

Identity Policies

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

- Identity policies, on page 1
- License requirements for identity policies, on page 2
- Requirements and prerequisites for identity policies, on page 2
- Create an identity policy, on page 3
- Identity rule conditions, on page 5
- Create an identity rule, on page 12
- Sample identity policies and rules, on page 14
- Manage an identity policy, on page 21
- Manage an identity rule, on page 21
- Troubleshoot user control, on page 22

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.

Configuration requirements

With the exception noted below, 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 **Integrations** > **Identity** > **Realms** > **Realms**. For more information, see Create an LDAP realm or an Active Directory realm and realm directory.
- You configure ISE/ISE-PIC, a passive authentication identity source, at **Integrations** > **Identity** > **Identity Sources**. For more information, see Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
- You configure the TS Agent, a passive authentication identity source, outside the 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 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 Configure AAA settings for a remote access VPN policy.

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 also filter traffic by network object, which limits the network each device monitors in the event your devices are at or near their memory limits.

After you configure one or more identity policies, you must associate 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 no identity policy is associated with an access control policy, the system does not apply identity policy rules to that policy's traffic. This does not disable authentication performed by independently configured services, such as remote access VPN. Follow the applicable identity-source and access-control requirements for user awareness and user control.

Exception to creating an identity policy

An identity policy is not required if all these conditions 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.

Related Topics

Set up an identity policy

License requirements for identity policies

This reference provides license requirements for identity policies.

Threat Defense License

Any

Requirements and prerequisites for identity policies

This reference provides the requirements and prerequisites necessary for implementing identity policies.

Model support

Any.

Supported domains

Any

User roles

- Administrator

- Access Admin
- Network Admin

Create an identity policy

Create an identity policy to control user and group access in a realm for access control policies.

This task discusses how to 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 an LDAP realm or an Active Directory 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 Create a network object.

An identity policy is not required if all these conditions 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.

Procedure

Step 1 Log in to the Firewall Management Center.

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

Step 3 Click **New Policy**

a) Enter a **Name** and, optionally, a **Description**.
b) Click **Save**.

Step 4 To add a rule to the policy, click **Add Rule** as described in Create an identity rule, on page 12.

Step 5 To create a rule category, click **Add Category**.

Step 6 To configure captive portal active authentication, click **Active Authentication** and see Create an identity policy and active authentication rule.

Step 7 (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 8 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 12.
- Associate the identity policy with an access control policy to allow or block selected users from accessing specified resources; see Associate prefilter, decryption, and identity policies with an access control.
- (Not required for Microsoft Entra ID (formerly Azure AD) realms.) Deploy configuration changes to managed devices; see Deploy configuration changes.

If you encounter issues, see Troubleshoot user control, on page 22.

Related Topics

Create an identity policy and active authentication rule
Captive portal fields
Troubleshoot user control, on page 22

Create an identity mapping filter

Create an identity mapping filter to limit the networks to which an identity rule applies and optimize device memory usage for managed devices.

An identity mapping filter can be used to limit the networks to which an identity rule applies. For example, if your Firewall Management Center manages FTDs that have a limited amount of memory, you can limit the networks they monitor.

You must create separate identity mapping filters for IPv4 and IPv6 addresses.

You can also optionally exclude subnets from the following:

- Receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE.
- Receiving user-to-IP mappings from the passive identity agent.

You should typically do this for lower-memory managed devices to prevent Snort identity health monitor memory errors.

Follow these steps to create an identity mapping filter.

Before you begin

Perform the following tasks:

- Create any of the following:
  - LDAP or Microsoft Active Directory realm. See Create an LDAP realm or an Active Directory realm and realm directory.
  - ISE/ISE-PIC identity source. See Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
  - Captive portal identity source. See Configure the captive portal for user control.
  - Passive Identity Agent identity source. See How to configure a passive identity agent identity source.
  - TS Agent identity source. See Terminal services agent identity source.
  - RA-VPN identity source. See Configure Remote Access VPN for AD-authenticated users.

- Create a network object or network group object as discussed in Networks. The network object or group you create should define the network you want managed devices to monitor in identity policies.

Procedure

Step 1 Start creating an identity policy.

Step 2 From the **Identity Mapping Filter** list, do any of the following:

- Click a network object from the list.
- Click **Add** (+) and follow the prompts on your screen to create either a network object or a network group object. For more information, see Networks.

