, click **Install Certificate**.

Step 6 From **Select Trustpoint Certificate to Install**, click one of the following:

- **Create** to add a new trustpoint object.
- **Choose**select a Trusted Certificate Authority Object.

Step 7 Click **Send**.

This installs the trusted CA file on the ASA device.

Export an Identity Certificate

You can export and import the keypair and issued certificates associated with a trustpoint in PKCS12 or PEM format. This format is useful to manually duplicate a trustpoint configuration on a different ASA.

Procedure

Step 1 In the navigation menu, click **Inventory**.

Step 2 In the navigation menu, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA**.

Step 5 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 6 Click the identity certificate to export the certificate configuration. Alternatively, you can search for the certificate by entering its name in the search field.

Step 7 In the **Actions** pane on the right, click **Export Certificate**.

Step 8 Choose the certificate format by clicking the **PKCS12 Format** or the **PEM Format**.

Step 9 Enter the encryption passphrase used to encrypt the PKCS12 file for export.

Step 10 Confirm the encryption passphrase.

Step 11 Click **Export** to export the certificate configuration.

An information dialog box appears, informing you that the certificate configuration file has been successfully exported to the location that you specified.

What to do next

If you want to view the downloaded identity certificate, execute the following commands in the directory where the certificate was downloaded:

1. To decode certificate in base64 format:

```
openssl base64 -d -in <file_name>.p12 -out <file_name>_b64.p12
```

2. To view certificate:

```
openssl pkcs12 -in <file_name>_b64.p12 -passin pass:<password>
```

Edit an Installed Certificate

You can modify only the advanced options of the installed certificate.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab.

Step 5 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 6 Click the certificate to modify and in the **Actions** pane on the right, click **Edit**.

Step 7 Modify the required parameters and click **Save**.

Delete an Existing Certificate from ASA

You can delete a certificate one after another. After deleting a certificate, it cannot be restored.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Select the ASA device and in the **Management** on the right, click **Trustpoints**.

Step 4 Click the certificate to be deleted and in the **Actions** pane on the right, click **Remove**.

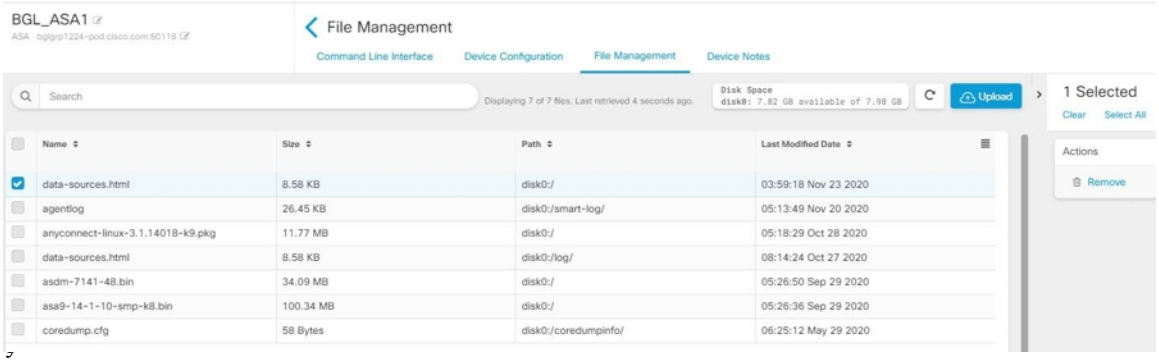
Step 5 Click **OK** to remove the selected certificate.

ASA file management

Security Cloud Control provides the file management tool to help you perform basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space.

Note You cannot manage files present on disk1.

The File Management screen lists all the files present on the device's flash (disk0). On a successful file upload, you can click the refresh icon to see the file. By default, this screen refreshes automatically every 10 minutes. The **Disk Space** field shows the amount of disk space on the disk0



You can upload the AnyConnect image to single or multiple ASA devices. After a successful upload, the AnyConnect image is associated with the RA VPN configuration on the selected ASA devices. This helps you to upload the newly released AnyConnect package to multiple ASA devices simultaneously.

Upload File to the Flash System

Security Cloud Control supports only URL based file upload from the remote server. The supported protocols for uploading the file are HTTP, HTTPS, TFTP, FTP, SMB, or SCP. You can upload any files such as the AnyConnect software images, DAP.xml, data.xml, and host scan image files to a single or multiple ASA device.

Note Security Cloud Control doesn't upload the file to selected ASA devices if the remote server's URL path is invalid or for any issues that may occur. You can navigate to the device **Workflows** for more details.

Suppose the device is configured for High Availability, Security Cloud Control uploads the file to the standby device first, and only after a successful upload, the file is uploaded to the active device. The same behavior applies during the file removal process.

The syntax of supported protocols for uploading the file:

Protocol	Syntax	Example
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	[illegible]
SMB	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/ filename]	scp://rootcisco123@10.10.16.6//root/events_send.py

Before You Begin

- Make sure that the remote server is accessible from the ASA device.
- Make sure that the file is already uploaded to the remote server.
- Make sure that there is a network route from the ASA device to that server.
- If FQDN is used in the URL, make sure that DNS is configured.
- The remote server's URL must be a direct link without prompting for authentication.
- If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Note If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Control does not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

Upload File to a Single ASA Device

Use this procedure to upload a file to a single ASA device.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select an ASA device.

Step 5 In the **Management** pane on the right, click **File Management**. You can view available disk space and the files present on the ASA device.

Step 6 Click the **Upload** button on the right.

Step 7 In the **URL link**, specify the server's path where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:/**DAPFiles/dap.xml" in the field.

Note
You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

Step 8 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled. **Note**: This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA device after a successful upload.

Step 9 Click **Upload**. Security Cloud Control uploads the file to the device.

Step 10 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 5, deploy the new RA VPN configuration to the ASA device.

Upload File to Multiple ASA Devices

Use this procedure to upload a file to multiple ASA devices at the same time.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select multiple ASA devices to perform a bulk upload.

Step 5 In the **Device Actions** pane on the right, click **Upload File**. Note: The **Upload File** link appears if ASA devices are online.

Step 6 In the **URL link**, specify the server's paths where the file is pre-uploaded. The **Destination Path** field shows the name of the file that is being uploaded to the **disk0** directory. If you want to upload the file to a specific

directory within disk0, specify its name in this field. For example, if you're going to upload a dap.xml file to the "DAPFiles" directory, specify "**disk0:**/DAPFiles/dap.xml" in the field.

Note
You can view the directories present in the disk0 folder by executing the **dir** command in the Security Cloud Control ASA CLI interface.

Step 7 If the specified server path points to an AnyConnect file, the **Associate file with RA VPN Configuration** check box is enabled.

Note
This check box is enabled only for an AnyConnect file name that follows the right naming convention, which is 'anyconnect-win-xxx.pkg', 'anyconnect-linux-xxx.pkg', or 'anyconnect-mac-xxx.pkg' format. On selecting this check box, Security Cloud Control associates the AnyConnect file to the RA VPN configuration on the selected ASA devices after a successful upload.

Step 8 Click **Upload**.

