Identity Firewall

This chapter describes how to configure the ASA for the Identity Firewall.

About the Identity Firewall

In an enterprise, users often need access to one or more server resources. Typically, a firewall is not aware of the users' identities and, therefore, cannot apply security policies based on identity. To configure per-user access policies, you must configure a user authentication proxy, which requires user interaction (a username/password query).

The Identity Firewall in the ASA provides more granular access control based on users' identities. You can configure access rules and security policies based on user names and user group names rather than through source IP addresses. 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 usernames 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.

Identity-based firewall services enhance the existing access control and security policy mechanisms by allowing users or groups to be specified in place of source 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
- Simplifying the creation of security policies

- Providing the ability to easily identify user activities on network resources
- Simplifying user activity monitoring

Architecture for Identity Firewall Deployments

The Identity Firewall integrates with Window Active Directory in conjunction with an external Active Directory (AD) Agent that provides the actual identity mapping.

The identity firewall consists of three components:

- ASA
- Microsoft Active Directory

  Although Active Directory is part of the Identity Firewall on the ASA, Active Directory administrators manage it. The reliability and accuracy of the data depends on data in Active Directory.

  Supported versions include Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 servers.

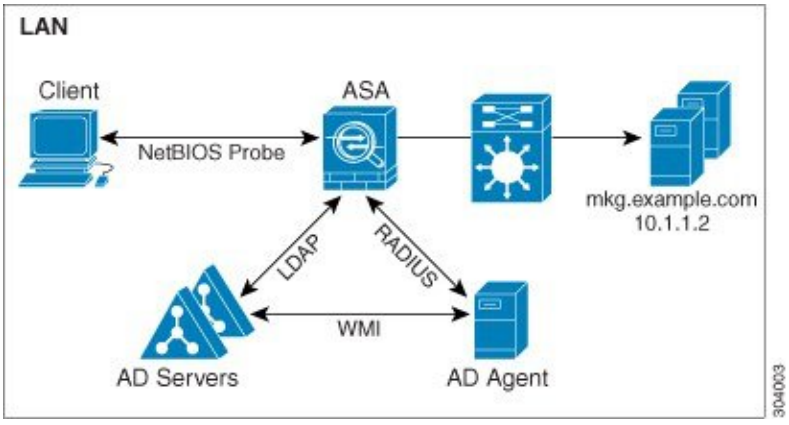
- Active Directory (AD) Agent

  The AD Agent runs on a Windows server. Supported Windows servers include Windows 2003, Windows 2008, and Windows 2008 R2.

Note Windows 2003 R2 is not supported for the AD Agent server.

The following figure show the components of the Identity Firewall. The succeeding table describes the roles of these components and how they communicate with one another.

Figure 1: Identity Firewall Components



1	**On the ASA**: Administrators configure local user groups and Identity Firewall policies.	4	**Client <-> ASA**: The client logs into the network through Microsoft Active Directory. The AD Server authenticates users and generates user login security logs. Alternatively, the client can log into the network through a cut-through proxy or VPN.
2	**ASA <-> AD Server**: The ASA sends an LDAP query for the Active Directory groups configured on the AD Server. The ASA consolidates local and Active Directory groups and applies access rules and Modular Policy Framework security policies based on user identity.	5	**ASA <-> Client**: Based on the policies configured on the ASA, it grants or denies access to the client. If configured, the ASA probes the NetBIOS of the client to pass inactive and no-response users.
3	**ASA <-> AD Agent**: Depending on the Identity Firewall configuration, the ASA downloads the IP-user database or sends a RADIUS request to the AD Agent that asks for the user's IP address. The ASA forwards the new mapped entries that have been learned from web authentication and VPN sessions to the AD Agent.	6	**AD Agent <-> AD Server**: The AD Agent maintains a cache of user ID and IP address mapped entries. and notifies the ASA of changes. The AD Agent sends logs to a syslog server.

Features of the Identity Firewall

The Identity Firewall includes the following key features.

Flexibility

- The ASA can retrieve user identity and IP address mapping from the AD Agent by querying the AD Agent for each new IP address or by maintaining a local copy of the entire user identity and IP address database.
- Supports host group, subnet, or IP address for the destination of a user identity policy.
- Supports a fully qualified domain name (FQDN) for the source and destination of a user identity policy.
- Supports the combination of 5-tuple policies with ID-based policies. The identity-based feature works in tandem with the existing 5-tuple solution.
- Supports use with application inspection policies.
- Retrieves user identity information from remote access VPN, AnyConnect VPN, L2TP VPN and cut-through proxy. All retrieved users are populated to all ASAs that are connected to the AD Agent.

Scalability

- Each AD Agent supports 100 ASAs. Multiple ASAs are able to communicate with a single AD Agent to provide scalability in larger network deployments.
- Supports 30 Active Directory servers provided the IP address is unique among all domains.
- Each user identity in a domain can have up to 8 IP addresses.
- Supports up to 64,000 user identity-IP address mapped entries in active policies for the ASA 5500 Series models. This limit controls the maximum number of users who have policies applied. The total number of users are the aggregate of all users configured in all different contexts.
- Supports up to 512 user groups in active ASA policies.
- A single access rule can contain one or more user groups or users.
- Supports multiple domains.