What to do next

Continue configuring your identity policy.

Identity rule conditions

Identity rule conditions enable you to fine-tune your identity policy to target specific users and networks you want to control. See one of the following topics for more information.

Related Topics

Security zone rule conditions
Network rule conditions
VLAN tag rule conditions
Best practice: use application-based rules over port-based rules
Realm & settings rule conditions, on page 9

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of the device's interfaces, that rule does not affect that device's performance.

Security zone conditions in multidomain environments

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

Network rule conditions

A network condition is a traffic matching criterion that

- matches traffic for rate limiting based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Note You *cannot* use FQDN network objects in identity rules.

Redirect to host name network rule conditions

(Snort 3.0 only)—You can use a network object that contains the fully-qualified host name (FQDN) of the interface that captive portal can use for active authentication requests.

The FQDN must resolve to the IP address of one of the interfaces on a managed device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to a managed device's IP address.

Certificate and redirection behavior

The certificate can specify one FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate.

If an identity rule requires active authentication for a user, but you do not specify a redirect FQDN, the user is redirected to the captive portal port on the managed device interface to which they are connected.

If you do not supply a Redirect to Host Name FQDN, the HTTP Basic, HTTP Response Page, and NTLM authentication methods redirect the user to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name *firewall-hostname.directory-server-domain-name*. If you use HTTP Negotiate without a Redirect to Host Name FQDN, update your DNS server to map this name to the IP addresses of all inside interfaces that require active authentication. If you do not update the DNS server, the redirection does not complete and users cannot authenticate.

We recommend that you always provide a Redirect to Host Name FQDN to ensure consistent behavior regardless of authentication method.

VLAN tag rule conditions

VLAN tag rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details



Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

Best practice: use application-based rules over port-based rules

Use application filtering criteria instead of port filtering to target traffic. Applications can be configured to use unique ports to bypass access control blocks.

Port conditions allow you to control traffic by its source and destination ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

The traditional method targets applications by using port specifications, but applications can manipulate unique ports to bypass these controls

Application filtering is recommended for applications to avoid blocking legitimate applications, like Firewall Threat Defense, that dynamically open separate channels for control and data flow. Port-based access control rules could block such applications, impacting desirable operations.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP).

- For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).
- If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

Port, protocol, and ICMP code rule conditions (concept)

A port, protocol, and ICMP code rule condition is a traffic matching criterion that

- matches traffic based on source and destination ports
- supports TCP, UDP, ICMP, and other protocols that do not use ports, and
- controls traffic flow in access control and other policy rules.

Port condition types

Port conditions match traffic based on the source and destination ports. Depending on the rule type, "port" can represent any of these types:

- TCP and UDP—Control TCP and UDP traffic based on the port. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP (6) /22.
- ICMP—Control ICMP and ICMPv6 (IPv6-ICMP) traffic based on its internet layer protocol plus an optional type and code. For example: ICMP(1):3:3.
- Protocol—Control traffic using other protocols that do not use ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Best practices for port-based rules

Specifying ports is the traditional method used to target applications. However, applications can be configured to use unique ports to bypass access control blocks. Use application filtering criteria when possible; however, note that application filtering is unavailable in prefilter rules.

Use application filtering for FTP and similar applications that open separate channels for control and data flow. Using port-based access control rules can prevent these kinds of applications from performing correctly and could result in blocking desirable connections.

Using source and destination port constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as destination port conditions in a single access control rule.

Matching non-TCP traffic with port conditions

You can match non-port-based protocols. By default, if you do not specify a port condition, you are matching IP traffic. Although configuring port conditions can match non-TCP traffic, restrictions apply:

- Access control rules—For Classic devices, match GRE-encapsulated traffic with an access control rule by using the GRE (47) protocol as a destination port condition. To a GRE-constrained rule, add only network-based conditions: zone, IP address, port, and VLAN tag. The system uses outer headers to match **all** traffic in access control policies with GRE-constrained rules. For Firewall Threat Defense devices, use tunnel rules in the prefilter policy to control GRE-encapsulated traffic.
- Decryption rules—These rules support only TCP port conditions.
- ICMP echo—A destination ICMP port with the type set to 0 or a destination ICMPv6 port with the type set to 129 only matches unsolicited echo replies. ICMP echo replies, sent in response to ICMP echo requests, are ignored. To match any ICMP echo, use ICMP type 8 or ICMPv6 type 128.

