Managing Identity-Aware Firewall Policies

Identity-aware firewall policies allow you to control traffic based on user identity or a host's fully-qualified domain name. For example, you can selectively allow a specific type of traffic for one user group while disallowing it for another user group, instead of allowing or disallowing all of that traffic. With fully-qualified domain names, you could disallow HTTP access to a specific server while allowing HTTP traffic to all other servers.

Identity awareness is integrated into several existing firewall rules; there is no unique identity-aware firewall policy. This chapter explains identity-aware firewall policies and how to implement them in the various policies that support identity awareness.

This chapter contains the following topics:

Overview of Identity-Aware Firewall Policies

In traditional firewall policies, decisions are made based on source and destination IP addresses, ports, and services. The Identity Firewall in the ASA provides more granular control based on either or both of the following:

- User identity—You can configure access rules and security policies based on user names and user group names rather than through source IP addresses alone. The ASA applies the security policies based on an association of IP addresses to Windows Active Directory login information and reports events based on the mapped user names instead of network IP addresses.

  The Identity Firewall integrates with Microsoft Active Directory in conjunction with an external Active Directory (AD) agent that provides the actual identity mapping. The ASA uses Windows Active Directory as the source to retrieve the current user identity information for specific IP addresses and allows transparent authentication for Active Directory users. For information on setting up and configuring the AD agent, see *Installation and Setup Guide for the Active Directory Agent* on Cisco.com at http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html.
- FQDN network objects—You can use a host's fully-qualified domain name (FQDN) in a rule instead of its IP address. Thus, if the host's address changes (for example, because it acquires the address through DHCP), the rule will still apply.

Identity-based firewall services enhance the existing access control and security policy mechanisms by allowing users or groups to be specified as sources, and FQDNs in place of source or destination IP addresses. Identity-based security policies can be interleaved without restriction between traditional IP address based rules.

The key benefits of the Identity Firewall include:

- Decoupling network topology from security policies. The rules will apply to a user regardless of where the user connects in the network.
- Simplifying the creation of security policies.
- Providing the ability to easily identify user activities on network resources.
- Simplify user activity monitoring.

This section contains the following topics:

User Identity Acquisition

When you specify Active Directory user names or user group names in a firewall policy, the ASA eventually needs to map the name to an IP address to process packets. The ASA uses two primary sources for this information:

- User group membership—If you specify a user group in a rule, the ASA contacts the configured Active Directory (AD) server to obtain group membership.
- User-to-IP address mappings—For users who log into the network domain on your standard (non-VPN) network, the AD agent, in communication with the AD server, obtains the login information and creates a user-to-IP address mapping table. This information is supplied to the ASA.

You must install and configure the required AD servers and agents before you can configure user-based identity firewall policies. For an explanation of the various deployment scenarios, see the ASA configuration guide for ASDM or CLI at http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html.

User names are acquired for the following types of traffic, and include the AD domain unless noted otherwise:

- Standard traffic.
- Remote access VPN, including IPsec IKEv1 and IKEv2, AnyConnect clients, and L2TP VPN. If you use LDAP authentication for the VPN, and use the same server group for a domain for the VPN and identity firewall, the users are associated with the domain used for authentication. For all other authorization mechanisms, users acquired through VPN are considered to be in the LOCAL domain. The ASA reports these users to the AD agent, which distributes them to other ASAs or clients registered with the AD agent.

Note User names are not acquired for clientless SSL VPN.

- IPv4 cut-through proxy. User names are not acquired for IPv6 cut-through proxy. If the user includes the domain name during authentication, the user is associated with the domain name. Otherwise, the domain is the default domain as configured in the Identity Options policy. See Configuring Cut-Through Proxy, page 13-23.

Requirements for Identity-Aware Firewall Policies

Identity-aware firewall policies are not supported by all types of device and operating systems. The following table explains the requirements and some limits for implementing these types of policies in your network.

Table 13-1 Requirements for Identity-Aware Firewall Policies

Requirement	Description
Firewall device	ASA running ASA Software version 8.4(2) or higher, but not including the ASA-SM running 8.5(1). Single or multiple context configurations. **Tip** The ASA must have on-board encryption acceleration. To determine if the device has the required ability, log into the device console and use the **show version** command. The output should include "Encryption hardware device." You can register up to 100 ASAs with a single Active Directory agent.
Active Directory (AD)	You must use Active Directory to define users and user groups. The ASA obtains user group information directly from the AD server, which runs the LDAP protocol. You cannot use other types of LDAP servers. For detailed information on the types of AD servers supported, and their configuration requirements, see *Installation and Setup Guide for the Active Directory Agent* on Cisco.com at http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html. **Tip** You can have multiple AD servers, but they must have unique IP addresses among all domains. No other type of LDAP server is supported.

Table 13-1 Requirements for Identity-Aware Firewall Policies (continued)

Requirement	Description
AD agent	You must configure off-box AD agents to act as an intermediary between the ASA and the AD servers. The AD agent maintains an active mapping of users to IP address. By default, except for the 5505, the ASA obtains this list when it boots or reloads, and the AD agent sends new mappings as they are collected. The 5505 queries the AD agent on an as-needed basis in response to traffic matching rules that include identity criteria. We recommend that you use this default behavior, although you can change it using the Identity Options policy. The AD agent uses the RADIUS protocol. For information on setting up and configuring the AD agent, see *Installation and Setup Guide for the Active Directory Agent* on Cisco.com at http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html.
Client systems	Users who pass traffic through the device must use one of the following client platforms: • Windows XP SP3. • Windows Vista. • Windows 7. • Other systems that use Active Directory in a manner consistent with the explicitly supported platforms.
IPv6	IPv6 is supported with the following exceptions: • NetBIOS over IPv6 is not supported. • Multiple IPv6 addresses on user workstations is not supported. Windows 64-bit systems can use temporary IPv6 addresses when initiating some communications. If a user registers with the AD agent using one IPv6 address, then initiates communication with another address, an identity-aware firewall rule for the user would not be applied and instead a rule that matches the second IPv6 address would be applied. There are two options for disabling the use of these temporary addresses: – Disable IPv6 routing advertisements on all interfaces on all networking devices in the network. – On each Windows machine, open a command window, enter the following commands, and reboot the workstation: **netsh interface ipv6 set privacy state=disable** **netsh interface ipv6 set global randomizeidentifiers=disabled**

Table 13-1 Requirements for Identity-Aware Firewall Policies (continued)

Requirement	Description
NetBIOS logout probing (Optional.)	If you enable NetBIOS logout probing, the ASA can use NetBIOS to determine if an inactive user is logged off so the user can be removed from the database. The probe uses UDP-encapsulated NetBIOS traffic. Thus, you must ensure that access rules allow the following traffic on the networks between the ASA, AD agent, and user workstations: • Query packets: any UDP source port to UDP port 137 (UDP/137). • Query responses: UDP/137 source to any UDP port. In addition, you must configure workstations to provide user name information in NetBIOS reply packets. For Windows workstations, you need to enable the messenger service and configure WINS. If the messenger service is not turned on, the response from the workstation is the same whether the user is logged on or off. **Tips** • The NetBIOS logout probe is never used with VPN or cut-through proxy users. • The ASA has an inactive user timeout that is also used to remove users from the database. The timer applies to all user types. Thus, implementing NetBIOS probing is not required to remove inactive users from the database.