Step 9 If you have chosen to associate the AnyConnect package with the RA VPN configuration in step 4, deploy the new RA VPN configuration to ASA devices.

You can view the progress of uploading the file on individual devices. Select the ASA device, and in the **Management** pane on the right, click **File Management**. If the file upload is in progress, wait for the operation to complete.

You don't have to deploy the configuration changes on the device.

Remove Files from ASA

You are not allowed to remove AnyConnect files associated with the RA VPN configuration. You have to disassociate the AnyConnect file from the corresponding RA VPN configuration and then remove the file from the File Management tool.

Note If you upload a file to an ASA that is configured as a peer in a failover, Security Cloud Controldoes not acknowledge the new file for the other peer in the failover pair and the device status changes to **Not Synced**. You must manually deploy changes to **both** devices for Security Cloud Control to recognize the file in both devices.

The remove operation deletes the selected files permanently from the flash memory. A message appears when deleting files asking for confirmation. Use the following procedure to remove files from a selected ASA device:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select an ASA device.

Step 5 In the **Management** pane on the right, click **File Management**.

Step 6 Select the files you want to remove, and under **Actions** on the right, click **Remove**. A maximum of 25 files can be selected. If Security Cloud Control fails to remove some files, you can see the device **Workflows** to determine the removed and retained files.

Step 7 If you have chosen to remove the AnyConnect package, deploy the new RA VPN configuration to the ASA device.

Managing ASAs with pre-existing High Availability configuration

Configuration Changes Made to ASAs in Active-Active Failover Mode

When Security Cloud Control) changes an ASA's running configuration with the one staged on Security Cloud Control, or when it changes the configuration on Security Cloud Control with the one stored on the ASA, it attempts to change only the relevant lines of the configuration file if that aspect of the configuration can be managed by the Security Cloud Control GUI. If the desired configuration change cannot be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file to make the change.

Here are two examples:

- You *can* create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it overwrites the relevant lines of the running configuration file on the ASA when the change occurs.
- You *cannot* create a new ASA user using the Security Cloud Control GUI. If a new user is added to the ASA using the ASA's ASDM or CLI, when that out-of-band change is accepted and Security Cloud Control updates the stored configuration file, Security Cloud Control attempts to overwrite that ASA's entire configuration file staged on Security Cloud Control.

These rules are not followed when the ASA is configured in active-active failover mode. When Security Cloud Control manages an ASA configured in active-active failover mode, Security Cloud Control cannot always deploy all configuration changes from itself to the ASA or read all configuration changes from the ASA into itself. Here are two instances in which this is the case:

- **Changes to an ASA's configuration file made in Security Cloud Control, that Security Cloud Control does not otherwise support in the Security Cloud Control GUI, cannot be deployed to the ASA**. Also, a combination of changes made to the configuration file that Security Cloud Control does not support, along with changes made to the configuration file that Security Cloud Control does support, cannot be deployed to the ASA. In both cases, you receive the error message, "Security Cloud Control does not support replacing full configurations for devices in failover mode at this time. Please click Cancel and apply changes to the device manually." Along with the message in the Security Cloud Control interface, you see a Replace Configuration button that is disabled.
- **Out-of-band changes made to an ASA configured in active-active failover mode will not be rejected by Security Cloud Control**. If you make an out-of-band change to an ASA's running configuration, the ASA gets marked with "Conflict Detected" on the **Security Devices** page. If you review the conflict and

try to reject it, Security Cloud Control blocks that action. You receive the message, "Security Cloud Control does not support rejecting out-of-band changes for this device. Either this device is running an unsupported software version or is a member of a active/active failover pair. Please proceed to accept the out-of-band changes by clicking Continue."



Caution If you find yourself having to accept out-of-band changes from the ASA, any configuration changes staged on Security Cloud Control, but not yet deployed to the ASA, will be overwritten and lost.

Security Cloud Control does support configuration changes made to an ASA in failover mode when those changes are supported by the Security Cloud Control GUI.

Manage ASA configuration files

ASA stores their configurations in a single configuration file. You can view the device configuration file on Security Cloud Control Firewall Management and perform a variety of operations on it depending on the device.

View a Device's Configuration File

The ASA stores the entire configuration in a single configuration file. You can view the configuration file using Security Cloud Control.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the ASA device type tab.

Step 4 Select the device or model whose configuration it is you want to view.

Step 5 In the **Management** pane on the right, click **Configuration**.
The full configuration file is displayed.

About System Log Activity

When you set up a new rule, you can specify how often and at what severity level you want to collect its activity. To do this, you can select the corresponding severity levels and then choose the frequency of data collection. This will ensure that you have the necessary information to monitor and analyze the activity generated by your rules.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

You have the option to adjust the logging interval, which indicates how frequently the log records are updated. This interval is measured in seconds and can be set from 1 to 600. By default, the interval is set to 300 seconds. This interval value is also utilized as a timeout period for removing an inactive flow from the cache that collects drop statistics.

Table 2: Log Rule Activity

Security Level	Description
emergencies	System is unusable.
alert	Immediate action is needed.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notification	Normal but significant conditions.
informational	Informational messages only.
debugging	Debugging messages only.

Configure DNS on ASA

Use this procedure to configure a domain name server (DNS) on each of your ASAs.

Prerequisites

- The ASA must be able to reach the internet.
- Before you begin, gather this information:
  - The name of the ASA interface that can reach the DNS server; for example, inside, outside, or dmz.
  - The IP address of the DNS server your organization uses. If you don't maintain your own DNS server, you can use Cisco Umbrella. The IP address for Cisco Umbrella is 208.67.220.220.

Procedure

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the **ASA** tab and select all the ASAs on which you want to configure DNS.

Step 5 In the Actions pane to the right, select **Command Line Interface**.

Step 6 Click the CLI macro favorites star.

Step 7 Select the **Configure DNS** macro in the Macros panel.

Step 8 Se;ect **>_View Parameters** and in the parameters column, fill in the values for these parameters:

- IF_Name - The name of the ASA interface that can reach the DNS server.
- IP_ADDR - The IP address of the DNS server your organization uses.

Step 9 Click **Send to devices**.

ASA command line interface

You can use the Security Cloud Control Firewall Management command line interface (CLI) for managing or troubleshooting the ASA and other device types.

For more information, see .

Configure ASA Using Security Cloud Control CLI

You can configure an ASA device by running the CLI commands in the CLI interface provided in Security Cloud Control. See ASA command line interface, on page 45.

Add a New Logging Server

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts.

For more information, see the 'Monitoring' section of the 'Logging' chapter in the CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Configure the DNS Server

You need to configure DNS servers so that the ASA can resolve host names to IP addresses. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

For more information, see the 'Basic Settings' chapter of the 'Configure the DNS Server' section in CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide of the ASA version you are running.

Add Static and Default Routes

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing.

For more information, see the 'Static and Default Routes' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

Configure Interfaces

You can configure the management and data interfaces using CLI commands. For more information, see the 'Basic Interface Configuration' chapter of CLI Book1: Cisco ASA Series General Operations CLI Configuration Guide.

ASA Bulk CLI Use Cases

The following cases are possible workflows you may experience when using Security Cloud Control's bulk CLI function for ASA devices.