Realm & settings rule conditions

The **Realm & Settings** tab page enables you to choose a realm or realm sequence to which to apply the identity rule. If you are using captive portal, you have additional options.

Authentication realm

From the **Realm** list, click a realm or realm sequence.

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.

Active authentication only: other options

If you either choose **Active Authentication** as the authentication type or if you check the box, **Use active authentication if passive or VPN identity cannot be established**, you have these options.

Use active authentication if passive or VPN identity cannot be established

(Passive authentication rule only.) 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 settings for passive-authentication fallback. (That is, users must authenticate using the captive portal.)

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

Also see the discussion of the **Authentication Realm** list later in this topic,

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 to access your network as a guest. These users appear in the Firewall Management Center 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. An example of what users see when logging in with a response page is shown in Create a sample identity policy with an active authentication rule, on page 16.

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 pop-up 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 pop-up 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 pop-up 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 Firewall 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.

- Choose **HTTP Response Page** to enable users to choose a realm to log in to.

  You can optionally customize the response page; for example, to conform to company style standards.

Active Authentication Realm

(Passive authentication rule only.) If you clicked **Use active authentication if passive or VPN identity cannot be established**, you must click the name of a realm or realm sequence. The availability of a realm or realm sequence is determined by your choice for Authentication Protocol as follows:

- **HTTP Basic** or **HTTP Response Page** authentication protocol: You can choose either a realm or a realm sequence.
- **NTLM**, **Kerberos**, or **HTTP Negotiate** authentication protocol: You can choose a realm only. You *cannot* choose a realm sequence.

Create an identity rule

Identity rules enable you to control user authentication and traffic handling by specifying which identity realm should authenticate users for specific network criteria.

For details about configuration options for identity rules, see Identity rule fields, on page 13.

Before you begin

You must create and enable a realm or realm sequence.

- Create a Microsoft Active Directory realm and realm directory as discussed in Create an LDAP realm or an Active Directory realm and realm directory.
- (Microsoft AD realm only.) Download users and groups and enable the realm as discussed in Synchronize users and groups.
- Create a Microsoft Azure AD (SAML) realm as discussed in Create a Microsoft Azure AD (SAML) realm.
- (Optional.) Create a realm sequence as discussed in Create a realm sequence.
- Rules are evaluated top-down. For a connection that matches the specified network criteria of a given rule, the user is evaluated against the identity realm specified in the rule. If the user is not part of that realm, they will be marked as unknown, and no further rules in the identity policy will be evaluated. Thus, if you have more than one realm that needs to be evaluated, be sure to use realm sequences instead of a single realm.

Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include a decryption 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 assigned device handles traffic. Refer to Snort restart traffic behavior.

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.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Security policies** > **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**.

a) Enter a **Name**.
b) If the Specified rule is applicable, check the check box of **Enabled**.
c)
d) To add the rule to an existing category, indicate where you want to **Insert** the rule. To add a new category, click **Add Category**.
e) Choose a rule **Action** from the list.
f) If you're configuring captive portal, see Configure the captive portal for user control.
g) (Optional) To add conditions to the identity rule, see Identity rule conditions, on page 5.
h) Click **Add**.

Step 5 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 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Identity rule fields

Configure identity rules to specify authentication actions for users, including Passive Authentication, Active Authentication, or No Authentication. Learn how VPN identity preference affects authentication and rule processing in remote access scenarios.

Use these fields to configure identity rules.

Enabled

Enabling this option enables the identity rule in the identity policy. Unselecting 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 TLS/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 assigned device handles traffic. Refer to Snort restart traffic behavior.

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 system, see About user identity sources.

Sample identity policies and rules

These sections provide examples of configuring an identity policy with either a passive authentication rule or an active authentication rule. In addition, because you can authenticate users with active authentication using either realms or realm sequences, separate examples are provided.

Authentication types

Active authentication means the user authenticates using the captive portal; the user enters network credentials before being allowed to access allowed resources. (RA-VPN is another type of active authentication but it cannot be used together with captive portal authentication. For more information, see Remote access VPN identity sources.)

Passive authentication covers all other types. Passive authentication includes using Microsoft Active Directory realms, Microsoft Azure Active Directory realms, Cisco Identity Services Engine, and others.

You can use a Microsoft Azure Active Directory realm to authenticate users a different way that is not discussed here. For more information, see Create a Microsoft Azure AD (SAML) realm.