Table 13-1 Requirements for Identity-Aware Firewall Policies (continued)

Requirement	Description
DNS configuration (Required for fully-qualified domain name usage.)	If you use fully-qualified domain name (FQDN) network/host objects in firewall rules, you must configure the domain name system (DNS) settings as described in DNS Page, page 52-14. These settings identify the DNS servers used for looking up the names to determine the associated IP address. All processing is ultimately based on the IP address. When configuring DNS for FQDN usage, consider the following points: • DNS replies can be spoofed, which can open a security hole in your network. Specify only trusted DNS servers, ideally only those inside your network. • Some hosts can have constantly changing multiple IP addresses, so the ASA might not always have all valid IP addresses at any one time. • Host names with short time to live values will require frequent DNS lookups; this can impact the performance of the ASA. • Multiple host names can resolve to the same IP address. Ultimately, the firewall rules are applied based on IP address. Thus, if two names map to the same address, and your rules specify different services for those names, the service that is actually provided will be those specified on the first matched rule. Looked at another way, this means that you do not need to specify every version of an FQDN host name in your rules. When you know that several names always point to the same host, you can configure rules for the most commonly-used name and they will apply to all synonyms of that name.
Maximum limits	There are limits to the number of users, user groups, and IP addresses per user. If these limits are exceeded, identity-aware processing will not occur for the additional traffic: • IP address limits—A user can be associated with at most 8 IP addresses across all domains. • User group limits—Policies can be applied to up to 256 user groups. Users can be in multiple user groups. • User limits—Policies can be applied to up to the following number of users. This number is the total aggregate across all contexts defined on the device. – ASA 5505—1024 users. – Other ASA 5500 series—64,000 users.

Configuring the Firewall to Provide Identity-Aware Services

To provide identity-aware firewall services to your network, you need to configure several policies to enable the firewall to process user-based or fully-qualified domain name (FQDN)-based rules. The ASA depends on other servers in your network to provide the user, user group, and FQDN name resolution services required to implement your identity-aware policies.

The required configuration depends on which aspects of identity awareness that you will use:

- User, user group resolution—To use identity user group objects in your firewall rules, you must configure several objects and policies to identify the Active Directory servers that will supply user and user group information.
- FQDN resolution—To use FQDN network/host objects in your firewall rules, you must configure DNS servers to resolve FQDNs to IP addresses.

This procedure explains the overall process for implementing identity-aware policies.

Before You Begin

Your network must meet the requirements explained in Requirements for Identity-Aware Firewall Policies, page 13-3. The following procedure assumes that you are already using Active Directory (AD), that you have installed and configured the AD agents, and that these services are working correctly.

Step 1 Enable AD user and user group resolution.

a. Create the policy objects needed to identify the AD servers and agents and configure the NetBIOS domain for the server groups. For detailed information, see Identifying Active Directory Servers and Agents, page 13-8.

b. If you want non-default settings, change the identity options. Use these options to enable the NetBIOS logout probe and to configure various timers and error handling. For detailed information, see Configuring Identity Options, page 13-15.

c. If you want to create user groups defined on the ASA (in addition to AD-defined user groups), create the required identity user group policy objects. See Creating Identity User Group Objects, page 13-19.

Step 2 Enable FQDN network/host object resolution.

a. Configure DNS servers in the DefaultDNS group. DNS is required to resolve FQDNs to IP addresses. For information on configuring DNS, see DNS Page, page 52-14.

b. Create FQDN network/host objects as described in Creating Networks/Hosts Objects, page 6-82.

Step 3 Configure firewall rules to use FQDN objects, usernames, user group names, or identity user group objects. See Configuring Identity-Based Firewall Rules, page 13-21.

Step 4 Monitor the identity firewall system. See Monitoring Identity Firewall Policies, page 13-27.

Configuring Identity-Aware Firewall Policies

Identity awareness is integrated into several existing firewall rules; there is no unique identity-aware firewall policy. The topics in this section explain the various procedures for integrating identity awareness into firewall policies.

This section contains the following topics:

Enabling Identity-Aware Firewall Services

Use the Identity Options policy to enable identity-aware firewall services. To configure the policy, do one of the following:

- (Device view) Select an ASA device, then select **Identity Options** from the Policy selector.
- (Policy view) Select **Identity Options (ASA)** from the Policy selector. Select an existing policy or create a new one.

The policy includes the following tabs:

- **AD Setup**—Configure the Active Directory servers that define the users and user groups for the network, and the AD agent used to collect the information and provide it to the ASA. See Identifying Active Directory Servers and Agents, page 13-8.
- **Advanced**—Enable or disable user identity services and configure options for error handling, the NetBIOS logout probe, idle timeout, and AD agent communication settings. See Configuring Identity Options, page 13-15.

Identifying Active Directory Servers and Agents

Use the AD Setup tab of the Identity Options policy to identify the Active Directory servers and agents to use for user identity information. You must configure at least one AD server and one AD agent to enable identity-aware firewall policies that include user specifications (such as identity user group objects).

Note ASA Software 8.4(2+) is required for identity-aware firewall.

Before You Begin

The configuration uses AAA server group policy objects, and the server group objects incorporate AAA server objects. You can create these objects through the Policy Object Manager (by selecting Manage > Policy Objects), or you can create them while completing this procedure (by using the configuration wizard or by clicking the Add Object + button in the object selector dialog box).

