Create and Manage Identity Policies

The following topics discuss how to create and manage identity rules and identity policies:

About Identity Policies

Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

With the exception noted in the following paragraphs, you must configure realms and authentication methods you plan to use before you can invoke them in your identity rules:

- You configure realms outside of your identity policy, at **System** > **Integration** > **Realms**. For more information, see Create a Realm and Realm Directory.
- You configure ISE/ISE-PIC, a passive authentication identity source, at **System** > **Integration** > **Identity Sources**. For more information, see Configure ISE/ISE-PIC for User Control.
- You configure the TS Agent, a passive authentication identity source, outside the Firepower System. For more information, see the *Cisco Terminal Services (TS) Agent Guide*.
- You configure captive portal, an active authentication identity source, within the identity policy. For more information, see How to Configure the Captive Portal for User Control.
- You configure Remote Access VPN, an active authentication identity source, in Remote Access VPN policies. For more information, see Remote Access VPN Authentication.

After you add multiple identity rules to a single identity policy, order the rules. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles the traffic.

You can optionally configure an identity policy to filter traffic by network object, which limits the network each device monitors in the event your devices are at or near their memory limits. Devices must run FTD version 6.7 or later to apply network filtering to them.

After you configure one or more identity policies, you must associate one identity policy with your access control policy. When traffic on your network matches the conditions in your identity rule, the system associates the traffic with the specified realm and authenticates the users in the traffic using the specified identity source.

If you do not configure an identity policy, the system does not perform user authentication.

Exception to creating an identity policy

An identity policy is not required if all of the following are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.
- You use Security Group Tags (SGT) in access control policies. For more information, see ISE SGT vs Custom SGT Rule Conditions.

Video YouTube video on creating an identity policy and rule.

Related Topics

How to Set Up an Identity Policy

License Requirements for Identity Policies

FTD License

Any

Classic License

Control

Requirements and Prerequisites for Identity Policies

Model Support

Any.

Supported Domains

Any

User Roles

- Admin
- Access Admin

- Network Admin

Create an Identity Rule

For details about configuration options for identity rules, see Identity Rule Fields, on page 4.

Before you begin

You must create and enable a realm or realm sequence.

- Create a realm and realm directory as discussed in Create a Realm and Realm Directory.
- (Optional.) Create a realm sequence as discussed in Create a Realm Sequence.
- Download users and groups and enable the realm as discussed in Synchronize Users and Groups.

Procedure

Step 1 If you haven't done so already, log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** .

Step 3 Click **Edit** ( ) next to the identity policy to which to add the identity rule.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 Click **Add Rule**.

Step 5 Enter a **Name**.

Step 6 Specify whether the rule is **Enabled**.

Step 7 To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.

Step 8 Choose a rule **Action** from the list.

Step 9 Click **Realms & Settings**.

Step 10 Choose a realm or realm sequence for the identity rule from the **Realms** list. You must associate a realm or realm sequence with every identity rule.

The only exception to the realm requirement is implementing user control using only the ISE SGT attribute tag. In this case, you do not need to configure a realm or realm sequence for the ISE server. ISE SGT attribute conditions can be configured in policies with or without an associated identity policy.

Step 11 If you're configuring captive portal, see How to Configure the Captive Portal for User Control.

Step 12 (Optional) To add conditions to the identity rule, see Rule Condition Types.

Step 13 Click **Add**.

Step 14 In the policy editor, set the rule position. Click and drag or use the right-click menu to cut and paste. Rules are numbered starting at 1. The system matches traffic to rules in top-down order by ascending rule number. The first rule that traffic matches is the rule that handles that traffic. Proper rule order reduces the resources required to process network traffic and prevents rule preemption.

Step 15 Click **Save**.

Identity Rule Fields

Use the following fields to configure identity rules.

Enabled

Choosing this option enables the identity rule in the identity policy. Deselecting this option disables the identity rule.