These examples use these assumptions:

- Microsoft Active Directory (AD) realm named forest.example.com with two child domains configured in a trust relationship:
  - US-West
  - US-East
- A realm sequence named US that includes both realms
- Passive authentication rule that authenticates users with a realm sequence
- Two active authentication rules:
  - One rule that authenticates users with a realm and uses the NTLM authentication protocol
  - One rule that authenticates users with a realm sequence and uses the HTTP Response Page authentication protocol

- Each sample identity rule is associated with a different identity policy

When you configure a Passive Authentication identity rule, you can choose to authenticate users either with LDAP, a Microsoft Active Directory realm, or a Microsoft AD realm sequence. You can use a realm to authenticate with any authentication type; realm sequence restricts the authentication types you can use. For an example, see Create an identity policy with a passive authentication rule, on page 15.

When you configure an Active Authentication identity rule, you can choose to authenticate users either with LDAP, a Microsoft Active Directory realm, or a Microsoft AD realm sequence. You can use a realm to authenticate with any authentication type; realm sequence restricts the authentication types you can use.

You can also authenticate users with a Microsoft Active Directory realm sequence except for these authentication types:

- NTLM
- Kerberos
- HTTP Negotiate

For an example, see Create a sample identity policy with an active authentication rule, on page 16.

Create an identity policy with a passive authentication rule

Create an identity policy that authenticates users using passive authentication with realm sequences for user identification.

This task discusses how to create an identity policy with a passive authentication rule that authenticates users using the US realm sequence. If a user is not found in the first realm in the sequence, the system searches the other realms in the sequence in the order listed in the realm sequence. If a user is still not found in the realm or realm sequence, the user is identified as Unknown.

You can optionally authenticate a user with the captive portal (that is, active authentication) if the user is not found in any realm in the sequence. For more information, see Best practices for captive portal guidelines and limitations.

Procedure

Step 1 Log in to the Firewall Management Center.

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

Step 3 Click **New Policy**.

a) Enter a **Name** for the policy and an optional **Description**.
b) Click **Save**.

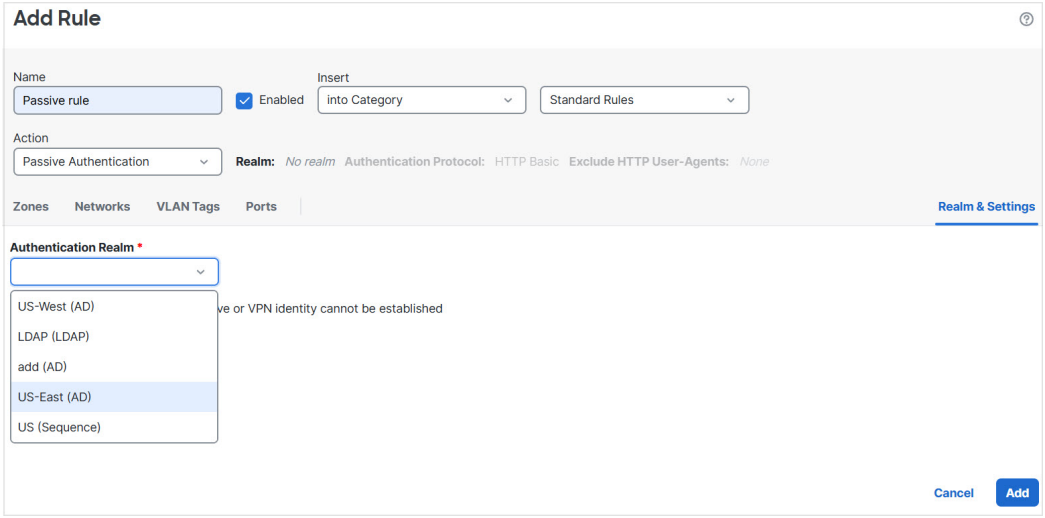
Step 4 Click **Add Rule**.

a) Enter a **Name** for the rule.
b) From the list, click **Passive Authentication**.

Step 5 Click the **Realms & Settings** tab page.

a) From the list, click the name of a realm or realm sequence.

The following figure shows an example.



- If you choose a realm (such as **US-East** in the example), the system searches that realm for users to match the rule. If a user is not found, the user is identified as Unknown.
- If you choose a realm sequence (**US (Sequence)** in the example), users are searched in every realm in the sequence in the order specified in the sequence. If the user is not found, the user is identified as Unknown.
- You can also choose an LDAP realm.
- For additional ways to authenticate the user, check **Use active authentication if passive or VPN identity cannot be established**. For more information, see Best practices for captive portal guidelines and limitations.