The objects need to meet these requirements:

- AD servers—Must use the LDAP protocol. If you select Microsoft as the LDAP server type, you can also specify the LDAP Group Base DN to identify the base directory for user group searches, to reduce search time. If you select Auto Detect, you cannot configure the group base DN, even though

Microsoft AD servers are the only type of LDAP server that you can use in the identity firewall configuration. You must also abide by the following limitations for communications between Security Manager and Active Directory:

  - Do not select the Enable LDAP over SSL option.
  - Do not select the SASL Kerberos Authentication option. Only simple and SASL MD5 authentication mechanisms are supported. The simple mechanism, in which usernames and passwords are transmitted in clear text, is used if you do not select one of the SASL options.

- AD agents—Must use the RADIUS protocol. In the AAA server group object, select the **AD Agent Mode** option.

  You should install the AD agents and configure them prior to configuring this policy. You can configure at most two AD agents in the server group: the second agent is used only if the first agent ceases to respond to queries. Any agents defined after the first two are ignored.

  Obtain the AD agent software from http://www.cisco.com/go/asa. For information on setting up and configuring the AD agent, see *Installation and Setup Guide for the Active Directory Agent* on Cisco.com.

Related Topics

- Requirements for Identity-Aware Firewall Policies, page 13-3
- Understanding AAA Server and Server Group Objects, page 6-27
- Creating AAA Server Objects, page 6-32
- AAA Server Dialog Box—LDAP Settings, page 6-40
- Creating AAA Server Group Objects, page 6-48
- Configuring Identity Options, page 13-15

Step 1 Do one of the following:

- (Device view) Select an ASA device, then select **Identity Options** from the Policy selector. Select the **AD Setup** tab.
- (Policy view) Select **Identity Options (ASA)** from the Policy selector. Select an existing policy or create a new one. Select the **AD Setup** tab.

Step 2 If you want to be guided through the AD setup, click the **Configure Identity** button to start the Identity configuration wizard. The wizard walks you through the process of configuring the AD servers for a domain, and the AD agents, and can create the required AAA server and AAA server group objects for you.

The wizard goes through the following steps:

- AD Server Settings—To configure the AD servers for a domain. See Identity Configuration Wizard Active Directory Settings, page 13-11.
- AD Agent Settings—To configure the AD agents for the ASA. See Identity Configuration Wizard Active Directory Agent, page 13-13.
- Preview—To show you which objects will be created. See Identity Configuration Wizard Preview, page 13-15.

Tip You can use the wizard multiple times to configure different NetBIOS domains. However, the wizard always prompts for AD agent information. Because you can configure a single group for AD agents, not a separate group per domain, the selection overwrites any AD agent configuration that you have already made. So be sure to select the same AAA server group for the AD agents each time you run the wizard.

Step 3 If not using the wizard, configure the AD servers. The AD servers are used for obtaining user membership information for any AD user groups that you use in identity-aware firewall policies.

The table lists the AD servers for the network. You need to add an entry for each NetBIOS domain name. Each row defines the AAA server group used to identify the AD LDAP servers for the domain, and whether identity-aware firewall rules for the domain are active or inactive if the AD server group is unavailable.

You can do the following:

- To add an entry, click the **Add Row (+)** button and fill in the Add AD Domain Server dialog box. See Domain AD Server Dialog Box, page 13-10.
- To edit an entry, select it and click the **Edit Row (pencil)** button.
- To delete an entry, select it and click the **Delete Row (trash can)** button.

Step 4 If not using the wizard, configure the AD agents. The AD agents obtain user login/logoff and IP address mappings from the AD servers. The ASA then obtains the information from the AD agent.

In **Active Directory Agent Group**, enter the name of the AAA server group object that defines the list of AD agents, or click **Select** to select it from a list or to create a new group object.

Step 5 In **Default Domain**, select the domain to configure as the default domain on the device. You must add the domain to the AD server table before you can select it as the default domain.

The default is LOCAL, which applies to user groups defined on the device or to VPN users who authenticate using a method other than an AD server configured for identity services. This setting is also used if you configure cut-through proxy (see Configuring Cut-Through Proxy, page 13-23).

Step 6 Click **Save** to save your changes.

You are asked if the identity settings page in the administrative settings should be updated with the domain-to-AD server mappings. The identity settings determine which servers are used when you use the Find feature when specifying users or user groups in a firewall policy or an identity user group object. The identity administrative settings do not affect the configuration of the ASA.

Domain AD Server Dialog Box

Use the Add or Edit Domain AD Server dialog box to define the Active Directory server group for a NetBIOS domain. If you configure firewall rules for a user group in the NetBIOS domain, the user membership is determined by querying the AD servers defined for the domain.

Navigation Path

Do one of the following:

- From the AD Setup tab of the Identity Options page, click the Add or Edit buttons for the domain table. See Identifying Active Directory Servers and Agents, page 13-8.

- From the Identity Settings Security Manager Administration page, click the Add or Edit buttons for the settings table. These settings determine which servers are used when using Find to locate a user or user group name when configuring firewall rules or identity user group objects. See Identity Settings Page, page 11-38.

Field Reference

Table 13-2 Domain AD Server Dialog Box

Element	Description
Domain	The NetBIOS domain for this AD server group. The domain name can be up to 32 characters, typically in all uppercase. For example, if the user specification is DOMAIN\user1, DOMAIN is the NetBIOS domain name.
AD Server Group	The name of the AAA server group policy object that identifies the AD servers for this domain. The object must use the LDAP protocol. Click **Select** to select the object or to create a new one.
Disable Rules When Server Is Down (Identity Options policy only.)	Whether to disable all identity-aware firewall rules for this domain if the domain controller is down. If you select this option, all users for a domain are marked as disabled until the server becomes available.
Update Administrative Settings (Identity Options policy only.)	Whether to add the domain and server mapping to the Security Manager Administration Identity Settings page. This administrative page determines which AD servers are queried when you try to find users or user groups when adding them to firewall policies or to identity user group objects. For more information, see Identity Settings Page, page 11-38.

Identity Configuration Wizard Active Directory Settings

Use the Active Directory Settings page of the Identity Configuration wizard to identify the Active Directory (AD) servers for a NetBIOS domain. These settings are required to enable user-identity-aware firewall policies for users in the domain.

Navigation Path

Do one of the following:

- From the AD Setup tab of the Identity Options page, click the **Configure Identity** button. See Identifying Active Directory Servers and Agents, page 13-8.
- If the Identity Options policy is not already configured, you can start the wizard from the AAA Rules, Access Rules, or Inspection Rules policies by clicking the Select button for the User field and then clicking Yes when asked if you want to configure identity.