Availability

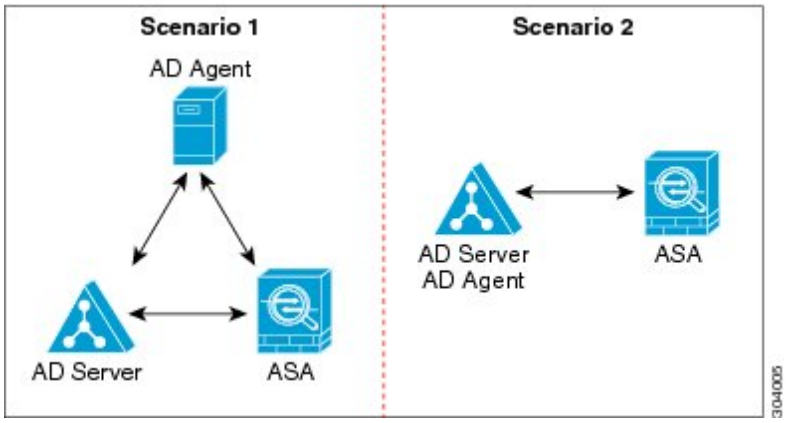
- The ASA retrieves group information from the Active Directory and falls back to web authentication for IP addresses when the AD Agent cannot map a source IP address to a user identity.
- The AD Agent continues to function when any of the Active Directory servers or the ASA are not responding.
- Supports configuring a primary AD Agent and a secondary AD Agent on the ASA. If the primary AD Agent stops responding, the ASA can switch to the secondary AD Agent.
- If the AD Agent is unavailable, the ASA can fall back to existing identity sources such as cut-through proxy and VPN authentication.
- The AD Agent runs a watchdog process that automatically restarts its services when they are down.
- Allows a distributed IP address/user mapping database for use among ASAs.

Deployment Scenarios

You can deploy the components of the Identity Firewall in the following ways, depending on your environmental requirements.

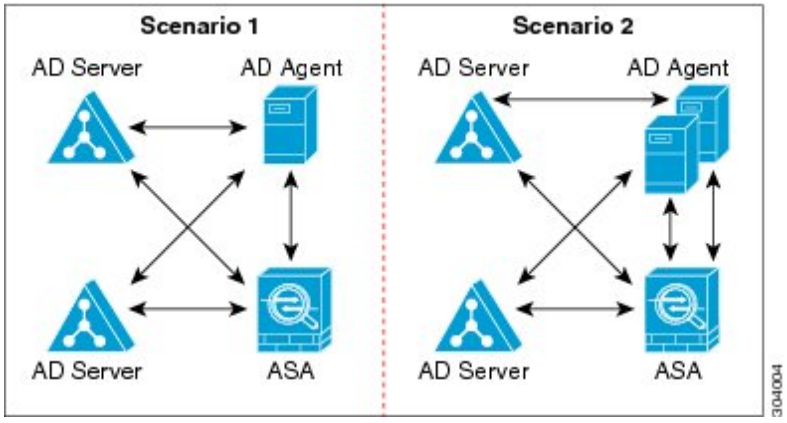
The following figure shows how you can deploy the components of the Identity Firewall to allow for redundancy. Scenario 1 shows a simple installation without component redundancy. Scenario 2 also shows a simple installation without redundancy. However, in this deployment scenario, the Active Directory server and AD Agent are co-located on the same Windows server.

Figure 2: Deployment Scenario without Redundancy



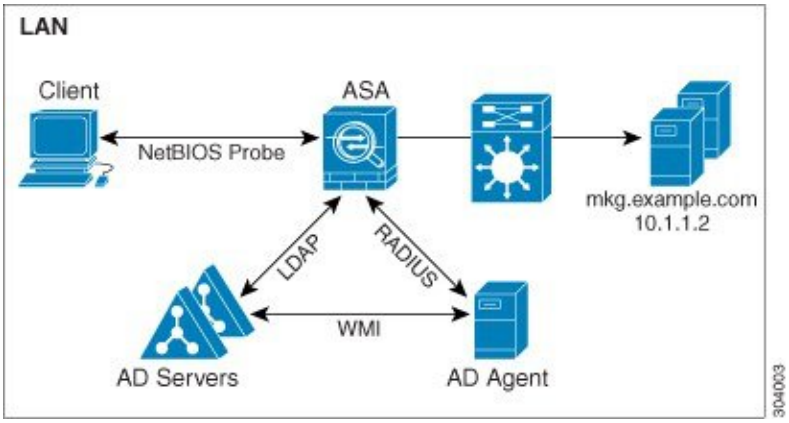
The following figure shows how you can deploy the Identity Firewall components to support redundancy. Scenario 1 shows a deployment with multiple Active Directory servers and a single AD Agent installed on a separate Windows server. Scenario 2 shows a deployment with multiple Active Directory servers and multiple AD Agents installed on separate Windows servers.