Step 6 (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 7 Set identity rule conditions as discussed in Identity rule conditions, on page 5.

Step 8 Associate the identity policy with an access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control.

Deploy configuration changes to managed devices; see Deploy configuration changes.

Create a sample identity policy with an active authentication rule

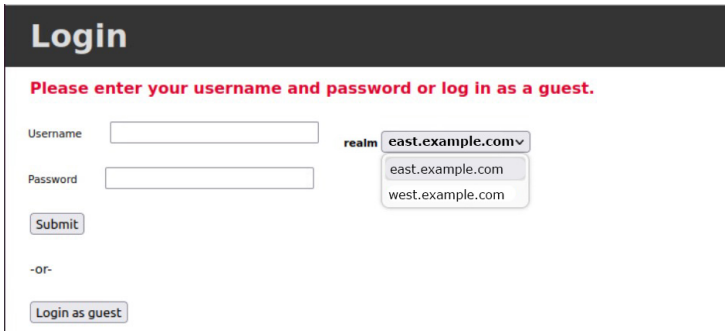
This task shows you how to configure an identity policy with an Active Authentication rule where authentication is performed using either a realm or a realm sequence. This enables secure network access management through customizable captive portal settings.

The associated tasks show examples of configuring an identity policy with an **Active Authentication** rule where authentication is performed using either a realm or a realm sequence.

The differences follow:

- *Realm* enables you to use any supported authentication type (currently, **HTTP Basic**, **NTLM**, **Kerberos**, **HTTP Negotiate**, or **HTTP Response Page**).
- *Realm sequence* limits you to only the **HTTP Basic** or **HTTP Response Page** authentication types.

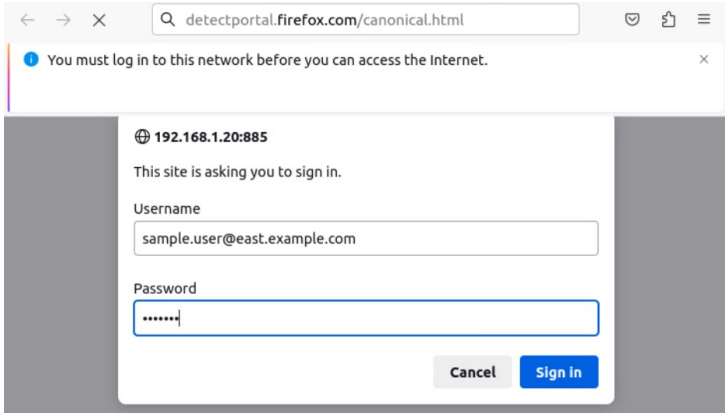
  Users who authenticate with a realm sequence and the HTTP Response Page authentication type see the following by default:



  The user can authenticate in any of the following ways:

  - If a list of realms in the realm sequence is displayed (as shown), the user must enter their user name and password in the provided fields and click the name of their realm from the list.
  - If realms are not displayed in a list, the user can enter their credentials in `username@domain` format.

  Users who authenticate with a realm and the HTTP Basic authentication page see the following:



  The user must enter their user name in `username@domain` format.

Procedure

Step 1 Log in to the Firewall Management Center.

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

Step 3 Click **New Policy**.

a) Enter a **Name** for the policy and an optional **Description**.

b) Click **Save**.

Step 4 Click the **Active Authentication** tab.

Enter the following information:

- **Server Certificate**: From the list, click an internal certificate object to use for secure connection to the Firewall Threat Defense device, or click **Add** (+) to add one.
- **Redirect to Host Name**: (Optional.) From the list, click a network object to which to redirect captive portal requests. If you omit this value, requests redirect to the IP address of the managed device. You can click **Add** (+) to create a new network object. For more information, see Redirect to host name network rule conditions, on page 6.

  Managed devices must have Snort 3 enabled to use this option.
- **Port**: Enter a port for the captive portal to use. This port must be unique for the captive portal and must match an access control rule you set up as discussed in Create a TCP port access control rule. (Default is 885.)
- **Maximum login attempts**: Enter the maximum number of login attempts before login fails. (Default is 3.)
- **Share active authentication sessions across firewalls**: Uncheck to enable the Firewall Management Center to force users to reauthenticate every time they access your network using a different managed device than the last time.