Show all users in the running configuration of an ASA and then delete one of the users

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the **ASA** tab.

Step 5 Search and filter the device list for the devices from which you want to delete the user and **select** them.

Note
Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, `dir`, `copy`, and `write`.

Step 6 Click **>_Command Line Interface** in the details pane. Security Cloud Control lists the devices you chose in the My List pane. If you decide to send the command to fewer devices, uncheck devices in that list.

Step 7 In the command pane, enter `show run | grep user` and click **Send.** All the lines in the running configuration file that contain the string user will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 8 Click the By Response tab and review the responses to determine which devices have the user that you want to delete.

Step 9 Click the My List tab and select the list of devices from which you want to delete the user.

Step 10 In the command pane, enter the no form of the user command to delete user2 and then click **Send**. For the sake of this example, you are going to delete user2:

```
no user user2 password reallyhardpassword privilege 10
```

Step 11 Look in the history panel for the instance of the `show run | grep user` command, you used to search for the user name. Select that command, look at the list of devices in the Execution list and select **Send**. You should see that the username has been deleted from the devices you specified.

Step 12 If you are satisfied that you have deleted the correct users from the running configuration and that the correct users remain in the running configuration:

a. Select the `no user user2 password reallyhardpassword privilege 10` command from the history pane.

b. Click the **By Device** tab and click **Execute a command on these devices**.

c. In the command pane, click **Clear** to clear the command pane.

d. Enter the command `deploy memory` and click **Send**.

Find all SNMP configurations on selected ASAs

This procedure shows you all the SNMP configuration entries in the running configuration of the ASA.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the **ASA** tab.

Step 5 Filter and search for the devices on which you want to analyze the SNMP configuration in the running configuration and **select** them.

Note
Make sure that the devices you choose are synced. Only the following commands are allowed when the device is not synced: `show`, `ping`, `traceroute`, `vpn-sessiondb`, `changeto`, and `dir`.

Step 6 Click **Command Line Interface** in the details pane. The devices you chose are in the My List pane. If you decide to send the command to fewer devices, uncheck devices in the list.

Step 7 In the command pane, enter `show run | grep snmp` and click **Send.** All the lines in the running configuration file that contain the string snmp will be displayed in the response pane. The Execution tab opens to display the devices on which the command was executed.

Step 8 Review the command output in the response pane.

ASA Command Line Interface Documentation

Security Cloud Control fully supports the ASA command line interface. We provide a terminal-like interface within Security Cloud Control for users to send ASA commands to single devices and multiple devices simultaneously. The ASA command line interface documentation is extensive. Rather than recreating parts of it in the Security Cloud Control documentation, here are pointers to the ASA CLI documentation on Cisco.com.

ASA Command Line Interface Configuration Guides

Starting with ASA version 9.1, the ASA CLI Configuration Guide is broken into three separate books:

- CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide
- CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide
- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide

You can reach the ASA CLI Configuration Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Configure > Configuration Guides.

A Few Specific ASA Command Line Interface Configuration Guide Sections

Filtering show and more Command Output. You can learn about filtering show command output by using regular expressions in CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide under Filter show and more Command Output.

ASA Command Reference

The ASA Command Reference Guide is an alphabetical listing of all the ASA commands and their options. The ASA command reference is not version specific. It is published in four books:

- Cisco ASA Series Command Reference, A - H Commands
- Cisco ASA Series Command Reference, I - R Commands
- Cisco ASA Series Command Reference, S Commands
- Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM

You can reach the ASA Command Reference Guides on Cisco.com by navigating, Support > Products by Category > Security > Firewalls > ASA 5500 > Reference Guides > Command References > ASA Command References.

Manage the Device Configuration

The ASA stores its configuration in a single configuration file. You can view the configuration file on Security Cloud Control and perform a variety of operations on it.

Compare ASA Configurations Using Security Cloud Control

Use this procedure to compare the configurations of two ASAs.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the ASA device or the **Templates** tab to locate the ASA model device.

Step 4 Click the **ASA** tab.

Step 5 Filter your device list for the devices you want to compare.

Step 6 Select two of your ASAs. Their status does not matter. You are comparing the configurations of the ASAs stored on Security Cloud Control.

Step 7 In the Device Actions pane on the right, click **Compare.**

Step 8 In the Comparing Configurations dialog, click **Next** and **Previous** to skip through the differences, highlighted in blue, in the configuration files.

Restore an ASA Configuration

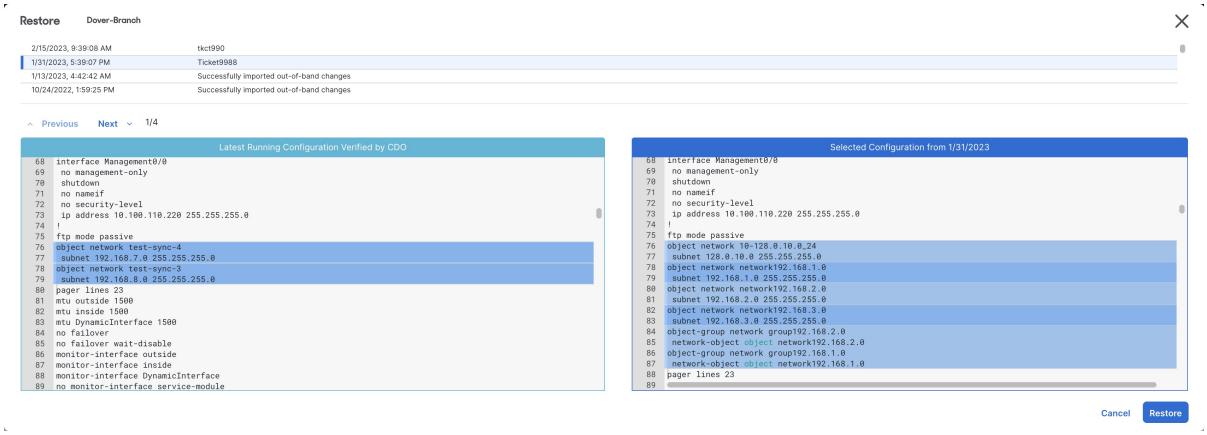
If you make a change to an ASA's configuration, and you want to revert that change, you can restore an ASA's past configuration. This is a convenient way to remove a configuration change that had unexpected or undesired results.

About Restoring an ASA Configuration

Review these notes before restoring a configuration:

- Security Cloud Control compares the configuration you choose to restore with the last known configuration deployed to the ASA, it does not compare the configuration you choose to restore with a configuration that is staged but not deployed to the ASA. If you have any undeployed changes on your ASA and you restore a past configuration, the restore process will overwrite your undeployed changes and you will lose them.
- Before you can restore a past configuration, the ASA can be in a Synced or Not Synced state but if the device is in a Conflict Detected state, the conflict must be resolved before you restore a past configuration.
- Restoring a past configuration overwrites all intermediate deployed configurations changes. For example, restoring the configuration from 1/31/2023 in the list below overwrites the configuration changes made on 2/15/2023.
- Clicking the Next and Previous buttons will move you through the configuration file and highlight the configuration file changes
- If you originally applied a change request label to your configuration changes, that label appears in the Restore Configuration list.