Figure 3: Deployment Scenario with Redundant Components



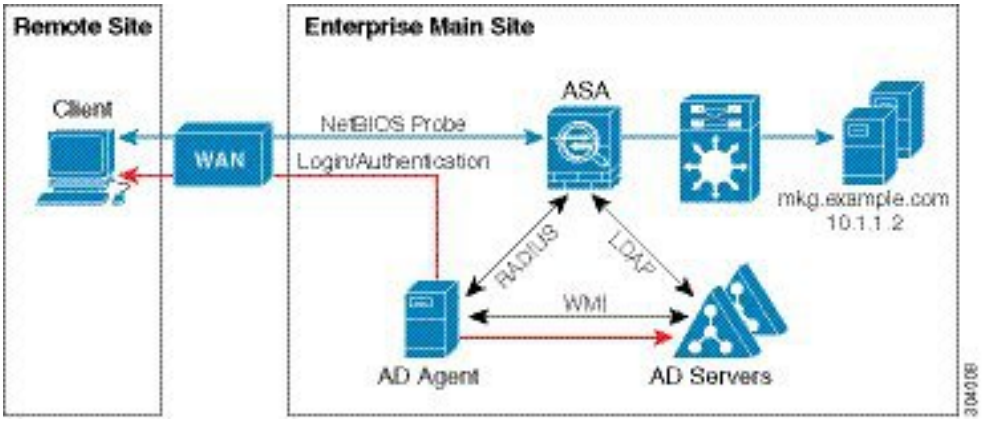
The following figure shows how all Identity Firewall components—Active Directory server, the AD Agent, and the clients—are installed and communicate on the LAN.

Figure 4: LAN -based Deployment



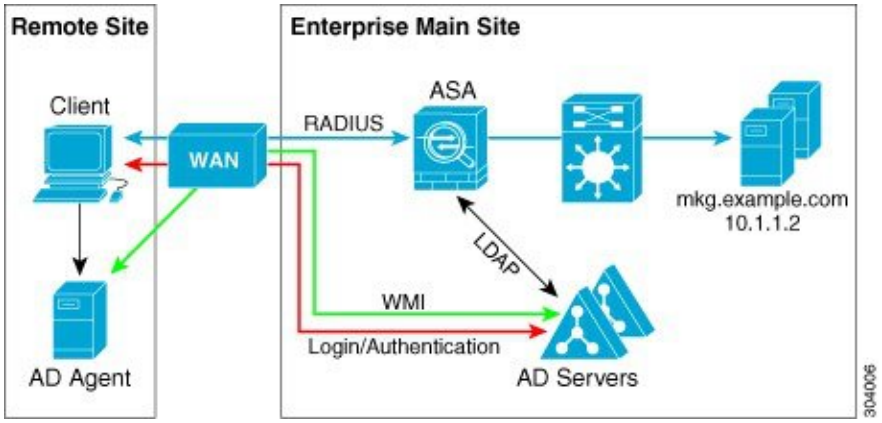
The following figure shows a WAN-based deployment to support a remote site. The Active Directory server and the AD Agent are installed on the main site LAN. The clients are located at a remote site and connect to the Identity Firewall components over a WAN.

Figure 5: WAN-based Deployment



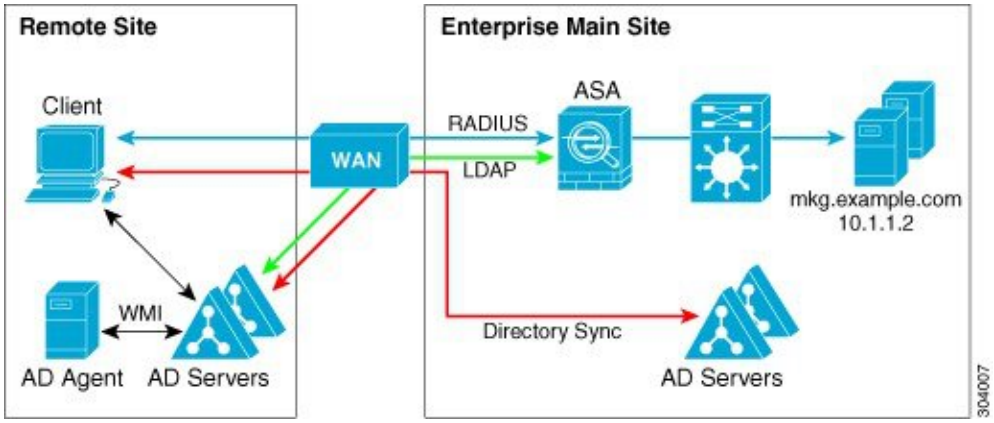
The following figure also shows a WAN-based deployment to support a remote site. The Active Directory server is installed on the main site LAN. However, the AD Agent is installed and accessed by the clients at the remote site. The remote clients connect to the Active Directory servers at the main site over a WAN.

Figure 6: WAN-based Deployment with Remote AD Agent



The following figure shows an expanded remote site installation. An AD Agent and Active Directory servers are installed at the remote site. The clients access these components locally when logging into network resources located at the main site. The remote Active Directory server must synchronize its data with the central Active Directory servers located at the main site.

Figure 7: WAN-based Deployment with Remote AD Agent and AD Servers



Guidelines for the Identity Firewall

This section describes the guidelines and limitations that you should check before configuring the Identity Firewall.

Failover

- The Identity Firewall supports user identity-IP address mapping and AD Agent status replication from active to standby when Stateful Failover is enabled. However, only user identity-IP address mapping, AD Agent status, and domain status are replicated. User and user group records are not replicated to the standby ASA.
- When failover is configured, the standby ASA must also be configured to connect to the AD Agent directly to retrieve user groups. The standby ASA does not send NetBIOS packets to clients even when the NetBIOS probing options are configured for the Identity Firewall.