  For more information about this option, see Captive portal fields.
- **Active Authentication Response Page**: Choose a system-provided or custom login page for captive portal users. For more information about your options, see Captive portal fields.

Step 5 Click **Save** to save your changes to the identity policy.

Step 6 Click the **Rules** tab.

Step 7 Click **Add Rule**.

a) Enter a **Name** for the rule.
b) From the list, click **Active Authentication**.

Step 8 Click the **Realms & Settings** tab page. Then configure an active authentication method for the users.

What to do next

Continue with one of the following sections:

- Active authentication using a realm, on page 18
- Active authentication using a realm sequence, on page 19

Active authentication using a realm

This task authenticates captive portal users with a realm and any available authentication protocol (currently, **HTTP Basic**, **NTLM**, **Kerberos**, **HTTP Negotiate**, or **HTTP Response Page**).

Active authentication using a realm provides secure user verification for captive portal access by integrating with your organization's authentication infrastructure.

Before you begin

Complete the task discussed in Create a sample identity policy with an active authentication rule, on page 16.

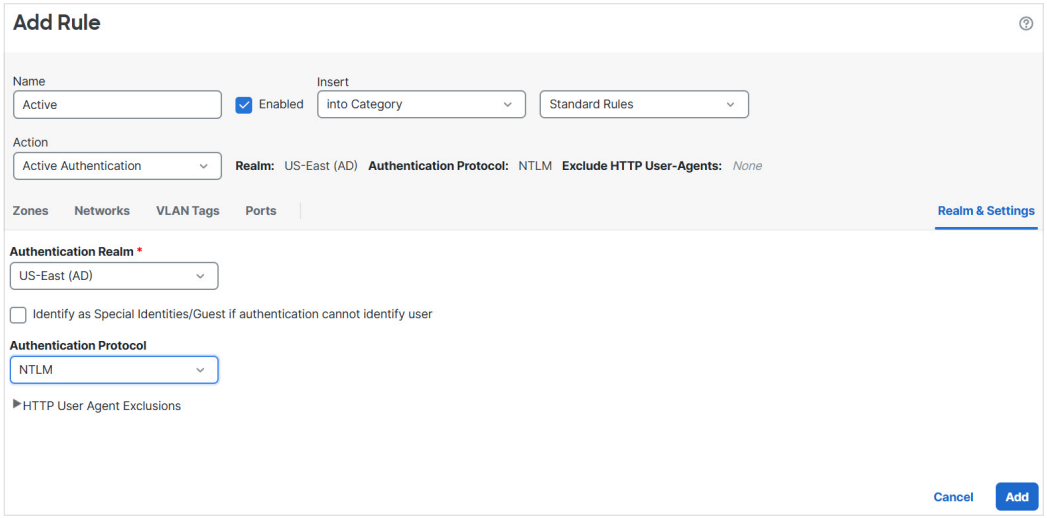
Procedure

Step 1 Continue from Create a sample identity policy with an active authentication rule, on page 16.

Step 2 On the **Realms & Settings** tab page, click **US-East**.

Step 3 From the **Authentication Protocol** list, click **NTLM**.

The following figure shows an example.



If you choose a realm (such as in the example), the system searches that realm for users to match the rule. If a user is not found, the user is identified as Unknown.

Step 4 Click **Add**.

Step 5 (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 6 Set identity rule conditions as discussed in Identity rule conditions, on page 5.

Step 7 Associate the identity policy with an access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control.

Step 8 Deploy configuration changes to managed devices; see Deploy configuration changes.

Active authentication using a realm sequence

This task enables authentication of captive portal users using a realm sequence, allowing you to control access through HTTP Basic or HTTP Response Page protocols. It helps you select realms, set identity rule conditions, and associate them with access control rules to filter network traffic and manage user identification.

This task discusses how to authenticate captive portal users with a realm sequence, which restricts you to the **HTTP Basic** or **HTTP Response Page** authentication protocols.

Before you begin

Complete the task discussed in Create a sample identity policy with an active authentication rule, on page 16.

