ISE/ISE-PIC Identity Source, page 33-4

User Identity Sources

The ASA FirePOWER module supports the following identity sources:

- Authoritative *User Agent* reporting collects user data for user awareness and user access control. If you want to configure User Agents to monitor users when they log in and out of hosts or authenticate with Active Directory credentials, see The User Agent Identity Source, page 33-3.
- Authoritative *Identity Services Engine (ISE)* or *ISE-PIC* reporting collects user data for user awareness and user access control. If you have an ISE/ISE-PIC deployment and you want to configure ISE/ISE-PIC to monitor users as they authenticate via Active Directory domain controllers (DC), see The ISE/ISE-PIC Identity Source, page 33-4.
- Authoritative *captive portal authentication* actively authenticates users on your network and collects user data for user awareness and user control. If you want to configure virtual routers or Firepower Threat Defense devices to perform captive portal authentication, see The Captive Portal Active Authentication Identity Source, page 33-7.

Data from those identity sources is stored in the ASA FirePOWER module users database and the user activity database.You can configure database-server queries to automatically download new data to your module.

For more information about user detection in the ASA FirePOWER module, see User Detection Fundamentals, page 31-1.

Troubleshooting Issues with User Identity Sources

License: Any

See the following sections for information about troubleshooting issues with your identity sources.

User Agent

If you experience issues with the User Agent connection, see the *Firepower User Agent Configuration Guide*.

If you experience issues with user data reported by the User Agent, note the following:

- After the system detects activity from a User Agent user whose data is not yet in the database, the system retrieves information about them from the server. In some cases, the system requires up to 60 minutes to successfully retrieve this information from Active Directory servers. Until the data retrieval succeeds, activity seen by the User Agent user is handled by access control rules, and is not displayed in the web interface.

ISE/ISE-PIC

If you experience issues with the ISE/ISE-PIC connection, check the following:

- The pxGrid Identity Mapping feature within ISE must be enabled before you can successfully integrate ISE with the Firepower System.
- All ISE system certificates and Firepower Management Center certificates must include the **serverAuth** and **clientAuth** extended key usage values.
- The time on your ISE device must be synchronized with the time on the Firepower Management Center. If the appliances are not synchronized, the system may perform user timeouts at unexpected intervals.
- If your deployment includes a primary and a secondary pxGrid node, the certificates for both nodes must be signed by the same certificate authority.
- If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.

If you experience issues with user data reported by ISE/ISE-PIC, note the following:

- After the system detects activity from an ISE user whose data is not yet in the database, the system retrieves information about them from the server. In some cases, the system requires up to 60 minutes to successfully retrieve this information from Active Directory servers. Until the data retrieval succeeds, activity seen by the ISE user is handled by access control rules, and is not displayed in the web interface.
- You cannot perform user control on ISE users who were authenticated by an LDAP, RADIUS, or RSA domain controller.
- The ASA FirePOWER module does not receive user data for ISE Guest Services users.
- Your ISE version and configuration impact how you can use ISE in the Firepower System. For more information, see The ISE/ISE-PIC Identity Source, page 33-4.
- ISE-PIC does not provide ISE attribute data.

Captive Portal

If you experience issues with captive portal authentication, note the following:

- The time on your captive portal server must be synchronized with the time on the ASA FirePOWER module.
- If you have DNS resolution configured and you create an identity rule to perform Kerberos (or HTTP Negotiate, if you want Kerberos as an option) captive portal, you must configure your DNS server to resolve the fully qualified domain name (FQDN) of the captive portal device. The FQDN must match the hostname you provided when configuring DNS.

  For ASA with FirePOWER Services devices, the FQDN must resolve to the IP address of the routed interface used for captive portal.
- If you select Kerberos (or HTTP Negotiate, if you want Kerberos as an option) as the **Authentication Type** in an identity rule, the **Realm** you select must be configured with an **AD Join Username** and **AD Join Password** in order to perform Kerberos captive portal active authentication.

- If you select HTTP Basic as the **Authentication Type** in an identity rule, users on your network may not notice their sessions time out. 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.
- If the device you want to use for captive portal contains both inline and routed interfaces, you must configure a zone condition in your captive portal identity rules to target only the routed interfaces on the captive portal device.

The User Agent Identity Source

License: Any

The User Agent is a passive authentication method and one of the authoritative identity sources supported by the ASA FirePOWER module. When integrated with the ASA FirePOWER module, the agent monitors users when they log in and out of hosts or authenticate with Active Directory credentials. The User Agent does not report failed login attempts. The data gained from the User Agent can be used for user awareness and user control. You invoke passive authentication in your identity policy.

Installing and using User Agents allows you to perform user control; the agents associate users with IP addresses, which allows access control rules with user conditions to trigger. You can use one agent to monitor user activity on up to five Active Directory servers.