- When a client is determined to be inactive by the active ASA, the information is propagated to the standby ASA. User statistics are not propagated to the standby ASA.
- When you have failover configured, you must configure the AD Agent to communicate with both the active and standby ASAs. See the *Installation and Setup Guide for the Active Directory Agent* for the steps to configure the ASA on the AD Agent server.

IPv6

- The AD Agent supports endpoints with IPv6 addresses. It can receive IPv6 addresses in log events, maintain them in its cache, and send them through RADIUS messages. The AAA server must use an IPv4 address.
- NetBIOS over IPv6 is not supported.

Additional Guidelines

- A full URL as a destination address is not supported.
- For NetBIOS probing to function, the network between the ASA, AD Agent, and clients must support UDP-encapsulated NetBIOS traffic.
- MAC address checking by the Identity Firewall does not work when intervening routers are present. Users logged into clients that are behind the same router have the same MAC addresses. With this implementation, all the packets from the same router are able to pass the check, because the ASA is unable to ascertain the actual MAC addresses behind the router.
- Although you can use user specifications in VPN filter ACLs, the user-based rules are interpreted uni-directionally rather than bi-directionally, which is how VPN filter usually works. That is, you can filter based on user-initiated traffic, but the filter does not apply for going from the destination back to the user. For example, you could include a rule that allows a specific user to ping a server, but that rule will not allow the server to ping the user.
- The following ASA features do not support using the identity-based object and FQDN in an extended ACL:
  - Crypto maps
  - WCCP
  - NAT
  - Group policy (except for VPN filters)
  - DAP
- You can use the **user-identity update active-user-database** command to actively initiate a user-IP address download from the AD agent.

  By design, if a previous download session has finished, the ASA does not allow you to issue this command again.

  As a result, if the user-IP database is very large, the previous download session is not finished yet, and you issue another **user-identity update active-user-database** command, the following error message appears:

```
"ERROR: one update active-user-database is already in progress."
```

You need to wait until the previous session is completely finished, then you can issue another **user-identity update active-user-database** command.

Another example of this behavior occurs because of packet loss from the AD Agent to the ASA.

When you issue a **user-identity update active-user-database** command, the ASA requests the total number of user-IP mapped entries to be downloaded. Then the AD Agent initiates a UDP connection to the ASA and sends the change of authorization request packet.

If for some reason the packet is lost, there is no way for the ASA to discern this. As a result, the ASA holds the session for 4-5 minutes, during which time this error message continues to appear if you have issued the **user-identity update active-user-database** command.

- When you use the Cisco Context Directory Agent (CDA) in conjunction with the ASA or Cisco Ironport Web Security Appliance (WSA), make sure that you open the following ports:
  - Authentication port for UDP—1645
  - Accounting port for UDP—1646
  - Listening port for UDP—3799

    The listening port is used to send change of authorization requests from the CDA to the ASA or to the WSA.

- If the **user-identity action domain-controller-down** *domain_name* **disable user-identity-rule** command is configured and the specified domain is down, or if the **user-identity action ad-agent-down disable user-identity-rule** command is configured and the AD Agent is down, all the logged-in users have the disabled status.
- For domain names, the following characters are not valid: \/:*?"<>|.
- For usernames, the following characters are not valid: \/[]:;=,+*?"<>|@.
- For user group names, the following characters are not valid: \/[]:;=,+*?"<>|.
- How you configure the Identity Firewall to retrieve user information from the AD Agent affects the amount of memory used by the feature. You specify whether the ASA uses on-demand retrieval or full download retrieval. Choosing on-demand retrieval has the benefit of using less memory, because only users of received packets are queried and stored.

Prerequisites for the Identity Firewall

This section lists the prerequisites for configuring the Identity Firewall.

AD Agent

- The AD Agent must be installed on a Windows server that is accessible to the ASA. Additionally, you must configure the AD Agent to obtain information from the Active Directory servers and to communicate with the ASA.
- Supported Windows servers include Windows 2003, Windows 2008, and Windows 2008 R2.

Note Windows 2003 R2 is not supported for the AD Agent server.

- For the steps to install and configure the AD Agent, see the *Installation and Setup Guide for the Active Directory Agent*.
- Before configuring the AD Agent in the ASA, obtain the secret key value that the AD Agent and the ASA use to communicate. This value must match on both the AD Agent and the ASA.

Microsoft Active Directory

- Microsoft Active Directory must be installed on a Windows server and accessible by the ASA. Supported versions include Windows 2003, 2008, and 2008 R2 servers.
- Before configuring the Active Directory server on the ASA, create a user account in Active Directory for the ASA.
- Additionally, the ASA sends encrypted log-in information to the Active Directory server by using SSL enabled over LDAP. SSL must be enabled on the Active Directory server. See the documentation for Microsoft Active Directory for how to enable SSL for Active Directory.

Note Before running the AD Agent Installer, you must install the patches listed in the *README First for the Cisco Active Directory Agent* on each Microsoft Active Directory server that the AD Agent monitors. These patches are required even when the AD Agent is installed directly on the domain controller server.

Configure the Identity Firewall

To configure the Identity Firewall, perform the following tasks:

Procedure

Step 1 Configure the Active Directory domain in the ASA.

Step 2 Configure the AD Agent in ASA.

Step 3 Configure Identity Options.