Procedure

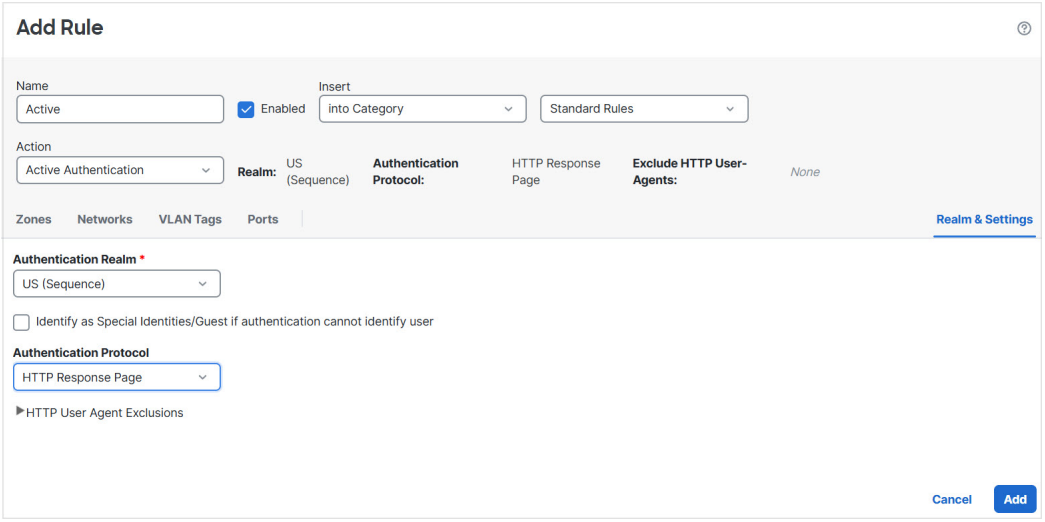
Step 1 Continue from Create a sample identity policy with an active authentication rule, on page 16.

Step 2 On the **Realms & Settings** tab page, click the name of a realm from the list.

Step 3 From the list, click **US-East**.

Step 4 From the **Protocol** list, click **HTTP Response Page**.

The following figure shows an example.



If you choose a realm sequence (such as in the example), the system searches realms in the sequence in the order specified in the realm sequence. The first realm in the sequence can be referred to as the *default* realm; it's the realm that is used if the user does not change it. If a user is not found, the user is identified as Unknown.

(Only if you upgraded to version 7.4.1 from an earlier version.) Edit the HTTP response page so it shows the list of realms in the sequence as discussed in Update a custom authentication form.

Step 5 Click **Add**.

Step 6 (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 7 Set identity rule conditions as discussed in Identity rule conditions, on page 5.

Step 8 Associate the identity policy with an access control policy as discussed in Associate prefilter, decryption, and identity policies with an access control.

Step 9 Deploy configuration changes to managed devices; see Deploy configuration changes.

Manage an identity policy

This task allows you to manage identity policies by performing various administrative actions including editing, deleting, copying, generating reports, and organizing policies into categories for optimized security policy administration.

Identity policies control access to network resources based on user identity. Managing these policies effectively ensures proper security enforcement and administrative organization within the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Security policies** > **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 3. 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 Generate current policy reports.

Step 7 To compare policies, see Compare policies.

Step 8 To create a folder in which to organize policies, click **Add Category**.

What to do next

Deploy configuration changes; see Deploy configuration changes.

Manage an identity rule

This task allows you to edit, delete, or organize identity rules in access control policies to manage user access and security within the Secure Firewall Management Center.

Use this procedure to modify existing identity rules, remove unnecessary rules, or organize rules using categories to maintain effective security policies.

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Policies** > **Security policies** > **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 3.

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.

Troubleshoot user control

If you notice unexpected user rule behavior, consider tuning your rule, identity source, or realm configurations. For other related troubleshooting information, see:

- Troubleshoot Cisco ISE/ISE-PIC or Cisco TrustSec issues
- Troubleshoot the TS agent identity source
- Troubleshoot the captive portal identity source
- Troubleshoot realms and user downloads

Rules targeting realms, users, or user groups are not matching traffic

If you configure a TS Agent or ISE/ISE-PIC device to monitor a large number of user groups, or if you have a very large number of users mapped to hosts on your network, the system may drop user records due to your Firewall Management Center user limit. As a result, rules with user conditions may not match traffic as expected.

Rules targeting user groups or users within user groups are not matching traffic as expected

If you configure a rule with a user group condition, your LDAP or Active Directory server must have user groups configured. The system cannot perform user group control if the server organizes the users in basic object hierarchy.