Figure 1: ASA Restore Configuration Screen



How Long are Configuration Changes Kept?

You can restore an ASA configuration that is 1 year old or less. Security Cloud Control restores configuration changes logged in its changelog. The change log records changes every time a configuration change is written to or read from an ASA. Security Cloud Control stores 1 year's worth of changelogs and there is no limitation on the number of the backups made within the previous year.

How to Restore an ASA Configuration

Procedure

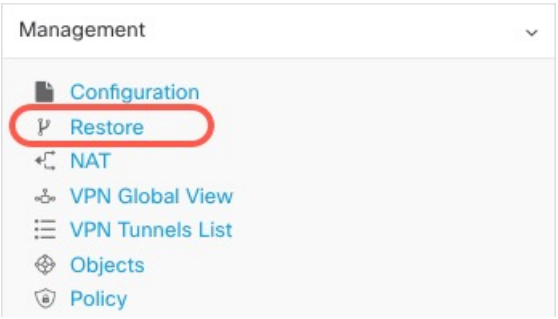
Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

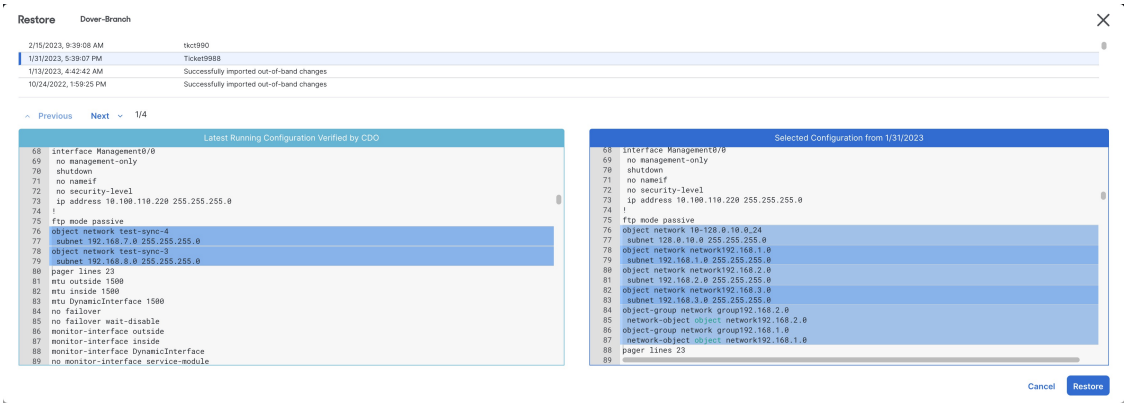
Step 3 Click the ASA tab.

Step 4 Select the ASA whose configuration it is you want to restore.

Step 5 In the **Management** pane, click **Restore.**



Step 6 In the **Restore** page, select the configuration you want to revert to.



For example, in the picture above, the configuration from 1/31/2023 is selected.

Step 7 Compare the "Latest Running Configuration Verified by Security Cloud Control" and the "Selected Configuration from <*date*>" to ensure you want to restore the configuration displayed in the Selected Configuration from <*date*> window. Use the Previous and Next to compare all the changes.

Step 8 Click **Restore,** this stages the configuration in Security Cloud Control. In the **Security Devices** page, you see that the configuration status of the device is now "Not Synced."

Step 9 Click **Deploy Changes...** in the right-hand pane to deploy the changes and sync the ASA.

Troubleshooting

How do I recover changes I lost but wanted to keep?

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the ASA tab.

Step 5 Select the required device.

Step 6 Click **Change Log** in the right pane.

Step 7 Review the changes in the change log. You may be able to reconstruct your lost configurations from those records.

View a Device's Configuration File

The ASA stores the entire configuration in a single configuration file. You can view the configuration file using Security Cloud Control.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the ASA device type tab.

Step 4 Select the device or model whose configuration it is you want to view.

Step 5 In the **Management** pane on the right, click **Configuration**.
The full configuration file is displayed.

Edit a Complete Device Configuration File

For these devices, you can view the device configuration file on Security Cloud Control and perform a variety of operations on it depending on the device.

Currently, only ASA configuration files can be edited directly using Security Cloud Control.



Caution This procedure is for advanced users who are familiar with the syntax of the device's configuration file. This method makes changes directly to copy of the configuration file stored on Security Cloud Control.

Procedure

Step 1 In the left pane, click **Inventory**.
Step 2 In the left pane, click **Security Devices**.
Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
Step 4 Click the **ASA** tab.
Step 5 Select the device whose configuration it is you want to edit.
Step 6 In the **Management** pane on the right, click **Configuration**.
Step 7 In the **Device Configuration** page, click **Edit**.
Step 8 Click the editor button on the right and select the **Default** text editor, **Vim**, or **Emacs** text editors.
Step 9 Edit the file and save the changes.
Step 10 Return to the **Security Devices** page and preview and deploy the change.

Network Address Translation

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private and not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security-Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions-Overlapping IP addresses are not a problem when you use NAT.
- Flexibility-You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only)-If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

You can use Security Cloud Control to create NAT rules for many different use cases. Use the NAT rule wizard or these topics to create different NAT rules:

Order of processing NAT rules

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 3: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Twice NAT (ASA) Manual NAT (FTD)	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1.
Section 2	Network Object NAT (ASA) Auto NAT (FTD)	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addressesâ€”From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, object "Arlington" is assessed before object "Detroit."
Section 3	Twice NAT (ASA) Manual NAT (FTD)	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)

- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 172.16.1.0/24 (dynamic) (object Arlington)

The resultant ordering would be:

- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object Arlington)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 192.168.1.0/24 (dynamic)

Network Address Translation wizard

The Network Address Translation (NAT) wizard helps you create NAT rules on your devices for these types of access:

- **Enable Internet Access for Internal Users**. You may use this NAT rule to allow users on an internal network to reach the internet.
- **Expose an Internal Server to the Internet**. You may use this NAT rule to allow people outside your network to reach an internal web or email server.

Prerequisites to "Enable Internet Access for Internal Users"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- If you want to allow only specific users to reach the internet, you need the subnet addresses for those users.

Prerequisites to "Expose an Internal Server to the Internet"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- The IP address of the server inside your network that you would like to translate to an internet-facing IP address.

- The public IP address you want the server to use.

What to do Next

See Create a NAT Rule by using the NAT Wizard.

Create a NAT Rule by using the NAT Wizard

Before you begin

See Network Address Translation wizard for the prerequisites needed to create NAT rules using the NAT wizard.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Use the filter and search fields to find the device for which you want to create the NAT rule.

Step 6 In the **Management** area of the details panel, click **NAT** NAT.

Step 7 Click + > **NAT Wizard**.

Step 8 Respond to the NAT Wizard questions and follow the on-screen instructions.

- Before you can save the NAT rule, all IP addresses need to be defined as network objects.