The User Agent requires a multi-step configuration, and includes the following:

- Computers or servers with the agent installed.
- Connections between an ASA FirePOWER module and the computers or Active Directory servers with the agent installed.
- Connections between the ASA FirePOWER module and the monitored LDAP servers, configured as directories within identity realms.

For detailed information about the multi-step User Agent configuration and a complete discussion of the server requirements, see the *User Agent Configuration Guide*.

The ASA FirePOWER module connection not only allows you to retrieve metadata for the users whose logins and logoffs were detected by User Agents, but also is used to specify the users and groups you want to use in access control rules. If the agent is configured to exclude specific user names, login data for those user names are not reported to the ASA FirePOWER module. User agent data is stored in the user database and user activity database on the device.

Note User Agents cannot transmit Active Directory user names ending with the `$` character to the ASA FirePOWER module. You must remove the final `$` character if you want to monitor these users.

If multiple users are logged into a host using remote sessions, the agent may not detect logins from that host properly. For information about how to prevent this, see the *User Agent Configuration Guide*.

Configuring a User Agent Connection

License: Control

Before you Begin

- If you plan to implement user access control, configure and enable an Active Directory realm for your User Agent connection as described in Creating a Realm, page 32-4

To configure a User Agent Connection:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration > Identity Sources**.

Step 2 Select **User Agent** for the **Service Type** to enable the User Agent connection.

Note To disable the connection, select **None**.

Step 3 Click the **Add New Agent** button to add a new agent.

Step 4 Type the **Hostname** or **Address** of the computer where you plan to install the agent. You must use an IPv4 address; you cannot configure the ASA FirePOWER module to connect to a User Agent using an IPv6 address.

Step 5 Click **Add**.

Step 6 To delete a connection, click the delete icon ( ) and confirm that you want to delete it.

What to Do Next

- Continue User Agent setup as described in the *Firepower User Agent Configuration Guide*.

The ISE/ISE-PIC Identity Source

License: Any

You can integrate your Cisco Identity Services Engine (ISE) or ISE Passive Identity Connector (ISE-PIC) deployment with the ASA FirePOWER module to use ISE/ISE-PIC for passive authentication. You invoke passive authentication in your identity policy.

ISE/ISE-PIC is an authoritative identity source, and provides user awareness data for users who authenticate via Active Directory (AD), LDAP, RADIUS, or RSA. Additionally, you can perform user control on AD users. ISE/ISE-PIC does not report failed login attempts or the activity of ISE Guest Services users.

Note The ASA FirePOWER module does not support 802.1x machine authentication alongside AD authentication, because the system does not associate machine authentication with users. If you use 802.1x active logins, configure ISE to report only 802.1x active logins (both machine and user). That way, a machine login is reported only once to the system.

For more information on Cisco ISE/ISE-PIC, see the *Cisco Identity Services Engine Administrator Guide* and the *Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*.

Your ISE/ISE-PIC version and configuration affects its integration and interaction with the ASA FirePOWER module, as follows:

- Synchronize the time on the ISE/ISE-PIC server and the ASA FirePOWER module. Otherwise, the system may perform user timeouts at unexpected intervals.
- If you configure ISE/ISE-PIC to monitor a large number of user groups, the system may drop user mappings based on groups, due to memory limitations. As a result, access control rules with realm or user conditions may not fire as expected.

- Version 2.0 patch 4 of ISE includes support for IPv6-enabled endpoints.
- ISE-PIC does not provide ISE attribute data.

For the specific versions of ISE/ISE-PIC that are compatible with this version of the ASA FirePOWER module, see the *Cisco Firepower Compatibility Guide*.

Configuring an ISE connection populates the ASA FirePOWER module database with ISE attribute data. You can use the following ISE attributes for user awareness and user control. This is not supported with ISE-PIC.

Security Group Tags (SGT)

The Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) automatically generates the SGT when a user adds a security group in TrustSec or ISE. SGA then applies the SGT attribute as packets enter the network. You can use SGTs for access control by configuring ISE as an identity source or creating custom SGT objects. For more information, see ISE SGT v. Custom SGT Rule Conditions, page 10-1.

SGT ISE attribute rule conditions can be configured in policies with or without an associated identity policy.

Endpoint Location (also known as the Location IP)

The Endpoint Location attribute is applied by Cisco ISE and identifies the IP address of the endpoint device.

You can only configure Location IP as an ISE attribute rule condition in policies with an associated identity policy.

Endpoint Profile (also known as the Device Type)

The Endpoint Profile attribute is applied by Cisco ISE and identifies the endpoint device type for each packet.

You can only configure Device Type as an ISE attribute rule condition in policies with an associated identity policy.

ISE/ISE-PIC Fields

The following fields are used to configure a connection to ISE/ISE-PIC.