Field Reference

Table 13-3 Identity Configuration Wizard Active Directory Settings

Element	Description
NetBIOS Domain	The NetBIOS domain for this AD server group. The domain name can be up to 32 characters, typically in all uppercase. For example, if the user specification is DOMAIN\user1, DOMAIN is the NetBIOS domain name.
Select Existing AD Server Group	Select this option if the AAA server group policy object that identifies the required AD servers already exists. The object must use the LDAP protocol. Click **Select** next to the Group Name field to select the object.
Create New AD Server Group	Select this option if the AAA server group policy object does not already exist, or you want the wizard to create a new object. Configure the remaining options to identify the group and the servers that it contains.
Create AD Server Group Properties	
Group Name (When creating the group in the wizard.)	The name of the AAA server group object that you want to create. The name can be up to 16 characters.
AD Server Name/IP	One of the following: • The name of an existing AAA server object that defines the AD server. Click **Select** to select the object from a list. If you select an object, you cannot configure the remaining properties. • The IP address of the AD server.
Username	The name of the user or the directory object in the LDAP hierarchy used for authenticated binding (maximum of 128 characters). Authenticated binding is required by some LDAP servers (including the Microsoft Active Directory server) before other LDAP operations can be performed. This field describes the authentication characteristics of the device. These characteristics should correspond to those of a user with administrator privileges. This string is case-sensitive. Spaces are not permitted in the string, but other special characters are allowed. Typically, this is a username such as DOMAIN\Administrator. However, you can use the more traditional format too, for example, cn=Administrator,OU=Employees,DN=example,DN=com.
Password Confirm	The case-sensitive, alphanumeric password for accessing the LDAP server (maximum of 64 characters). Spaces are not allowed.

Table 13-3 Identity Configuration Wizard Active Directory Settings (continued)

Element	Description
Interface	The interface whose IP address should be used for all outgoing packets (known as the source interface). Enter the name of an interface or interface role, or click **Select** to select it from a list or to create a new interface role. **Tips** • If you enter the name of an interface, make sure the policy that uses this AAA object is assigned to a device containing an interface with this name. • If you enter the name of an interface role, make sure the role represents a single interface, not multiple interfaces. • Only one source interface can be defined for the AAA servers in a AAA server group, so if you specify more than one server, ensure that they all use the same interface.
Add Another AD Server	Click this button only if you want to create an additional server. When you click the button, the information in the server fields is saved and the fields are cleared so that you can add information about the next server. You can add up to 16 servers in single-context mode and 4 servers in multiple-context mode.

Identity Configuration Wizard Active Directory Agent

Use the Active Directory Agent Settings page of the Identity Configuration wizard to identify the Active Directory (AD) agents for a NetBIOS domain. These settings are required to enable user-identity-aware firewall policies for users in the domain.

Tip You can configure a single AD agent group for an ASA; you do not configure a different group for each NetBIOS domain. Thus, if you already configured the correct AD agent group in the Identity Options policy, select the same group on this wizard page. Your selection here will replace the group defined in the policy.

Navigation Path

Do one of the following:

- From the AD Setup tab of the Identity Options page, click the **Configure Identity** button and proceed to this page. See Identifying Active Directory Servers and Agents, page 13-8.
- If the Identity Options policy is not already configured, you can start the wizard from the AAA Rules, Access Rules, or Inspection Rules policies by clicking the Select button for the User field and then clicking Yes when asked if you want to configure identity.

Field Reference

Table 13-4 Identity Configuration Wizard Active Directory Agent Settings

Element	Description
Select Existing AD Agent Group	Select this option if the AAA server group policy object that identifies the required AD agents already exists. The object must use the RADIUS protocol, and should have the option **AD Agent Mode** selected. Click **Select** next to the Group Name field to select the object.
Create New AD Agent Group	Select this option if the AAA server group policy object does not already exist, or you want the wizard to create a new object. Configure the remaining options to identify the group and the servers that it contains.
Create AD Agent Group Properties	
Group Name (When creating the group in the wizard.)	The name of the AAA server group object that you want to create. The name can be up to 16 characters.
AD Agent Name/IP	One of the following: • The name of an existing AAA server object that defines the AD agent. Click **Select** to select the object from a list. If you select an object, you cannot configure the remaining properties. • The IP address of the AD agent.
Secret Key Confirm	The shared secret that is used to encrypt data between the network device (client) and AAA server. The key is a case-sensitive, alphanumeric string of up to 127 characters. Special characters are permitted. The key you define in this field must match the key on the RADIUS server. Enter the key again in the Confirm field. If you do not define a key, all traffic between the AAA server and its AAA clients is sent unencrypted.
Interface	The interface whose IP address should be used for all outgoing packets (known as the source interface). Enter the name of an interface or interface role, or click **Select** to select it from a list or to create a new interface role. **Tips** • If you enter the name of an interface, make sure the policy that uses this AAA object is assigned to a device containing an interface with this name. • If you enter the name of an interface role, make sure the role represents a single interface, not multiple interfaces. • Only one source interface can be defined for the AAA servers in a AAA server group, so if you specify more than one server, ensure that they all use the same interface.

Table 13-4 Identity Configuration Wizard Active Directory Agent Settings (continued)

Element	Description
Add Secondary AD Agent	Click this button only if you want to create an additional agent. The agent is used in case the first agent becomes unavailable. When you click the button, the information in the agent fields is saved and added to the preview pane, and the fields are cleared so that you can add information about the secondary agent.

Identity Configuration Wizard Preview

Use the Preview page of the Identity Configuration wizard to verify the information you entered into the wizard.

The preview summarizes the objects that will be created or used for the Active Directory configuration for the NetBIOS domain.

- AD server group shows the name of the AAA server group object for the AD servers used in the domain. The table shows the AAA server objects that define each of the AD servers.
- AD Agent shows the name of the AAA server group object for the AD agents. The primary and secondary agent shows the AAA server object that defines the agents.

For objects that the wizard will create, names are automatically generated for the AAA server objects, either adding **ldap_** or **radius_** as a prefix to the server IP address.

To make changes, click **Back**. Otherwise, click **Finish** to save the settings.

Tip After you complete the wizard, you can edit the properties of the newly-created objects to configure settings that the wizard left as default settings.

Navigation Path

Do one of the following:

- From the AD Setup tab of the Identity Options page, click the **Configure Identity** button and proceed to this page. See Identifying Active Directory Servers and Agents, page 13-8.
- If the Identity Options policy is not already configured, you can start the wizard from the AAA Rules, Access Rules, or Inspection Rules policies by clicking the Select button for the User field and then clicking Yes when asked if you want to configure identity.