Rules targeting users in secondary groups are not matching traffic as expected

If you configure a rule with a user group condition that includes or excludes users who are members of a secondary group on your Active Directory server, your server may be limiting the number of users it reports.

By default, Active Directory servers limit the number of users they report from secondary groups. You must customize this limit so that all of the users in your secondary groups are reported to the Firewall Management Center and eligible for use in rules with user conditions.

Rules are not matching users when seen for the first time

After the system detects activity from a previously-unseen user, the system retrieves information about them from the server. Until the system successfully retrieves this information, activity seen by this user is *not* handled by matching rules. Instead, the user session is handled by the next rule it matches (or the policy's default action, if applicable).

For example, this might explain when:

- Users who are members of user groups are not matching rules with user group conditions.
- Users who were reported by a TS Agent or ISE device are not matching rules, when the server used for user data retrieval is an Active Directory server.

Note that this might also cause the system to delay the display of user data in event views and analysis tools.

Rules are not matching all ISE/ISE-PIC users

This is expected behavior. You can perform user control on ISE/ISE-PIC users who were authenticated by an Active Directory domain controller. You cannot perform user control on ISE/ISE-PIC users who were authenticated by an LDAP, RADIUS, or RSA domain controller.

Users and groups using too much memory

If processing users and groups is using too much memory, health alerts are displayed. Remember that all user sessions are propagated to all devices managed by the Firewall Management Center. If your Firewall Management Center manages devices with different amounts of memory, the device with the least amount of memory determines the number of user sessions the system can handle without errors.

It's not possible to tune memory allocated to identity processes; even if a device has available memory, it can report out-of-memory issues. If issues persist, you have these options:

- Segregate lower capacity managed devices on subnets and configure ISE/ISE-PIC to not report passive authentication data to those subnets.

  See the chapter on managing network devices in the *Cisco Identity Services Engine Administrator Guide*.

- Unsubscribe from Security Group Tags (SGTs).

  For more information, see Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.

- Upgrade your managed device to a model with more memory.

Identity synchronization issues

If your managed devices display missing or incomplete identity information, fail to handle user traffic properly, or exhibit unexpected identity-related behavior, resynchronize the user identities. The **Resynchronize identity** functionality synchronizes the user identities from Firewall Management Center to your managed devices.

Use the **Resynchronize identity** option only if standard troubleshooting steps do not resolve the problem, as this action is intended as a last resort. If identity information on managed devices becomes incomplete, inconsistent, or out of sync, this functionality reinitializes the identity feed connections on the device. Ongoing user sessions might be interrupted briefly.

We recommend that you generate the troubleshooting files for the Firewall Management Center and the managed devices before resynchronizing identities.

Note Devices must run version 10.1 or later to use the **Resynchronize identity** feature.

For information on how to resynchronize the identities from Firewall Management Center to your managed devices, refer to Resynchronize identity.

Resynchronize identities

Use the **Resynchronize Identity** function to resynchronize the identities from Firewall Management Center to your managed devices.

If identity information on your managed devices becomes incomplete, inconsistent, or out of sync,the **Resynchronize Identity** functionality reinitializes the identity feed connections on the devices. Note that ongoing user sessions may be temporarily interrupted during reinitialization.

Before you begin

Make sure that the devices run version 10.1 or later.

Procedure

Step 1 Choose **Device** > **Device Management**.

Step 2 For a cluster, do *one* of these steps:

- Use the check box to select the cluster and select **Resynchronize identity** from the **Select Action** list in the top menu bar.
- Click **Edit** ( ) for the cluster. In the **Device** tab of the cluster details page, click **Resynchronize identity**.

Step 3 For a High Availability (HA) pair, do *one* of these steps:

- Use the check boxes to select the managed devices, then select **Resynchronize identity** from the **Select Action** list in the top menu bar.
- Next to the HA device, click **Edit** ( ). In the **Summary** tab of the HA pair details page, click **Resynchronize identity**.

Step 4 For a managed device, *one* of these steps:

- Click the ellipsis icon next to the device name and select **Resynchronize identity** from the list.
- Click the device name.

  In the device details page, select the **Summary** tab and click **Resynchronize identity** for the **Identity feeds** setting.

Step 5 To view the resynchronization status, click **Notifications** > **Tasks**.

The identity feed connections on the device are reinitialized. During the reinitialization, ongoing user sessions might be interrupted briefly.