Step 9 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Common use cases for NAT

Twice NAT and Manual NAT

Here are some common tasks that can be achieved using "Network Object NAT", also known as "Auto NAT":

- Enable a Server on the Inside Network to Reach the Internet Using a Public IP address
- Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address
- Make a Server on the Inside Network Available on a Specific Port of a Public IP Address
- Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Network Object NAT and Auto NAT

Here is a common task that can be achieved using "Twice NAT", also know as "Manual NAT":

- Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Enable a Server on the Inside Network to Reach the Internet Using a Public IP address

Use Case

Use this NAT strategy when you have a server with a private IP address that needs to be accessed from the internet and you have enough public IP addresses to NAT one public IP address to the private IP address. If you have a limited number of public IP addresses, see Make a server on the inside network available to users on a specific port of a public IP address (that solution may be more suitable).

Strategy

Your server has a static, private IP address, and users outside your network have to be able to reach your server. Create a network object NAT rule that translates the static private IP address to a static public IP address. After that, create an access policy that allows traffic from that public IP address to reach the private IP address. Finally, deploy these changes to your device.

Before you begin

Before you begin, create two network objects. Name one object *servername*_inside and the other object *servername*_outside. The *servername*_inside network object should contain the private IP address of your server. The *servername*_outside network object should contain the public IP address of your server.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  > **Network Object NAT.**

Step 8 In section 1, **Type**, select **Static.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, perform these actions:

a. Expand the Original Address menu, click **Choose**, and select the **servername_inside** object.

b. Expand the Translated Address menu, click **Choose**, and select the **servername_outside** object.

Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**.

Step 14 For ASA, deploy a Network Policy rule or for FDM-managed device, deploy an access control policy rule to allow the traffic to flow from *servername*_inside to *servername*_outside.

Step 15 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

NAT rules created by this procedure:

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address

Use Case

Allow users and computers in your private network to connect to the internet by sharing the public address of your outside interface.

Strategy

Create a port address translation (PAT) rule that allows all the users on your private network to share the outside interface public IP address of your device.

After the private address is mapped to the public address and port number, the device records that mapping. When incoming traffic bound for that public IP address and port is received, the device sends it back to the private IP address that requested it.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  **Network Object NAT.**

Step 8 In section 1, **Type**, select **Dynamic.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **any** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, perform these actions :

a. Expand the Original Address menu, click **Choose** and select the **any-ipv4** or **any-ipv6** object depending on your network configuration.

b. Expand the Translated Address menu, and select **interface** from the available list. Interface indicates to use the public address of the outside interface.

Step 11 For an FDM-managed device, in section 5, **Name**, enter a name for the NAT rule.

Step 12 Click **Save**.

Step 13 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

NAT rules created by this procedure:

```
object network any_network
nat (any,outside) dynamic interface
```

Make a Server on the Inside Network Available on a Specific Port of a Public IP Address

Use Case

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Prerequisites

Before you begin, create three separate network objects, one each for an FTP, HTTP, and SMTP server. For the sake of the following procedures, we call these objects **ftp-server-object**, **http-server-object**, and **smtp-server-object**.

NAT Incoming FTP Traffic to an FTP Server

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  > **Network Object NAT.**

Step 8 In section 1, **Type**, select **Static.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **ftp**-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **ftp, ftp.**



Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**. The new rule is created in section 2 of the NAT table.

Step 14 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here is the entry that is created and appears in the ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network ftp-object
host 10.1.2.27
```

NAT rule created by this procedure

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

NAT Incoming HTTP Traffic to an HTTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the http server. For the sake of this procedure, we will call the object, **http-object**.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  > **Network Object NAT.**

Step 8 In section 1, **Type**, select **Static.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **http**-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **http**, http.



Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**. The new rule is created in section 2 of the NAT table.

Step 14 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network http-object
host 10.1.2.28
```

NAT rule created by this procedure

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

NAT Incoming SMTP Traffic to an SMTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the smtp server. For the sake of this procedure, we will call the object, **smtp-object**.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click + > **Network Object NAT.**

Step 8 In section 1, **Type**, select **Static.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the smtp-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **smtp**, **smtp.**



Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**. The new rule is created in section 2 of the NAT table.

Step 14 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Object created by this procedure

```
object network smtp-object
host 10.1.2.29
```

NAT rule created by this procedure

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Use Case

Use this approach if you have a group of specific device types, or user types, that need to have their IP addresses translated to a specific range so that the receiving devices (the devices on the other end of the transaction) allow the traffic in.

Translate a Pool of Inside Addresses to a Pool of Outside Addresses

Before you begin

Create a network object for the pool of private IP addresses you want to translate and create a network object for the pool of public addresses you want to translate those private IP addresses into.

For the ASA, the "original address" pool, (the pool of private IP addresses you want to translate) can be a network object with a range of addresses, a network object that defines a subnet, or a network group that includes all the addresses in the pool. For the FTD, the "original address" pool can be a network object that defines a subnet or a network group that includes all the addresses in the pool.

Note For the ASA FTD, the network group that defines the pool of "translated address" cannot be a network object that defines a subnet.

For the sake of the following procedure, we named the pool of private addresses, **inside_pool** and name the pool of public addresses, **outside_pool.**

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  > **Network Object NAT**.

Step 8 In section 1, **Type**, select **Dynamic** and click **Continue**.

Step 9 In section 2, **Interfaces**, set the source interface to **inside** and the destination interface to **outside**. Click **Continue**.

Step 10 In section 3, **Packets**, perform these tasks:

- For the Original Address, click **Choose** and then select the **inside_pool** network object (or network group) you made in the prerequisites section above.
- For the Translated Address, click **Choose** and then select the **outside_pool** network object (or network group) you made in the prerequisites section above.

Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**.

Step 14 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

NAT rules created by this procedure

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Use Case

Use this Twice NAT use case to enable site-to-site VPN.

Strategy

You are translating a pool of IP addresses to itself so that the IP addresses in one location on the network arrives unchanged in another.

Create a Twice NAT Rule

Before you begin

Create a network object or network group that defines the pool of IP addresses you are going to translate to itself. For the ASA, the range of addresses can be defined by a network object that uses an IP address range, a network object that defines a subnet, or a network group object that includes all the addresses in the range. For the FTD, the range of addresses can be defined by a network object that defines a subnet or a network group object that includes all the addresses in the range.

For the sake of the following procedure, we are going call the network object or network group, Site-to-Site-PC-Pool.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device you want to create the NAT rule for.

Step 6 Click **NAT** in the **Management** pane at the right.

Step 7 Click  > **Twice NAT.**.

Step 8 In section 1, **Type**, select **Static.** Click **Continue**.

Step 9 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 10 In section 3, **Packets**, make these changes:

- Expand the Original Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.
- Expand the Translated Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.

Step 11 Skip section 4, **Advanced**.

Step 12 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 13 Click **Save**.

Step 14 For an ASA, create a crypto map. See CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide and review the chapter on LAN-to-LAN IPsec VPNs for more information on creating a crypto map.

Step 15 Review and deploy now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

These are the entries that would appear in an ASA's saved configuration file as a result of these procedures.

Note This does not apply to FDM-managed devices.

Objects created by this procedure

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

NAT rules created by this procedure

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

Manage security policies in Security Cloud Control Firewall Management

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

Manage ASA network security policy

The ASA network security policy includes access control lists (ACLs) that determine whether to permit or deny traffic from accessing another network through the ASA firewall. This section outlines the steps to create an ASA access list and configure access rules within it. It also details the steps to assign an interface to an access control list and share it among other ASA devices managed by Security Cloud Control Firewall Management.