Configuring Identity Options

Use the Advanced tab of the Identity Options policy to enable or disable user identity services and configure options for error handling, the NetBIOS logout probe, idle timeout, and AD agent communication settings. The options on this tab have default values, so you need to change them only if you want to fine-tune the settings for your network.

Navigation Path

- (Device view) Select an ASA device, then select **Identity Options** from the Policy selector. Select the **Advanced** tab.
- (Policy view) Select **Identity Options (ASA)** from the Policy selector. Select an existing policy or create a new one. Select the **Advanced** tab.

Related Topics

- Identifying Active Directory Servers and Agents, page 13-8
- Requirements for Identity-Aware Firewall Policies, page 13-3

Field Reference

Table 13-5 Identity Options Advanced Tab

Element	Description
Enable User Identity	Whether to enable the device to obtain user identity information from the AD agent and AD servers, if they are configured on the **AD Setup** tab. The default is enabled. If you change this option and deploy, the change has the following effect based on the new setting: • Disabled—The entire IP address to user mapping database is flushed and all users without activated user-specific rules are released. The AD agent and servers are no longer queried for updates, and all activated user-identity-based rules will have no effect on traffic. • Enabled—Activated users are recreated gradually through communications with the AD agent. VPN users might need to reauthenticate. Queries to the AD agent and AD server recommence.
Error Conditions	
Disable Rules When Active Directory Agent Is Down	Whether to disable all rules that include user identity if the connection to the AD agent is unavailable. If you select this option, all user-to-IP address mappings are marked disabled and all rules that include user specifications are not applied to traffic. By default the option is disabled.
Remove User IP When NetBIOS Probe Fails	Whether to remove the User's IP address mapping from the database if the NetBIOS probe for the user fails for any reason, whether the probe is somehow blocked in the network or the probe fails because the user is not in operation. The user must log into the workstation again. This option has effect only if you enable the NetBIOS logout probe on this page. By default the option is disabled.
Remove User IP When User's MAC Address is Inconsistent	Whether to check the Media Access Control (MAC) address in each request from a user-mapped IP address to the MAC address in the previous packet. If you select this option, and the MAC address changes between packets, the user-to-IP address mapping is removed from the database, subsequent packets are dropped, and the user must reauthenticate to Active Directory. The AD agent is notified if the user-to-IP mapping is removed due to MAC mismatch. By default this option is enabled. MAC checking occurs only on packets from IP addresses on networks that are directly attached to the ASA. VPN users are not checked.
Track User Not Found	Whether to enable user-not-found tracking. By default, the option is disabled.

Table 13-5 Identity Options Advanced Tab (continued)

Element	Description
NetBIOS Logout Probe	
Enable (NetBIOS Logout Probe)	Whether to enable the NetBIOS logout probe. You can use the probe to proactively determine if a user has logged out of the network, allowing the device to remove the user-to-IP address mapping more quickly than if idle timeout is the only mechanism used for this purpose. By default the probe is disabled, and users are removed only if they are idle for longer than the Idle Timeout value. Users are probed only if they are in the active state and they are used in at least one activated rule. VPN and cut-through proxy users are not probed. The AD agent is notified if the user-to-IP mapping is removed by the NetBIOS logout probe. In addition to configuring the following options, see Requirements for Identity-Aware Firewall Policies, page 13-3.
Probe Timer	The frequency of sending NetBIOS probes to activated users, regardless of whether the user is idle. The default is 15 minutes, the range is 1 to 65535 minutes.
Retry Interval	The frequency of retrying the probe if a response is not received from an IP address, and the number of times the probe should be retried. The default is 3 seconds and 3 retries. The range is 1 to 65535 seconds, for retry count, 1 to 256. If there is no response from the final retry, the user-to-IP address mapping is removed if you selected the **Remove User IP When NetBIOS Probe Fails** option; otherwise, the address is probed during the next interval.
User Name	When a NetBIOS response is received, how to handle the response based on the usernames returned: • **Match Any** (the default)—Any username in the response can match the username in the database for the IP address. If there are multiple names in the response (that is, more than one user is logged into the workstation), if any user in the response matches a user in the database, the probe is considered successful and the mapping is retained. • **User Not Needed**—The usernames in the NetBIOS response are ignored; the query response is sufficient to maintain the user-to-IP address mapping. This option is useful if the messenger service is not turned on in the workstation, in which case the NetBIOS response will not contain usernames. The option is also useful when multiple users log into a workstation. • **Exact Match**—There must be one username in the NetBIOS response, and it must exactly match the username in the user-to-IP address mapping database. If there is more than one user, or if the username does not match, the mapping is removed from the database and the IP address is marked as inactive.

Table 13-5 Identity Options Advanced Tab (continued)

Element	Description
Users	
Idle Timeout	The amount of time, in minutes, to allow the user to be idle before removing the user-to-IP address mapping in the database. Once removed, the user must log in again to update the mapping (for example, by using Ctrl+Alt+Delete to lock the workstation, then log in again). The default is 60 minutes, the range is 1 to 65535 minutes. You can deselect the option to disable idle timeout checking, in which case user-to-IP mappings are not removed due to idleness. VPN and cut-through proxy users are not subject to this timer. The AD agent is not notified if the user-to-IP address mapping is removed due to idle timeout.
Active Directory Agent	
Hello Timer	The frequency of sending Hello packets to the AD agent. The ASA uses Hello packets to obtain ASA replication status and domain status. If the ASA does not receive a response after the final retry, the AD agent is considered down, and the ASA switches to the backup AD agent, if you configure one. By default, Hello packets are sent every 30 seconds, and up to 5 retries are attempted if no response is received. The range is 10 to 65535 seconds and 1 to 65535 retries.
Poll Groups Timer	How often the Active Directory server should be queried to obtain user membership lists for user groups that you have specified in firewall rules. The ASA queries the server for membership in a group only if you have used the group; it does not query every group defined in the AD server. The default is 8 hours, the range is 1 to 65535 hours. **Tip** If group membership changes, the changes are not reflected in rule processing until this timer expires and the ASA polls the AD server for updated information. Thus, you should configure the timer based on the frequency of changes to group membership in your network, balancing the need to update group membership in the ASA with the desire to reduce the amount of polling.