Primary and Secondary Host Name/IP Address

The hostname or IP address for the primary and, optionally, the secondary ISE servers.

pxGrid Server CA

The certificate authority for the pxGrid framework. If your deployment includes a primary and a secondary pxGrid node, the certificates for both nodes must be signed by the same certificate authority.

MNT Server CA

The certificate authority for the ISE certificate when performing bulk downloads. If your deployment includes a primary and a secondary MNT node, the certificates for both nodes must be signed by the same certificate authority.

MC Server Certificate

The certificate and key that the ASA FirePOWER module should provide to ISE when connecting to ISE or performing bulk downloads.

The **MC Server Certificate** must include the **clientAuth** extended key usage value, or it must not include any extended key usage values.

ISE Network Filter

An optional filter you can set to restrict the networks monitored by ISE. If you provide a filter, ISE monitors the networks within that filter. You can specify a filter in the following ways:

- Leave the field blank to specify any.
- Enter a single IPv4 address block using CIDR notation.
- Enter a list of IPv4 address blocks using CIDR notation, separated by commas.

Note This version of the Firepower System does not support filtering using IPv6 addresses, regardless of your ISE version.

Configuring an ISE/ISE-PIC Connection

License: Control

Before You Begin

- Configure a realm as described in Creating a Realm, page 32-4. A user download (automatic or on-demand) must be performed before you can configure an ISE attribute condition in an access control rule.

Note Configuring a realm is optional if you plan to configure SGT ISE attribute conditions but not user, group, realm, Endpoint Location, or Endpoint Profile conditions.

To configure an ISE/ISE-PIC Connection:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Integration** > **Identity Sources**.

Step 2 Select **Identity Services Engine** for the **Service Type** to enable the ISE/ISE-PIC connection.

Note To disable the connection, select **None**.

Step 3 Type a **Primary Host Name/IP Address** and, optionally, a **Secondary Host Name/IP Address**.

Step 4 Select the appropriate certificates from the **pxGrid Server CA**, **MNT Server CA**, and **MC Server Certificate** drop-down lists. Optionally, click the add icon ( ) to create an object on the fly.

Step 5 Optionally, type an **ISE Network Filter** using CIDR block notation.

Step 6 If you want to test the connection, click **Test**.

The Captive Portal Active Authentication Identity Source

License: Any

Captive portal is one of the authoritative identity sources supported by the ASA FirePOWER module. It is the only active authentication method supported by the ASA FirePOWER module, where users can authenticate onto the network through a device.

Active authentication via captive portal is performed on HTTP and HTTPS traffic only. If you want to perform captive portal on HTTPS traffic, you must create SSL rules to decrypt the traffic originating from the users you want to authenticate using captive portal.

When configured and deployed, users from specified realms authenticate through ASA FirePOWER devices in routed mode running Version 9.5(2) or later. The authentication data gained from captive portal can be used for user awareness and user control.

Captive portal also records failed authentication attempts. A failed attempt does not add a new user to the list of users in the database. The user activity type for failed authentication activity reported by captive portal is **Failed Auth User**.

You use the `captive-portal` ASA CLI command to enable captive portal for active authentication as described in the *ASA Firewall Configuration Guide* for your version: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html. You continue configuring captive portal in your identity policy and invoke it (active authentication) in your identity rules. Identity policies are invoked in your access control policies. For more information, see Configuring Captive Portal (Active Authentication), page 32-10

Captive portal can only be performed by a device with one or more routed interfaces configured.

Note the following access control rule and SSL rule requirements:

- You must create an access control rule to allow traffic destined for the IP address and port you plan to use for captive portal. Traffic cannot be authenticated using captive portal if the destination port is not allowed in your access control policy.
- If you want to perform active authentication via captive portal on HTTPS traffic, you must create SSL rules to decrypt the traffic originating from the users you want to authenticate using captive portal.
- If you want to decrypt traffic in the captive portal connection, you must create an SSL rule to decrypt the traffic destined for the port you plan to use for captive portal.

ASA FirePOWER Module-Server Downloads

License: Any

Connections between the ASA FirePOWER module and your LDAP or AD servers allow you to retrieve user and user group metadata for certain detected users:

- LDAP and AD users authenticated by captive portal or reported by a User Agent or ISE/ISE-PIC. This metadata can be used for user awareness and user control.
- POP3 and IMAP user logins detected by traffic-based detection, if those users have the same email address as an LDAP or AD user. This metadata can be used for user awareness.

You configure an ASA FirePOWER module user database-server connection as a directory within a realm. You must select the **Download users and user groups for access control** check box to download a realm's user and user group data for user awareness and user control.

The ASA FirePOWER module obtains the following information and metadata about each user:

- LDAP user name
- first and last names
- email address
- department
- telephone number