Step 4 Configure Identity-based Security Policy. After the AD domain and AD Agent are configured, you can create identity-based object groups and ACLs for use in many features.

Configure the Active Directory Domain

Active Directory domain configuration on the ASA is required for the ASA to download Active Directory groups and accept user identities from specific domains when receiving IP-user mapping from the AD Agent.

Before you begin

- Active Directory server IP address
- Distinguished Name for LDAP base DN
- Distinguished Name and password for the Active Directory user that the Identity Firewall uses to connect to the Active Directory domain controller

To configure the Active Directory domain, perform the following steps:

Procedure

Step 1 Create the AAA server group and configure AAA server parameters for the Active Directory server.

aaa-server *server-tag* **protocol ldap**

Example:

```
ciscoasa(config)# aaa-server adserver protocol ldap
```

Step 2 Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the Active Directory server.

aaa-server *server-tag* [(*interface-name*)] **host**{*server-ip* | *name*} [*key*] [**timeout***seconds*]

Example:

```
ciscoasa(config-aaa-server-group)# aaa-server adserver (mgmt) host 172.168.224.6
```

Step 3 Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.

ldap-base-dn *string*

Example:

```
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=SAMPLE,DC=com
```

Specifying the **ldap-base-dn** command is optional. If you do not specify this command, the ASA retrieves the defaultNamingContext from the Active Directory and uses it as the base DN.

Step 4 Specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-scope subtree

Example:

```
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

Step 5 Specify the login password for the LDAP server.

ldap-login-password *string*

Example:

```
ciscoasa(config-aaa-server-host)# ldap-login-password obscurepassword
```

Step 6 Specify the name of the directory object that the system should bind this as.

ldap-login-dn *string*

Example:

```
ciscoasa(config-aaa-server-host)# ldap-login-dn SAMPLE\user1
```

The ASA identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the ASA.

The *string* argument is a case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

You can specify the traditional or simplified format.

The typical **ldap-login-dn** command format includes: CN=username,OU=Employees,OU=Sample Users,DC=sample,DC=com.

Step 7 Configure the LDAP server model for the Microsoft Active Directory server.

server-type microsoft

Example:

```
ciscoasa(config-aaa-server-host)# server-type microsoft
```

Step 8 Specify the location of the Active Directory groups configuration in the Active Directory domain controller.

ldap-group-base-dn *string*

Example:

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Sample Groups,DC=SAMPLE,DC=com
```

If not specified, the value in the **ldap-group-base-dn** command is used. Specifying this command is optional.

Step 9 Allow the ASA to access the Active Directory domain controller over SSL.

ldap-over-ssl enable

Example:

```
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
```

To support LDAP over SSL, Active Directory server needs to be configured to have this support.

By default, the Active Directory does not have SSL configured. If SSL is not configured in the Active Directory, you do not need to configure it on the ASA for the Identity Firewall.

Step 10 Specify the server port.

server-port *port-number*

Example:

```
ciscoasa(config-aaa-server-host)# server-port 389

ciscoasa(config-aaa-server-host)# server-port 636
```

By default, if the **ldap-over-ssl** command is not enabled, the default server port is 389; if the **ldap-over-ssl** command is enabled, the default server port is 636.

Step 11 Set the amount of time before LDAP queries time out.

group-search-timeout *seconds*

Example:

```
ciscoasa(config-aaa-server-host)# group-search-timeout 300
```

Configure Active Directory Agents

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to the secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between the ASA and AD Agent.

Before you begin

- AD agent IP address
- Shared secret between the ASA and AD agent

To configure the AD Agents, perform the following steps:

Procedure

Step 1 Create the AAA server group and configure AAA server parameters for the AD Agent.

aaa-server *server-tag* **protocol radius**

Example:

```
ciscoasa(config)# aaa-server adagent protocol radius
```

Step 2 Enable the AD Agent mode.

ad-agent-mode

Example:

```
ciscoasa(config)# ad-agent-mode
```

Step 3 Configure the AAA server as part of a AAA server group and the AAA server parameters that are host-specific for the AD Agent.

aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout***seconds*]

Example:

```
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
```

Step 4 Specify the server secret value used to authenticate the ASA to the AD Agent server.

key *key*

Example:

```
ciscoasa(config-aaa-server-host)# key mysecret
```

Step 5 Define the server group of the AD Agent.

user-identity ad-agent aaa-server *aaa_server_group_tag*

Example:

```
ciscoasa(config-aaa-server-hostkey# user-identity ad-agent aaa-server adagent
```

The first server defined in the *aaa_server_group_tag* argument is the primary AD Agent and the second server defined is the secondary AD Agent. The Identity Firewall supports defining only two AD Agent hosts.

When the ASA detects that the primary AD Agent is down and a secondary agent is specified, it switches to the secondary AD Agent. The AAA server for the AD agent uses RADIUS as the communication protocol, and should specify a key attribute for the shared secret between the ASA and AD Agent.