About ASA Access Control Lists and Access Groups

ASA Access Control Lists

Access control lists (ACLs) are used to identify traffic flows based on various characteristics such as source and destination IP address, IP protocol, ports, source, and other parameters.

The following is an access list sample:

```
access-list ACL extended permit ip any any
```

`ACL` is the name of the access list.

You can avoid the creation of the same access list on multiple devices individually, and instead create a single access list and share it across multiple ASA devices. Changes made to the shared access list automatically apply to all the devices to which the ACL is assigned. You also have the option to copy the access list to other ASA devices as needed.

Access Rules

An access list includes access rules that permit or deny traffic flow to a network based on specific characteristics such as source and destination IP addresses, IP protocol, port number, and security group tags.

ASA Access Groups

An access group is a specific association that is established when an access list is assigned to a device interface configured for traffic flow in any direction. The access list contains specific rules that either permit or deny traffic passing through the device interface.

The following is an access group sample that is created when a device interface is assigned to an access list.

```
access-group ACL out interface giginterface0
```

`ACL` is the name of the access list and `giginterface0` is the logical name of the device interface that is assigned to the access list.

Note To use API endpoints to manage your ASA access groups, see Get Access Groups on the Cisco DevNet website.

Create an ASA Access List

When configuring an access list on an ASA firewall, a rule is automatically created to allow traffic from a source to a destination outside your network. You can create additional rules and assign the access list to an interface to regulate the traffic network.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 Click **Create Access List**.

Step 5 In the **Name** field, enter a name for the access list and click **Save**.

Note
You cannot have two access lists with the same name on a device.

Step 6 Click **Save**.

Security Cloud Control creates an access group and a default rule that permits all traffic.

You can now add new rules to the access list. See Add a Rule to an ASA Access List, on page 67.

To assign interfaces and traffic directions to the access list, see Assign Interfaces to ASA Access Control List, on page 69.

Add a Rule to an ASA Access List

You can add rules in ascending order by rule number. Packets will be verified against the rules in the sequence in which the rules were created, with the first rule taking precedence, followed by subsequent rules. You can adjust the position of any rule, if required.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, select an access list that you want.

Step 6 Click the **Add Rule** () icon that is displayed on the right.

Note
In the ordered list, hover over the desired position and click **Add Rule Here**.

Step 7 In the **New Access Rule** window, provide the following information:

- **Order**: Select where you want to insert the rule in the ordered list of rules. Rules are applied on a first-match basis and prioritized by position in the list of rules from 1 to last.
- **Action**: Specify whether you are allowing (permitting) the described traffic or are blocking (dropping) it.
- **Protocol**: Specify the protocol of the traffic, such as IP, TCP, UDP, ICMP, or ICMPv6. The default is IP, but you can select a more specific protocol to target traffic with more granularity.
- **Source/Destination**: Define the source (originating address) and destination (target address of the traffic flow). You typically configure the IPv4 address of hosts or subnets, which you can represent with network object groups. You can assign only one object to the source or destination.
- **Port**: Select the port object that pairs a service type, such as TCP or UDP, and a port number or a range of port numbers.
- **SGT Group**: Assign the security group you want from the list. By default, the value is **Any**. See Security Group Tags in ASA Policies.
- **Time Range**: Define a time range for ASA network policies to allow access to networks and resources based on time of day.
- **Logging**: Activity resulting from a network policy rule is not logged by default. You can activate logging for individual rules. See Log Rule Activity.

Step 8 Click **Save**.

The rule is added to the access list and set to **Active** state.

Step 9 Review and deploy the changes you made now, or wait and deploy multiple changes.

About System Log Activity

When you set up a new rule, you can specify how often and at what severity level you want to collect its activity. To do this, you can select the corresponding severity levels and then choose the frequency of data collection. This will ensure that you have the necessary information to monitor and analyze the activity generated by your rules.

Note ASA does not generate syslog messages with a severity level of zero (emergencies).

You have the option to adjust the logging interval, which indicates how frequently the log records are updated. This interval is measured in seconds and can be set from 1 to 600. By default, the interval is set to 300 seconds. This interval value is also utilized as a timeout period for removing an inactive flow from the cache that collects drop statistics.

Table 4: Log Rule Activity

Security Level	Description
emergencies	System is unusable.
alert	Immediate action is needed.
critical	Critical conditions.
error	Error conditions.
warning	Warning conditions.
notification	Normal but significant conditions.
informational	Informational messages only.
debugging	Debugging messages only.

Deactivate Rules in an Access Control List

When you create a new rule in an access control list, it is activated by default. However, you can temporarily deactivate individual rules to optimize traffic flow, resolve conflicts, or isolate issues.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose the access control list you want.

Step 6 In the rule list, check the corresponding rule check box that you want.

Step 7 In the selected row, slide the **Active** setting off.

Step 8 Review and deploy the changes you made now, or wait and deploy multiple changes.

About Security Group Tags in ASA Policies

If you onboard an ASA that uses security group tags (SGT) in its access control rules, Security Cloud Control allows you to edit the rules that use SGT groups and manage the policies that have these rules. However, you cannot create SGT groups or edit them using the Security Cloud Control GUI. To create or edit SGT groups, you must use ASA's Adaptive Security Device Manager (ASDM) or the CLI available in Security Cloud Control.

In Security Cloud Control's object page, when looking at the details of SGT groups, you'll see that those objects are identified as noneditable, system-provided objects.

Security Cloud Control administrators can perform these tasks on ACLs and ASA policies that contain SGT groups:

- Edit all aspects of ACLs except the source and destination security groups.
- Copy a policy containing SGT groups from one ASA to another.

For detailed instruction, on configuring Cisco TrustSec using the command line interface, see the "ASA and Cisco TrustSec" chapter of the ASA CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide pertaining to your ASA release.

Assign Interfaces to ASA Access Control List

When you assign ASA interfaces to access control list, the device establishes a specific association between the list and interfaces. The rules that are associated with access control list are applied only to the interfaces through which the traffic flows in the specified directions.

You can only assign one access list per interface for a single traffic flow direction.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose an access list.

Step 6 In the **Actions** pane displayed on the right, click **Assign Interfaces**.

Step 7 From the **Interface** drop-down list, choose an interface.

Step 8 From the **Direction** drop-down list, specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the ASA device, see Create an ASA Global Access List, on page 70.

Step 9 Click **Save**.

Step 10 Review and deploy the changes you made now, or wait and deploy multiple changes.

Create an ASA Global Access List

Global access policies are network policies that are applied to all the interfaces on an ASA. These policies are only applied to inbound network traffic. You can create a global access policy to ensure that a set of rules is applied uniformly to all the interfaces on an ASA.

Only one global access policy can be configured on an ASA. However, a global access policy can have more than one rule assigned to it, just like any other policy.

This is the order of rule-processing on the ASA:

1. Interface access rules
2. Bridge Virtual Interface (BVI) access rules
3. Global access rules
4. Implicit deny rules

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose an access list.

Step 6 In the **Actions** pane displayed on the right, click **Assign Interfaces**.