Action

Specify the type of authentication you want to perform on the users in the specified realm: **Passive Authentication** (default), **Active Authentication**, or **No Authentication**. You must fully configure the authentication method, or *identity source*, before selecting it as the action in an identity rule.

Additionally, if VPN is enabled (configured on at least one managed device), remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule action. This means that, if VPN is enabled, VPN identity determination is performed first for all sessions regardless of the selected action. If a VPN identity is found on the specified realm, this is the identity source used. No additional captive portal active authentication is done, even if selected.

If the VPN identity source is not found, the process continues according to the specified action. You cannot restrict the identity policy to VPN authentication only because if the VPN identity is not found, the rule is applied according to the selected action.

Caution Adding the first or removing the last active authentication rule when SSL decryption is disabled (that is, when the access control policy does not include an SSL policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

For information about which passive and active authentication methods are supported in your version of the Firepower System, see About User Identity Sources.

Realm

The realm or realm sequence containing the users you want to perform the specified **Action** on. You must fully configure a realm or realm sequence before selecting it as the realm in an identity rule.

Note If remote access VPN is enabled and your deployment is using a RADIUS server group for VPN authentication, make sure you specify the realm associated with this RADIUS server group.

Note If you select **Kerberos** (or **HTTP Negotiate**, if you want Kerberos as an option) as the **Authentication Protocol** for the identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.

Use active authentication if passive or VPN identity cannot be established

Selecting this option authenticates users using captive portal active authentication if a passive or a VPN authentication fails to identify them. You must configure captive portal active authentication in your identity policy in order to select this option.

If you disable this option, users that do not have a VPN identity or that passive authentication cannot identify are identified as Unknown.

Identify as Special Identities/Guest if authentication cannot identify user

Selecting this option allows users who fail captive portal active authentication the specified number of times times to access your network as a guest. These users appear in the Firepower Management Console identified by their username (if their username exists on the AD or LDAP server) or by **Guest** (if their user name is unknown). Their realm is the realm specified in the identity rule. (By default, the number of failed logins is 3.)

This field is displayed only if you configure **Active Authentication** (that is, captive portal authentication) as the rule **Action**.

Authentication Protocol

The method to use to perform captive portal active authentication. The selections vary depending on the type of realm, LDAP or AD:

- Choose **HTTP Basic** if you want to authenticate users using an unencrypted HTTP Basic Authentication (BA) connection. Users log in to the network using their browser's default authentication popup window.

  Most web browsers cache the credentials from **HTTP Basic** logins and use the credentials to seamlessly begin a new session after an old session times out.

- Choose **NTLM** to authenticate users using a NT LAN Manager (NTLM) connection. This selection is available only when you select an AD realm. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.
- Choose **Kerberos** to authenticate users using a Kerberos connection. This selection is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled. If transparent authentication is configured in a user's browser, the user is automatically logged in. If transparent authentication is not configured, users log in to the network using their browser's default authentication popup window.

Note The **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** to perform Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform Kerberos captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the host name you provided when configuring DNS.

For ASA with FirePOWER Services and Firepower Threat Defense devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.

- Choose **HTTP Negotiate** to allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection. This type is available only when you select an AD realm.

Note The **Realm** you choose must be configured with an **AD Join Username** and **AD Join Password** for **HTTP Negotiate** to choose Kerberos captive portal active authentication.

Note If you are creating an identity rule to perform **HTTP Negotiate** captive portal and you have DNS resolution configured, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN of the device you are using for captive portal must match the hostname you provided when configuring DNS.

For ASA with FirePOWER Services devices, the FQDN is the FQDN of the ASA FirePOWER module.

Create an Identity Policy

Before you begin

An identity policy is required to use users and groups in a realm in access control policies. Create and enable one or more realms as described in Create a Realm and Realm Directory.