Step 6 Test the communication between the ASA and the AD Agent server.

test aaa-server ad-agent

Example:

```
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

Configure Identity Options

To configure the Identity Options for the Identity Firewall, perform the following steps:

Procedure

Step 1 Enable the Identity Firewall feature. By default, the Identity Firewall feature is disabled.

user-identity enable

Example:

```
ciscoasa(config)# user-identity enable
```

Step 2 Specify the default domain for the Identity Firewall.

user-identity default-domain *domain_NetBIOS_name*

Example:

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

For the *domain_NetBIOS_name* argument, enter a name of up to 32 characters that consists of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name includes a space, enclose the entire name in quotation marks. The domain name is not case sensitive.

The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. For multiple context modes, you can set a default domain name for each context, as well as within the system execution space.

Note The default domain name that you specify must match the NetBIOS domain name configured on the Active Directory domain controller. If the domain name does not match, the AD Agent incorrectly associates the user identity-IP address mapped entries with the domain name that you enter when configuring the ASA. To view the NetBIOS domain name, open the Active Directory user event security log in any text editor.

The Identity Firewall uses the LOCAL domain for all locally defined user groups or locally defined users. Users logging in through a web portal (cut-through proxy) are designated as belonging to the Active Directory domain with which they authenticated. Users logging in through a VPN are designated as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with the Active Directory. In this case, the Identity Firewall can associate the users with their Active Directory domain.

Step 3 Associate the LDAP parameters defined for the AAA server for importing user group queries with the domain name.

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

Example:

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

For the *domain_nickname* argument, enter a name of up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name includes a space, you must enclose that space character in quotation marks. The domain name is not case sensitive.

Step 4 Enable NetBIOS probing.

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* **user-not-needed** [**user-not-needed** | **match-any** | **exact-match**]

Example:

```
ciscoasa(config)# user-identity logout-probe netbios
local-system probe-time minutes 10 retry-interval seconds 10
retry-count 2 user-not-needed
```

Enabling this option configures how often the ASA probes the user client IP address to determine whether the client is still active. By default, NetBIOS probing is disabled. To minimize the NetBIOS packets, the ASA only sends a NetBIOS probe to a client when the user has been idle for more than the specified number of minutes.

- **Exact match**—The username of the user assigned to the IP address must be the only one in the NetBIOS response. Otherwise, the user identity of that IP address is considered invalid.
- **User-not-needed**—As long as the ASA received a NetBIOS response from the client, the user identity is considered valid.

The Identity Firewall only performs NetBIOS probing for those users identities that are in the active state and exist in at least one security policy. The ASA does not perform NetBIOS probing for clients where the users logged in through cut-through proxy or by using a VPN.

Step 5 Specify the amount of time before a user is considered idle, meaning the ASA has not received traffic from the user's IP address for the specified amount of time.

user-identity inactive-user-timer minutes *minutes*

Example:

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

When the timer expires, the user's IP address is marked as inactive and removed from the local cached user identity-IP address mapping database, and the ASA no longer notifies the AD Agent about that IP address. Existing traffic is still allowed to pass. When this command is specified, the ASA runs an inactive timer even when the NetBIOS Logout Probe is configured.

By default, the idle timeout is set to 60 minutes. This option does not apply to VPN or cut-through proxy users.

Step 6 Specify the amount of time before the ASA queries the Active Directory server for user group information.

user-identity poll-import-user-group-timer hours *hours*

Example:

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours1
```

If a user is added to or deleted from an Active Directory group, the ASA received the updated user group after the import group timer ran. By default, the **poll-import user-group-timer hours** value is 8 hours.

To immediately update user group information, enter the **user-identity update import-user** command.

Step 7 Specify the action when a client does not respond to a NetBIOS probe.

user-identity action netbios-response-fail remove-user-ip

Example:

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

For example, the network connection might be blocked to that client or the client is not active.

When this command is configured, the ASA removes the user identity-IP address mapping for that client.

By default, this command is disabled.

Step 8 Specify the action when the domain is down, because the Active Directory domain controller is not responding.

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

Example:

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

When the domain is down and the **disable-user-identity-rule** keyword is configured, the ASA disables the user identity-IP address mapping for that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command.

By default, this command is disabled.

Step 9 Enable user-not-found tracking. By default, this command is disabled.

user-identity user-not-found enable

Example:

```
ciscoasa(config)# user-identity user-not-found enable
```

Only the last 1024 IP addresses are tracked.

Step 10 Specify the action when the AD Agent is not responding.

user-identity action ad-agent-down disable-user-identity-rule

Example:

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

When the AD Agent is down and this command is configured, the ASA disables the user identity rules associated with the users in that domain. Additionally, the status of all user IP addresses in that domain is marked as disabled in the output displayed by the **show user-identity user** command.

By default, this command is disabled.

Step 11 Specify the action when a user's MAC address is found to be inconsistent with the ASA IP address currently mapped to that MAC address.

user-identity actionmac-address-mismatch remove-user-ip

Example:

```
ciscoasa(config)# user-identity actionmac-address-mismatch remove-user-ip
```

When this command is configured, the ASA removes the user identity-IP address mapping for that client.

By default, the ASA uses the **remove-user-ip** keyword when this command is specified.

Step 12 Define how the ASA retrieves the user identity-IP address mapping information from the AD Agent.

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

Example:

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

By default, the ASA uses the **full-download** option.

- **Full-download**—Specifies that the ASA send a request to the AD Agent to download the entire IP-user mapping table when the ASA starts and then to receive incremental IP-user mapping information when users log in and log out. Full downloads are event driven, meaning that when there are subsequent requests to download the database, just the updates to the user identity-IP address mapping database are sent.
- **On-demand**—Specifies that the ASA retrieve the user mapping information of an IP address from the AD Agent when the ASA receives a packet that requires a new connection, and the user of its source IP address is not in the user-identity database.