Table 13-5 Identity Options Advanced Tab (continued)

Element	Description
Retrieve User Information	How the ASA should retrieve user-to-IP address mappings from the AD agent. • **Full Download** (default for ASA non-5505 devices)—On boot, the ASA obtains the full user-to-IP address mapping database from the AD agent, and then gets incremental updates as users log into and out of the network. Use this option on the 5505 only if there are fewer than 1024 users in the network, because the 5505 is limited to 1024 user-to-IP mappings. For the 5505, the default On Demand setting is appropriate if only a few users will pass traffic through the device. • **On Demand** (default for ASA 5505 devices)—The ASA queries the AD agent for user-to-IP mappings only when a new packet requires a connection and no mapping exists. This option uses less memory, but there can be a delay in getting the mapping, and the packets are initially evaluated based on traditional source and destination IP address and service information, which might result in the wrong action. The potential delay can be increased if a large number of users log in at the same time, either due to corporate culture or to a malicious attack.

Creating Identity User Group Objects

You can create identity user group objects to identify individual users, user groups, or a combination of users and groups. These users and groups must be defined in Active Directory (AD), you cannot define other types of users.

Tip Identity user groups are defined on the ASA. You do not need to create these groups to duplicate groups that are already defined in AD. You can directly specify AD groups in firewall rules. Identity user group objects are needed only to define collections of users and user groups that do not otherwise exist in AD.

There are two pre-defined identity user groups. These groups are used when configuring cut-through proxy, as described in Configuring Cut-Through Proxy, page 13-23.

- all-auth-users—To match any IP address that has been associated with an authenticated user.
- all-unauth-users—To match only IP addresses that have **not** been associated with authenticated users.

Tips

- Use of these objects is supported on ASA 8.4(2+) only.
- You must configure the Identity Options policy on the ASA to enable the use of these objects.
- You can create identity user group objects when defining policies or objects that use this object type. For more information, see Selecting Identity Users in Policies, page 13-21.

Related Topics

- Configuring Identity-Based Firewall Rules, page 13-21

- Requirements for Identity-Aware Firewall Policies, page 13-3
- Identity Settings Page, page 11-38
- Creating Policy Objects, page 6-9

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **Identity User Group** from the Object Type selector.

Step 3 Right-click in the work area, then select **New Object** to open the Identity User Group dialog box.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Add and remove items in the **Members in Group** list to identify the users and user groups defined in the object.

To populate the list, do any combination of the following:

- In **Available Identity User Group**, select an existing object and click the **Add >>** button between the lists.
- In **Search User/User Group**, select a user or user group from the Active Directory server configured for the domain in the Identity Settings administration options. You must configure the settings before you can select users or user groups, so that Security Manager knows which AD server to use.

  To find a user or user group, select the NetBIOS domain, indicate whether you are searching for a user or user group, and enter a search string. Then, click **Search** to find matches. A name is considered a match if the string appears anywhere within the name (first, middle initial, last), user ID, CN, or for groups, user group name.

  To add the user or group, select it in the list and click the **Add >>** button between the lists.
- In **Type in comma separated identity user or user group**, type in a valid name, then click the **Add >>** button between the lists. Separate multiple names with commas; they are added as separate lines in the members list.

  You can enter names in the following formats:

  – Individual users: NETBIOS_DOMAIN\user

  – User groups (note the double \): NETBIOS_DOMAIN\\user_group

  If you do not include the domain name, one is added for you based on the options selected in the Security Manager Administration Identity Settings page. If you precede the name with \ or \\, the default domain defined on the Identity Settings page is automatically added.
- To remove an item from the object, select it in the Members list and click the **<< Remove** button between the lists.

Step 6 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 7 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-18.

Step 8 Click **OK** to save the object.

Selecting Identity Users in Policies

In any policy or policy object that allows the specification of identity users, whether directly or through the selection of an identity user group object, you can click the Select button next to the User field to help you enter the information.

In the Identity User Group Selector dialog box, you can define the content of the User field by populating the **Members in Group** list. To populate the list, do any combination of the following:

- In **Available Identity User Group**, select an existing object and click the **Add >>** button between the lists. If the desired object does not exist, you can click the **Add (+)** button below the list to create a new object. You can also select an object and click the **Edit (pencil)** button to modify it or to examine its contents.

  There are two pre-defined identity user groups. These groups are used when configuring cut-through proxy, as described in Configuring Cut-Through Proxy, page 13-23.

  - all-auth-users—To match any IP address that has been associated with an authenticated user.
  - all-unauth-users—To match only IP addresses that have **not** been associated with authenticated users.

- In **Search User/User Group**, select a user or user group from the Active Directory server configured for the domain in the Identity Settings administrative options. You must configure the settings before you can select users or user groups, so that Security Manager knows which AD server to use.

  To find a user or user group, select the NetBIOS domain, indicate whether you are searching for a user or user group, and enter a search string. Then, click **Search** to find matches. A name is considered a match if the string appears anywhere within the name (first, middle initial, last), user ID, CN, or for groups, user group name.

  To add the user or group, select it in the list and click the **Add >>** button between the lists.

- In **Type in comma separated identity user or user group**, type in a valid name, then click the **Add >>** button between the lists. Separate multiple names with commas; they are added as separate lines in the members list.

  You can enter names in the following formats:

  - Individual users: NETBIOS_DOMAIN\user
  - User groups (note the double \): NETBIOS_DOMAIN\\user_group

  If you do not include the domain name, one is added for you based on the options selected in the Security Manager Administration Identity Settings page as explained in Identity Settings Page, page 11-38. If you precede the name with \ or \\, the default domain defined on the Identity Settings page is automatically added.

- To remove an item from the object, select it in the Members list and click the **<< Remove** button between the lists.

Configuring Identity-Based Firewall Rules

Identity awareness is integrated into the access control entries, or rules, in the ACLs used to provide firewall services. Because the feature is integrated into the ACL, the techniques for adding identity-based rules to a firewall policy are the same for all types of firewall policy. This topic provides general guidance on how to incorporate identity-based rules into your existing policies, and directs you to more specific information on configuring each type of policy that allows identity-based rules.

Guidelines For Adding Identity-Based Rules

Following are some general guidelines and recommendations for adding identity-based rules:

- FQDN (fully-qualified domain name) network/host objects are allowed in both Source and Destination fields. For information on configuring these objects, see Creating Networks/Hosts Objects, page 6-82.
- User, user group, and identity user group objects, which specify Active Directory (AD) user or user group names, are defined in a separate field: User. If you configure a rule with one or more user names, user group names, or identity user group objects, the specifications modify the Source address configuration only. They never apply to the addresses specified in the Destination field. For information on configuring these identity user group objects, see Creating Identity User Group Objects, page 13-19.