Step 7 Check the **Create as a global access list** check box.

Step 8 Click **Save**.

Step 9 Review and deploy the changes you made now, or wait and deploy multiple changes.

Share an ASA Access Control List with Multiple ASA Devices

Sharing access policies in network security effectively improves efficiency, consistency, and centralized management, leading to an overall improved security posture. To share an access control list across ASA

devices, create an access control list and define access rules on a single ASA device and then share it with the desired ASA devices rather than configuring them separately. This ensures consistency in the network and reduces the risk of misconfigurations. Additionally, shared access control lists provide scalability because networks grow and evolve by allowing you to manage access control lists for increasing users and ASA devices.

Keep the following points in mind:

- Access control list rules are shared, but the interfaces are not included.
- Sharing an access control list with other ASA devices will overwrite any existing access control lists with the same name.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose an access control list.

Step 6 In the **Actions** pane that is displayed on the right, click **Share**.

Step 7 Select the ASA devices by checking the corresponding check box and click **Save**.

In the **Device Relationships** pane displayed on the right, the ASA devices that share the selected access control list are displayed.

Step 8 Review and deploy the changes you made now, or wait and deploy multiple changes.

Copy an ASA Access Control List to Another ASA

An ASA access control list can be easily copied to another Security Cloud Control-managed device in the same tenant. After copying an access list file to a target ASA device, any further changes made to the access list won't be automatically applied to the target device. This is different from access control list sharing feature, where changes are automatically applied.

Keep the following points in mind:

- You cannot copy an access list to a target device if that device already has another access list with the same name.
- You cannot copy an access list if another access list on the target device is associated with the same interface and direction.
- You cannot only copy an access list to a disabled interface on the target device.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose an access list.

Step 6 In the **Actions** pane on the right, click **Copy**.

Step 7 Select the target device to which you want to copy the access list.

Step 8 Choose an interface and specify the direction for applying the selected access list.

The designated access list is applied to the interface through which traffic flows in the specified direction. This access list can be applied to multiple interfaces and directions.

To apply the access list to all the interfaces on the selected target, see Create an ASA Global Access List, on page 70.

Step 9 Click **Copy**.

A message appears at the bottom right corner on the Security Cloud Control screen on a successful copy.

Step 10 Review and deploy the changes you made now, or wait and deploy multiple changes.

Copy a Rule Within or Across ASA Access Lists and Devices

You can copy an access control rule in the following ways:

- Within the same access list.
- From one access list to another, either within the same ASA device or across different ASA devices.

Note The paste operation fails if you attempt to add a rule that already exists in the access list.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 3 In the **Management** pane on the right, click **Policy**.

Step 4 From the **Selected Access List** drop-down list, select an access list that you want.

Step 5 Select a rule by clicking the corresponding check box and in the **Actions** pane on the right, click **Copy**.

Step 6 Perform the following:

- To paste the rule within the same access list, hover the mouse pointer in the desired position until you see the **Paste Rule Here** option and click it. The Add/Edit rule dialog box is displayed, allowing you to modify the copied rule, as identical rules are not permitted in the same access list.
- To paste the rule within the same ASA device, from the **Selected Access List** drop-down list, select an access list you want.
- To paste the rule to a different ASA device, in the left pane, go to **Security Devices** > select an ASA device > **Policy** > **Selected Access List**.

Step 7 To paste the copied rule in the desired position, select a rule that comes after where you want the new rule to be. In the **Actions** pane on the right, click **Paste**. The copied rule will be inserted before the selected rule.

You can use the **Move Up** and **Move Down** buttons to position the rule as needed.

Note
Alternatively, you can hover over a desired position in the rule listing table until you see **Paste Rule Here**, and then click it.

Unshare a Shared ASA Access Control List

If the rules governing the interface handling your network become outdated, you can unshare the access control list from the devices currently linked. Unsharing an ASA device from the shared access control list will not have any impact on other ASA devices currently sharing this list.

Procedure

Step 1 In the left pane, click **Inventory**.
Step 2 In the left pane, click **Security Devices**.
Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.
Step 4 In the **Management** pane on the right, click **Policy**.
Step 5 From the **Selected Access List** drop-down list, choose an access list.
Step 6 In the **Actions** pane on the right, click **Share**.
Step 7 Uncheck the ASA devices that share the selected access list and click **Save**.
Step 8 Review and Deploy the changes you made now, or wait and deploy multiple changes.

View ASA Access Policies Listing Page

The ASA access policy listing page shows a comprehensive overview of all access lists associated with the ASA devices that have been onboarded to the Security Cloud Control tenant.

Note

Click the filter ( ) button, then click **Filter by Device** to search for policies that are either shared across multiple ASA devices or specific to a single ASA device.

Procedure

Step 1 In the left pane, choose **Policies > ASA Access Policies**click **Policies** > **ASA** > **Access Policies**.

The page provides the following information:

- **Name**: The name of the access list.
- **Device**: The corresponding ASA devices associated with each access list. Additionally, for access lists that are shared across multiple devices, it displays a list of all ASA devices that use the shared access list.

  Click the button to view the ASA devices associated with the selected access list.

  To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

  To return to this page, click **ASA Access Policies**.
- **Interfaces**: The network interfaces to which each access list is assigned.

Step 2 To view the ASA devices associated with an access list, click the corresponding button in the **Device** column.

Step 3 To navigate to the policy page of the selected device, click **View Policies**. You can create or edit an access list.

Step 4 To return to the policy listing page, in the top-left corner, click ← **ASA Access Policies**.

Global Search of ASA Access Lists

Use the global search functionality to search the following in your Security Cloud Control tenant:

- ASA devices and all their associated access lists.
- Access lists or shared access lists and their occurrences across all onboarded ASA devices.

Rename an ASA Access Control List

It is possible to modify the name of an access list to suit your specific needs. Whether you want to rename a global access list or a shared access control list, it is a straightforward process. If the access list is shared, changing its name updates the name on all the other devices where the shared access control list is used. Remember that the updated name will only reflect after the configuration is deployed to those devices.

Procedure

Step 1 In the left pane, click **Inventory**.
Step 2 In the left pane, click **Security Devices**.
Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.
Step 4 In the **Management** pane on the right, click **Policy**.
Step 5 From the **Selected Access List** drop-down list, choose an access list that you want to rename.
Step 6 Click the **Rename** ( ) icon in the right pane.
Step 7 Click the **Save** ( ) button.
Step 8 Review and deploy the changes you made now, or wait and deploy multiple changes.

Delete a Rule from an ASA Access Control List

You can remove access rules from the access list, but at least one rule must remain for the list to exist.

Procedure

Step 1 In the left pane, click **Inventory**.
Step 2 In the left pane, click **Security Devices**.
Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.
Step 4 In the **Management** pane on the right, click **Policy**.
Step 5 Click an access list and select the rules to be deleted.
Step 6 In the **Actions pane** on the right, click **Remove**.
Step 7 Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Delete an ASA Access Control List

This procedure can be used to delete the access control list, shared access list, or a global access list. Deleting a shared access list from one device does not impact other devices where the access list is in use. On those devices, the access list persists as a local access list.