When the ASA registers a change request with the AD Agent, the AD Agent sends a new event to the ASA.

Step 13 Define the hello timer between the ASA and the AD Agent.

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

Example:

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

The hello timer between the ASA and the AD Agent defines how frequently the ASA exchanges hello packets. The ASA uses the hello packet to obtain ASA replication status (in-sync or out-of-sync) and domain status (up or down). If the ASA does not receive a response from the AD Agent, it resends a hello packet after the specified interval.

By default, the hello timer is set to 30 seconds and 5 retries.

Step 14 Enable the ASA to keep track of the last event time stamp that it receives for each identifier and to discard any message if the event time stamp is at least 5 minutes older than the ASA's clock, or if its time stamp is earlier than the last event's time stamp.

user-identity ad-agent event-timestamp-check

Example:

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

For a newly booted ASA that does not have knowledge of the last event time stamp, the ASA compares the event time stamp with its own clock. If the event is at least 5 minutes older, the ASA does not accept the message.

We recommend that you configure the ASA, Active Directory, and Active Directory agent to synchronize their clocks among themselves using NTP.

Step 15 Define the server group of the AD Agent.

user-identity ad-agent aaa-server *aaa_server_group_tag*

Example:

```
ciscoasa(config)# user-identity ad-agent aaa-server ad-agent
```

For the *aaa_server_group_tag* argument, enter the value defined by the **aaa-server** command.

Configure Identity-Based Security Policy

You can incorporate identity-based policy in many ASA features. Any feature that uses extended ACLs (other than those listed as unsupported in the Guidelines section) can take advantage of an identity firewall. You can now add user identity arguments to extended ACLs, as well as network-based parameters.

Features that can use identity include the following:

- Access rules—An access rule permits or denies traffic on an interface using network information. With an identity firewall, you can control access based on user identity.
- AAA rules—An authentication rule (also known as cut-through proxy) controls network access based on the user. Because this function is very similar to an access rule plus an identity firewall, AAA rules can now be used as a backup method of authentication if a user's AD login expires. For example, for any user without a valid login, you can trigger a AAA rule. To ensure that the AAA rule is only triggered for users that do not have valid logins, you can specify special usernames in the extended ACL used for the access rule and for the AAA rule: None (users without a valid login) and Any (users with a valid login). In the access rule, configure your policy as usual for users and groups, but then include a AAA rule that permits all None users; you must permit these users so they can later trigger a AAA rule. Then, configure a AAA rule that denies Any users (these users are not subject to the AAA rule, and were handled already by the access rule), but permits all None users. For example:

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

For more information, see the legacy feature guide.

- VPN filter—Although a VPN does not support identity firewall ACLs in general, you can configure the ASA to enforce identity-based access rules on VPN traffic. By default, VPN traffic is not subject to access rules. You can force VPN clients to abide by access rules that use an identity firewall ACL (with the **no sysopt connection permit-vpn** command). You can also use an identity firewall ACL with the VPN filter feature; a VPN filter accomplishes a similar effect by allowing access rules in general.

Collect User Statistics

To activate the collection of user statistics by the Modular Policy Framework and match lookup actions for the Identify Firewall, perform the following steps:

Procedure

Activate the collection of user statistics by the Modular Policy Framework and matches lookup actions for the Identify Firewall.

user-statistics [**accounting** | **scanning**]

Example:

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-mapp-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
ciscoasa(config-pmap)# user-statistics accounting
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy p-identity-example-1 interface outside
```

The **accounting** keyword specifies that the ASA collect the sent packet count, sent drop count, and received packet count. The **scanning** keyword specifies that the ASA collect only the sent drop count.

When you configure a policy map to collect user statistics, the ASA collects detailed statistics for selected users. When you specify the **user-statistics** command without the **accounting** or **scanning** keywords, the ASA collects both accounting and scanning statistics.

Examples for the Identity Firewall

This section provides examples for the Identity Firewall.

AAA Rule and Access Rule Example 1

This example shows a typical cut-through proxy configuration to allow a user to log in through the ASA. In this example, the following conditions apply:

- The ASA IP address is 172.1.1.118.
- The Active Directory domain controller has the IP address 71.1.2.93.
- The end-user client has the IP address 172.1.1.118 and uses HTTPS to log in through a web portal.
- The user is authenticated by the Active Directory domain controller via LDAP.
- The ASA uses the inside interface to connect to the Active Directory domain controller on the corporate network.

```
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq
http
ciscoasa(config)# access-list AUTH extended permit tcp any 172.1.1.118 255.255.255.255 eq
https
ciscoasa(config)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 171.1.2.93
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-dn
cn=kao,OU=Employees,OU=CiscoUsers,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-login-password *****
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
ciscoasa(config-aaa-server-host)# aaa authentication match AUTH inside LDAP
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 0.0.0.0 0.0.0.0 inside
ciscoasa(config)#
ciscoasa(config)# auth-prompt prompt Enter Your Authentication
ciscoasa(config)# auth-prompt accept You are Good
ciscoasa(config)# auth-prompt reject Goodbye
```

AAA Rule and Access Rule Example 2

In this example, the following guidelines apply:

- In **access-list** commands, permit user NONE rules should be written before entering the **access-list 100 ex deny any any** command to allow unauthenticated incoming users to trigger AAA cut-through proxy.
- In the **auth access-list** command, permit user NONE rules guarantee only unauthenticated trigger cut-through proxy. Ideally, they should be the last lines.