  You must always configure a source address in a rule, even if you want the rule to primarily operate based on the specified users or user groups. The source and user specifications conjoin to control the scope of the rule. Based on the value of the Source field, the rules operate as follows:

  - **Source = any**—Use "any" as the source if you want the rule to apply based solely on the user specifications. These rules will match the user specification regardless of the workstation IP address from which the user sends traffic.
  - **Source = anything else**—If you specify anything other than "any" as the source address, the rule applies only if the user sends traffic from an IP address that matches the source address specification. Use this technique if you want to provide variable services based on the source network.

    For example, you might have an internal trusted network from which you would allow access to a sensitive destination for users in a particular user group, although you would deny access even to those users if they were outside of the trusted network. In this case, you would create a permit rule that specified the trusted network as the source, the trusted user group as the user, and the sensitive server as the destination. You could also create a specific deny rule with just the source and destination specified, or allow the default deny any rule to capture the non-matching traffic.
- Evaluate whether there are classes of traffic that will never be sensitive to user identity. For example, you might allow DNS traffic for all users. Place these types of rules above identity-based rules so that matching traffic can be quickly allowed before the device needs to evaluate identity-based rules.
- When troubleshooting rules, keep in mind that ultimately rules are applied based on IP address. FQDN rule matching is based on DNS lookups, and the IP address of a host can change between a successful lookup and the next time the lookup is refreshed. For users, IP address mappings are obtained from the AD agent configured in the network or by authentications conducted by the ASA itself.
- FQDN and user specifications are completely independent. You can use one without the other.

Firewall Policies That Allow Identity-Based Rules

Identity-based rules are allowed on ASA 8.4.2+ only. The following policies allow you to configure identity-based rules:

- AAA Rules—Select **Firewall > AAA Rules** and see Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4.

Tip You can use AAA rules to configure cut-through proxy, which allows users whose IP address mappings have become invalid, resulting in denied network access, to authenticate directly to the ASA to resolve the mapping problem. See Configuring Cut-Through Proxy, page 13-23.

- Access Rules—Select **Firewall > Access Rules** and see Configuring Access Rules, page 16-7.
- Inspection Rules—Select **Firewall > Inspection Rules** and see Configuring Inspection Rules, page 17-5.
- Policies that use extended ACL policy objects—Several firewall policies use extended ACL policy objects to define traffic matching criteria instead of incorporating a rule table directly in the policy. You can configure extended ACL policy objects to include FQDN objects or user specifications (see Creating Extended Access Control List Objects, page 6-54). You can then use these identity-based extended ACL objects in the following policies:
  - Botnet Traffic Filter Rules—Select **Firewall > Botnet Traffic Filter Rules** and see Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6. You can use identity-based ACLs as traffic classification for Enable and Drop rules.
  - IPS, QoS, and Connection Rules (service policy rules)—Select **Platform > Service Policy Rules > IPS, QoS, and Connection Rules** and see Service Policy Rules Page, page 58-5.

    Traffic match criteria in this policy is based on extended ACL policy objects that are incorporated into traffic flow policy objects. You must select one of the options for specifying an ACL in the traffic flow object to incorporate identity-based traffic classification. You can use identity-based ACLs for all service types. For more information, see Configuring Traffic Flow Objects, page 58-18.

    One of the services available in this policy, User Statistics, is specifically designed to collect accounting information for identity-based firewall users. See Collecting User Statistics, page 13-25.
  - VPN filter in remote access group policies—The VPN filter ACL is applied to VPN traffic. You can configure a VPN filter on the Connection Settings page in an ASA Group Policy object, which you use in a remote access connection policy. See ASA Group Policies Connection Settings, page 34-33 and Filtering VPN Traffic with Identity-Based Rules, page 13-26.

Policies That Do Not Allow Identity-Based Rules or Objects

There are several types of policy where you can specify network/host objects or extended ACL objects, but where the policy does not allow FQDN network/host objects or ACLs that use those objects or identity user group objects. Following are some examples where you cannot use these types of objects:

- Routing policies, including route maps.
- Network address translation (NAT).
- WCCP (web cache control protocol).
- Crypto maps in VPN configurations.
- Dynamic access policies in remote access VPN configurations.

Configuring Cut-Through Proxy

When you use identity-aware firewall policies, user-to-IP address mappings are obtained from various facilities, primarily from the AD agent in the network. Although mappings are updated regularly, there can occur instances where a firewall rule blocks a legitimate user because the user-to-IP address mapping is not synchronized.

You can configure cut-through proxy to account for this possibility. With cut-through proxy, if a user is blocked, the user can sign on directly to the ASA, and the ASA will update the user-to-IP mapping to correctly reflect the current IP address for the user. The new mapping is forwarded to all contexts that contain the interface where the HTTP/HTTPS packets are received and authenticated.

You use AAA rules to configure cut-through proxy. You have two configuration choices, based on whether there is one or more NetBIOS domains in the network:

- Single domain—Configure a regular AAA rule for authentication and specify the LDAP server group that identifies the Active Directory servers for the domain. Use "any" for the source, and the IP address of the ASA for the destination. For service, you can include HTTP and HTTPS. Then, when the user needs to authenticate to the server, the user enters one of the standard authentication URLs, where *interface_ip* is the IP address of the interface and *port* is optionally the port number, if you specify a non-default port for the protocol in the interactive authentication table: **http://***interface_ip*[**:***port*]**/netaccess/connstatus.html** or **https://***interface_ip*[**:***port*]**/netaccess/connstatus.html**.

Tip The user-to-IP mapping is put under the same domain as configured for the selected AD server group. If you use another means for authentication, the mapping is placed under the LOCAL domain.

- Multiple domains—Configure two authentication rules that use the User-Identity option instead of a specific AAA server group. The following procedure explains this setup. Note that this setup also works for single domain networks. Users authenticate to the ASA using the same URLs mentioned above.

  When you use the User-Identity option, authentication is handled as follows:

  – If the user includes the domain in the login credentials, in the format DOMAIN\username, the ASA uses the domain to determine which AD server to use for authentication based on the domain mappings in the Identity Options policy. If no AAA server is mapped to the domain, the authentication attempt is rejected.

  – If the login credentials do not include an identifiable domain name (typically, if the \ character is not included in the username string), the ASA uses the AD server assigned to the default domain selected in the Identity Options policy. If no AAA server is mapped to the default domain, the authentication attempt will be rejected.

Tip Cut-through proxy works for IPv4 addresses only; IPv6 is not supported.