Procedure

Step 1 In the left pane, click **Inventory**.
Step 2 In the left pane, click **Security Devices**.
Step 3 Click the **ASA** tab and select an ASA device by checking the corresponding check box.

Step 4 In the **Management** pane displayed on the right, click **Policy**.

Step 5 From the **Selected Access List** drop-down list, choose an access list you want to delete.

Step 6 In the **Actions** pane on the right, click **Delete**.

Step 7 Review and deploy the changes you made now, or wait and deploy multiple changes at once.

Compare ASA network policies

Procedure

Step 1 In the navigation pane, select **Policies> ASA Policies**.

Step 2 In the left pane, click **Policies** > **ASA** > **Access Policies**.

Step 3 Click **Compare** in the top right corner of the viewer.

Step 4 Select up to two policies to compare.

Step 5 Click **View Comparison** at the bottom of the viewer. This will bring up the comparison viewer. When you are finished, click **Done** and then **Done Comparing**.

Hit rates

Security Cloud Control enables you to evaluate the outcome of policy rules, on top of secure and scalable orchestration of policies, providing a simple visualization for more accurate policy analysis and an immediate, actionable pivot to root cause, all in a single pane from the cloud. The Hit Rates feature enables you to:

- Eliminate obsolete and never-matched policy rules, increasing security posture.
- Optimize firewall performance by instantly identifying bottlenecks as well as ensuring correct and efficient prioritization is enforced (for example, most triggered policy rule is prioritized higher).
- Maintain a history of Hit Rates information, even upon device or policy rule reset, for a configured data retention period (1 year).
- Strengthen validation of suspected shadow and unused rules based on actionable information. Removing doubt about update or delete.
- Visualize policy rule usage in the context of the entire policy, leveraging predefined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.) to evaluate impact on packets traversing the network.

View Hit Rates of ASA Policies

Procedure

Step 1 Select **Policies** > **ASA Access Policies** from the Security Cloud Control menu bar.

Step 2 In the left pane, click **Policies** > **ASA** > **System Settings**.

Step 3 Click the filter icon and pin it open.

Step 4 In the Hits area, click the various hit count filters to display which policies are being hit more or less often than others.

Search and filter ASA network rules in the access list

Search

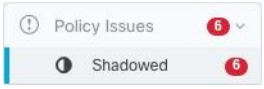
Use the search bar to search for names, keywords, or phrases in the names of the rules within the access list. Search is not case-sensitive.

Filter

Use the filter sidebar to find network policy issues. Filtering is not additive, each filter setting acts independently of the other.

Policy Issues

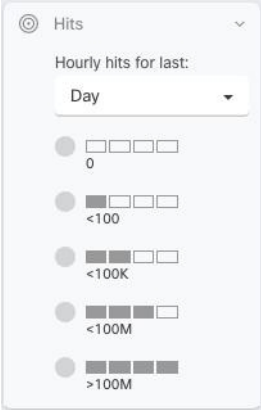
Security Cloud Control identifies network policies that contain shadow rules. The number of policies that contain shadow rules is indicated in the **Policy Issues** filter:



Security Cloud Control marks shadowed rules and network policies that contain them with the shadow badge shadow_badge.png on the network policies page. Click Shadowed to view all the policies containing shadow rules. See Shadow Rules for more information.

Hits

Use this filter to find rules across the access lists that have been triggered a number of times over a specified period.



Filter Use Cases

Find all rules that have zero hits

If you have rules without any hits, you can edit them to make them more effective or simply delete them.

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select 0 hits.

Find out how often rules in a network policy are being hit

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hits filters to see what category the different rules fall into.

Filter network policies by hit rate

1. Select an ASA device and in the **Management** pane on the right, click **Policy**.
2. Above the rule table, click **Clear** to clear any existing filters.
3. Click the filter icon and expand the **Hits** filter.
4. Select a time period.
5. Select the different hit rate categories. Security Cloud Control displays the rules that are getting hit at the rate you specify.

Shadowed rules

A network policy with shadowed rules is one in which at least one rule in the policy will never trigger because a rule that precedes it prevents the packet from being evaluated by the shadowed rule.

For example, consider these network objects and network rules in the "example" network policy:

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

No traffic is evaluated by this rule,

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

because the previous rule,

```
access-list example extended deny ip any4 object 02-50
```

denies any ipv4 address from reaching any address in the range 10.10.10.2 - 10.10.10.50.

Find Network Policies with Shadowed Rules

To find network policies with shadowed rules, use the network policies filter:

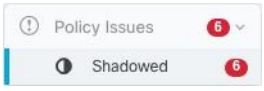
Procedure

Step 1 In the navigation pane, click **Policies** > **ASA Policies**.

Step 2 In the left pane, click **Policies** > **ASA** > **Access Policies**.

Step 3 Click the filter icon at the top of the ASA Access Policies table.

Step 4 In the Policy Issues filter, check **Shadowed** to view all the policies with shadowed rules.



Resolve Issues with Shadowed Rules

This is how Security Cloud Control displays the rules described in the "example" network policy above:



The rule on line 1 is marked with a shadow warning badge ⚠ because it's shadowing another rule in the policy. The rule on line 2 is marked as being shadowed ◑ by another rule in the policy. The action for the rule on line 2 is grayed-out because it's entirely shadowed by another rule in the policy. Security Cloud Control is able to tell you which rule in the policy shadows the rule in line 2.

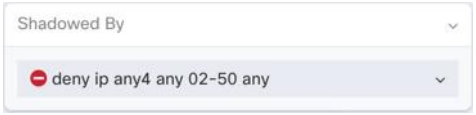
The rule on line 3 can only be triggered some of the time. This is a partially shadowed rule. Network traffic from any IPv4 address trying to reach an IP address in the range 10.10.10.2-10.10.10.50 would never be evaluated because it would have already been denied by the first rule. However, any IPv4 address attempting to reach an address in the range 10.10.10.51-10.10.10.100 would be evaluated by the last rule and would be permitted.

Caution Security Cloud Control does not apply a shadow warning badge ⚠ to partially shadowed rules.

Procedure

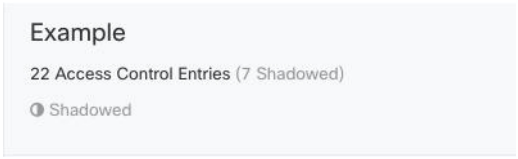
Step 1 Select the shadowed rule in the policy. In the example above, that means clicking on line 2.

Step 2 In the rule details pane, look for the **Shadowed By** area. In this example, the **Shadowed By** area for the rule in line 2 shows that it is being shadowed by the rule in line 1:



Step 3 Review the shadow*ing* rule. Is it too broad? Review the shadow*ed* rule. Do you really need it? Edit the shadow*ing* rule or delete the shadow*ed* rule.

Note
By deleting shadowed rules, you reduce the number of access control entries (ACEs) on your ASA. This frees up space for the creation of other rules with other ACEs. Security Cloud Control calculates the number of ACEs derived from all the rules in a network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it also lists that number.



Security Cloud Control also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:



Step 4 Determine which devices use the policy by looking in the Devices area of the network policy details pane.

Step 5 Open the **Security Devices** page and **Deploy Changes** back to the devices affected by the policy change.