```
ciscoasa(config)# access-list listenerAuth extended permit tcp any any
```

```
ciscoasa(config)# aaa authentication match listenerAuth inside ldap
ciscoasa(config)# aaa authentication listener http inside port 8888
ciscoasa(config)# access-list 100 ex permit ip user SAMPLE\user1 any any
ciscoasa(config)# access-list 100 ex deny ip user SAMPLE\user2 any any
ciscoasa(config)# access-list 100 ex permit ip user NONE any any
ciscoasa(config)# access-list 100 ex deny any any
ciscoasa(config)# access-group 100 in interface inside
ciscoasa(config)# aaa authenticate match 200 inside user-identity
```

VPN Filter Examples

The ASA reports users logging in through VPN authentication or a web portal (cut-through proxy) to the AD Agent, which distributes the user information to all registered ASA devices. Specifically, the IP-user mapping of authenticated users is forwarded to all ASA contexts that include the input interface where HTTP/HTTPS packets are received and authenticated. The ASA designates users logging in through a VPN as belonging the LOCAL domain.

There are two different ways to apply identity firewall rules to VPN users:

- Ensure that interface access rules, which can include identity firewall rules, are applied to VPN users.
- Bypass interface access rules, but apply a VPN filter to VPN traffic. VPN filters can include identity firewall rules.

The following topics provide examples.

Applying Interface Access Rules to VPN Traffic Example

By default, the **sysopt connection permit-vpn** command is enabled and VPN traffic is exempted from an access list check. To apply interface-based ACL rules for VPN traffic, you need to disable VPN traffic access list bypass.

In this example, if the user logs in from the outside interface, the identity firewall rules control which network resources are accessible. All VPN users are to be stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

```
 ! Apply VPN-Filter with bypassing access-list check disabled
no sysopt connection permit-vpn
access-list v1 extended deny ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended permit ip user LOCAL\idfw any 20.0.0.0 255.255.255.0
access-group v1 in interface outside
```

Applying VPN Filters with User Specifications Example

By default, the **sysopt connection permit-vpn** command is enabled and VPN traffic is exempted from an access list check. You can use a VPN filter to apply the identity firewall rules to the VPN traffic. You can define a VPN filter with identity firewall rules in the username and group policy.

In the example, when user idfw logs in, the user can access network resources in the 10.0.00/24 subnet. However, when user user1 logs in, access to network resources in 10.0.00/24 subnet is denied. Note that all VPN users are stored under the LOCAL domain. Therefore, it is only meaningful to apply the rules for LOCAL users or object groups that include LOCAL users.

Note Although you can use user specifications in VPN filter ACLs, the user-based rules are interpreted uni-directionally rather than bi-directionally, which is how VPN filter usually works. That is, you can filter based on user-initiated traffic, but the filter does not apply for going from the destination back to the user. For example, you could include a rule that allows a specific user to ping a server, but that rule will not allow the server to ping the user.

```
! Apply VPN-Filter with bypassing access-list check enabled
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v2 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
username user1 password QkBIIYVi6IFLEsYv encrypted privilege 0
username user1 attributes
    vpn-group-policy group1 vpn-filter value v2
username idfw password eEm2dmjMaopcGozT encrypted
username idfw attributes
    vpn-group-policy testgroup vpn-filter value v1
sysopt connection permit-vpn
access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0
access-list v1 extended deny ip user LOCAL\user1 any 10.0.0.0 255.255.255.0
group-policy group1 internal
group-policy group1 attributes
    vpn-filter value v1
    vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
```

Monitoring the Identity Firewall

See the following commands for monitoring the Identity Firewall status:

- **show user-identity ad-agent**

  This command shows the status of the AD Agent and the domains.

- **show user-identity ad-agent statistics**

  This command shows the statistics for the AD Agent.

- **show user-identity memory**

  This command shows the memory usage of various modules in the Identity Firewall.

- **show user-identity user all list**

  This command shows information about all users contained in the IP-user mapping database used by the Identity Firewall.

- **show user-identity user active user** *domainuser-name***list detail**

  This command shows additional information about an active user.

- **show user-identity group**

  This command shows the list of user groups configured for the Identity Firewall.

History for the Identity Firewall

Table 1: History for the Identity Firewall

Feature Name	Releases	Description
Identity Firewall	8.4(2)	The Identity Firewall feature was introduced. We introduced or modified the following commands: **user-identity enable**, **user-identity default-domain**, **user-identity domain**, **user-identity logout-probe**, **user-identity inactive-user-timer**, **user-identity poll-import-user-group-timer**, **user-identity action netbios-response-fail**, **user-identity user-not-found**, **user-identity action ad-agent-down**, **user-identity action mac-address-mismatch**, **user-identity action domain-controller-down**, **user-identity ad-agent active-user-database**, **user-identity ad-agent hello-timer**, **user-identity ad-agent aaa-server**, **user-identity update import-user**, **dns domain-lookup**, **dns poll-timer**, **dns expire-entry-timer**, **object-group user, show user-identity**, **show dns**, **clear configure user-identity**, **clear dns**, **debug user-identity**.