Related Topics

- Requirements for Identity-Aware Firewall Policies, page 13-3
- Configuring the Firewall to Provide Identity-Aware Services, page 13-7
- Configuring AAA Rules for ASA, PIX, and FWSM Devices, page 15-4
- Understanding How Users Authenticate, page 15-2

Step 1 Configure the Identity Options policy to specify all of the NetBIOS domains and their AD server groups, and the AD agent group, for the network, as described in Identifying Active Directory Servers and Agents, page 13-8.

Step 2 Do one of the following to open the AAA Rules Page, page 15-10:

- (Device view) Select **Firewall > AAA Rules** from the Policy selector.
- (Policy view) Select **Firewall > AAA Rules** from the Policy Type selector. Select an existing policy or create a new one.

Step 3 Create the following rules using the **Add Row** button. For detailed information about the fields in the Add AAA Rules dialog box, see Add and Edit AAA Rule Dialog Boxes, page 15-13.

Tip You can use more specific source, destination, or service specifications than the ones shown here.

- **Rule 1: Do not force users who have already authenticated to authenticate again.**
  - Select the **Authentication Action** and **User-Identity** options.
  - Action = Deny. For AAA authentication rules, "deny" means the user is not prompted for authentication, it does not mean the user's traffic is dropped.
  - Sources = any.
  - Users = all-auth-users.

    For users, **all-auth-users** means any user who has already authenticated to Active Directory, for which there is an IP mapping.
  - Destination = any.
  - Services = IP.
  - AAA Server Group = (no selection).
  - Interface = (your choice, typically inside interfaces).
- **Rule 2: Authenticate users who have not been authenticated yet.**
  - Select the **Authentication Action** and **User-Identity** options.
  - Action = Permit. This action requires matching users to authenticate.
  - User = all-unauth-users.

    In this case, **all-unauth-users** means any user who has not already authenticated to Active Directory.
  - All other options are identical to the first rule.

Collecting User Statistics

You can collect user statistics accounting information for identity-based firewall policies. These statistics are kept for users to which a firewall policy is applied based on username or user group membership.

Related Topics

- Requirements for Identity-Aware Firewall Policies, page 13-3
- Configuring the Firewall to Provide Identity-Aware Services, page 13-7
- Service Policy Rules Page, page 58-5
- Configuring Traffic Flow Objects, page 58-18

Step 1 Do one of the following:

- (Device view) Select an ASA device, then select **Platform > Service Policy Rules > IPS, QoS, and Connection Rules** from the Policy selector.

- (Policy view) Select **PIX/ASA/FWSM Platform > Service Policy Rules > IPS, QoS, and Connection Rules** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the row after which you want to add the rule, then click the **Add Row (+)** button below the table to start the Insert Service Policy Rule wizard.

Step 3 In step 1 of the wizard, select whether the rule will be Global or it will apply to specific interfaces or interface roles. Select Global if you want to collect statistics for users regardless of which interface their traffic passes through.

Click **Next**.

Step 4 In step 2, select the traffic class that defines the traffic for which you are collecting statistics. Select Use class-default if you want to collect statistics on all traffic. Otherwise, select Traffic Class and select the traffic flow object that defines the traffic matching attributes.

Click **Next**.

Step 5 In step 3, select the **User Statistics** tab.

- Select **Enable user statistics accounting**.
- Select the type of information you want to collect:
  - **Account for sent drop count**
  - **Account for sent packet, sent drop and received packet count**

Step 6 Click **Finish** to save your rule.

Filtering VPN Traffic with Identity-Based Rules

When you support remote access VPNs on an ASA, you configure user-sensitive access. You can also use identity-based rules to filter the traffic after validating the remote user access.

Before creating identity-based rules for VPN, understand the rules for VPN user names, to ensure that the rules use the correct domain name:

- If you use an Active Directory LDAP server group for authorization, and you configured that domain/server group in the Identity Options policy, the username is associated with the NetBIOS domain.
- For all other authorization mechanisms, the domain name for VPN users is LOCAL.

With this in mind, there are two methods you can use to filter the traffic on the VPN with identity-based ACL rules:

- Apply a VPN filter in the ASA Group Policy object. The filter applies to all users in the group. You can configure a VPN filter on the Connection Settings page in an ASA Group Policy object, which you use in a remote access connection policy. See ASA Group Policies Connection Settings, page 34-33.
- By default, VPN traffic bypasses interface access rules. You can change this behavior so that all VPN traffic must also pass through the interface access rules. If you take this approach, you must ensure that the interface rules are sensitive to your VPN traffic. To force VPN traffic to go through interface access rules, deselect the **Enable IPsec over Sysopt** option on the ISAKMP/IPsec tab of the RA VPN Global Settings policy. See Configuring VPN Global ISAKMP/IPsec Settings, page 26-32.

Monitoring Identity Firewall Policies

You can use Event Viewer to monitor identity-aware firewall policies the same way you would monitor other types of policies and events. The following are some tips to help you effectively monitor identity policies. For general information on using Event Viewer, see Chapter 69, "Viewing Events".

- There is a group of syslog messages that relate specifically to identity firewall: 746001-746019. You can find descriptions of these messages in the Syslog Message document for your ASA software version at http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html.

  The following messages are of particular concern:

  - **746004 and 746011**—These syslogs indicate that you have exceeded the supported number of references to user groups or users. You should consider changing your policies. For more information on these restrictions, see Requirements for Identity-Aware Firewall Policies, page 13-3.
  - **746003**—There was a failure in downloading user group or user mappings to IP address. The message explains the reason for the failure.
  - **746005**—The AD agent could not be reached. Ensure that the agent is functioning correctly and that there is a network path between the ASA and the agent.
  - **746010**—An update to the imported user or user group failed for the stated reason.
  - **746016**—DNS lookup for the fully-qualified domain name (FQDN) failed for the stated reason.
- Several existing syslog messages now include username or FQDN information. Event Viewer has two columns to display the information: Destination User Identity / FQDN and Source User Identity. Updated messages include:
  - 302005, 302006, 302013, 302014, 302016-302018, 302020, 302021.
  - 305005, 305006, 305009-305013.
  - 304001-304002 include identity information, but they are not parsed.
- You can filter on all identity-related syslog messages by creating a filter on Event Type and selecting the Identity Firewall Events folder.
- When you use the Go to Policy command on an event, as described in Looking Up a Security Manager Policy from Event Viewer, page 69-54, identity information is included in the lookup criteria. Note that identity information is not included in 106100, so policy lookup on that message cannot be sensitive to user identity.