(Optional.) If a particular managed device monitors a large number of user groups, the system might drop user mappings based on groups due to managed device memory limitations. As a result, rules with realm or user conditions might not perform as expected. Provided the devices run version 6.7 or later, you can configure the identity rule to monitor traffic by one network or network group object only. To create a network object, see Creating Network Objects.

An identity policy is not required if all of the following are true:

- You use the ISE/ISE-PIC identity source.
- You do not use users or groups in access control policies.

- You use Security Group Tags (SGT) in access control policies. For more information, see ISE SGT vs Custom SGT Rule Conditions.

Procedure

Step 1 Log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** and click **New Policy**.

Step 3 Enter a **Name** and, optionally, a **Description**.

Step 4 Click **Save**.

Step 5 To add a rule to the policy, click **Add Rule** as described in Create an Identity Rule, on page 3.

Step 6 To create a rule category, click **Add Category**.

Step 7 To configure captive portal active authentication, click **Active Authentication** as described in Configure the Captive Portal Part 1: Create an Identity Policy.

Step 8 (Optional.) To filter traffic by network object, click the **Identity Source** tab. From the list, click the network object to use to filter traffic for this identity policy. Click **Add** (+) to create a new network object.

Step 9 Click **Save** to save the identity policy.

What to do next

- Add rules to your identity policy that specify which users to match and other options; see Create an Identity Rule, on page 3.
- Associate the identity policy with an access control policy to allow or block selected users from accessing specified resources; see Associating Other Policies with Access Control.
- Deploy configuration changes to managed devices; see Deploy Configuration Changes.

If you encounter issues, see Troubleshoot User Control.

Related Topics

Configure the Captive Portal Part 1: Create an Identity Policy
Captive Portal Fields
Troubleshoot User Control
Create an Identity Mapping Filter, on page 7

Create an Identity Mapping Filter

An identity mapping filter can be used to limit the networks to which an identity rules apply. For example, if your FMC manages FTDs that have a limited amount of memory, you can limit the networks they monitor.

You can also optionally exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE. You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

Before you begin

Perform the following tasks:

1. Create a realm, which is required for an identity policy. See Create a Realm and Realm Directory.
2. Create an identity policy. See Create an Identity Policy, on page 6.
3. (Optional.) Create a network object or network group object as discussed in Creating Network Objects. The network object or group you create should define the network you want managed devices to monitor in identity policies.

   This step is optional because you can create one when you configure the identity mapping filter.

Procedure

Step 1 Log in to the FMC.

Step 2 Click **Policies** > **Identity**.

Step 3 Click **Edit** ( ).

Step 4 Click the **Identity Source** tab.

Step 5 From the **Identity Mapping Filter** list, click the name of a network object to use as a filter or click **Plus** ( ) to create a new one.

To create a new network object, see Creating Network Objects.

Step 6 Click **Save**.

What to do next

Associate the identity policy with an access control policy as discussed in Associating Other Policies with Access Control.

To check or change ISE identity mapping filters (also referred to as *subnet filters*), use the following commands:

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

Manage an Identity Rule

Procedure

Step 1 If you haven't already done so, log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** .

Step 3 Click **Edit** ( ) next to the policy you want to edit. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 To edit an identity rule, click **Edit** ( ) and make changes as described in Create an Identity Policy, on page 6.

Step 5 To delete an identity rule, click **Delete** ( ).

Step 6 To create a rule category, click **Add Category** and choose the position and the rule.

Step 7 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Manage an Identity Policy

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Procedure

Step 1 If you haven't done so already, log in to the Firepower Management Center.

Step 2 Click **Policies** > **Access Control** > **Identity** .

Step 3 To delete a policy, click **Delete** ( ). If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 4 To edit a policy, click **Edit** ( ) next to the policy and make changes as described in Create an Identity Policy, on page 6. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 5 To copy a policy, click **Copy** ( ).

Step 6 To generate a report for the policy, click **Report** ( ) as described in Generating Current Policy Reports.

Step 7 To compare policies, see Comparing Policies.