

Email Proxy

Email proxies extend remote email capability to users of Clientless SSL VPN. When users attempt an email session via email proxy, the email client establishes a tunnel using the SSL protocol.

The email proxy protocols are as follows:

POP3S

POP3S is one of the email proxies Clientless SSL VPN supports. By default the Security Appliance listens to port 995, and connections are automatically allowed to port 995 or to the configured port. The POP3 proxy allows only SSL connections on that port. After the SSL tunnel is established, the POP3 protocol starts, and then authentication occurs. POP3S is for a receiving email.

IMAP4S

IMAP4S is one of the email proxies Clientless SSL VPN supports. By default the Security Appliance listens to port 993, and connections are automatically allowed to port 993 or to the configured port. The IMAP4 proxy allows only SSL connections on that port. After the SSL tunnel is established, the IMAP4 protocol starts, and then authentication occurs. IMAP4S is for receiving email.

SMTPS

SMTPS is one of the email proxies Clientless SSL VPN supports. By default, the Security Appliance listens to port 988, and connections automatically are allowed to port 988 or to the configured port. The SMTPS proxy allows only SSL connections on that port. After the SSL tunnel establishes, the SMTPS protocol starts, and then authentication occurs. SMTPS is for sending email.

- Configure Email Proxy, on page 2
- Set AAA Server Groups, on page 2
- Identify Interfaces for Email Proxy, on page 3
- Configure Authentication for Email Proxy, on page 4
- Identify Proxy Servers, on page 5
- Configure Delimiters, on page 6

Configure Email Proxy

Requirements for Email Proxy

- Users who access email from both local and remote locations via email proxy require separate email accounts on their email program for local and remote access.
- Email proxy sessions require that the user authenticate.

Set AAA Server Groups

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **AAA.**

Step 2 Choose the appropriate tab (POP3S , IMAP4S , or SMTPS) to associate AAA server groups and configure the default group policy for those sessions.

- AAA server groups—Click to go to the AAA Server Groups panel (Configuration > Features > Properties > AAA Setup > AAA Server Groups), where you can add or edit AAA server groups.
- group policies—Click to go to the Group Policy panel (Configuration > Features > VPN > General > Group Policy), where you can add or edit group policies.
- Authentication Server Group—Select the authentication server group for user authentication. The default is to have no authentication servers configured. If you have AAA set as the authentication method (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel), you must configure an AAA server and choose it here, or authentication always fails.
- Authorization Server Group—Select the authorization server group for user authorization. The default is to have no authorization servers configured.
- Accounting Server Group—Select the accounting server group for user accounting. The default is to have no accounting servers configured.
- Default Group Policy—Select the group policy to apply to users when AAA does not return a CLASSID attribute. The length must be between 4 and 15 alphanumeric characters. If you do not specify a default group policy, and there is no CLASSID, the ASA cannot establish the session.
- Authorization Settings—Set values for usernames that the ASA recognizes for authorization. This applies to users that authenticate with digital certificates and require LDAP or RADIUS authorization.
  - Use the entire DN as the username—Select to use the Distinguished Name for authorization.
  - Specify individual DN fields as the username—Select to specify specific DN fields for user authorization.

    You can choose two DN fields, primary and secondary. For example, if you choose EA, users authenticate according to their email address. Then a user with the Common Name (CN) John Doe and an email address of johndoe@cisco.com cannot authenticate as John Doe or as johndoe. He

must authenticate as johndoe@cisco.com. If you choose EA and O, John Doe must authenticate as johndoe@cisco.com and Cisco Systems, Inc.

- Primary DN Field—Select the primary DN field thar you want to configure for authorization. The default is CN. Options include the following:

DN Field	Definition
Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
DN Qualifier (DNQ)	A specific DN attribute.
E-mail Address (EA)	The email address of the person, system or entity that owns the certificate.
Generational Qualifier (GENQ)	A generational qualifier such as Jr., Sr., or III.
Given Name (GN)	The first name of the certificate owner.
Initials (I)	The first letters of each part of the certificate owner's name.
Locality (L)	The city or town where the organization is located.
Name (N)	The name of the certificate owner.
Organization (O)	The name of the company, institution, agency, association, or other entity.
Organizational Unit (OU)	The subgroup within the organization.
Serial Number (SER)	The serial number of the certificate.
Surname (SN)	The family name or last name of the certificate owner.
State/Province (S/P)	The state or province where the organization is located.
Title (T)	The title of the certificate owner, such as Dr.
User ID (UID)	The identification number of the certificate owner.

- Secondary DN Field—(Optional) Select the secondary DN field that you want to configure for authorization. The default is OU. Options include all of those in the preceding table, with the addition of **None**, which you choose if you do not want to include a secondary field.

Identify Interfaces for Email Proxy

The Email Proxy Access screen lets you identify interfaces on which to configure email proxy. You can configure and edit email proxies on individual interfaces, and you can configure and edit email proxies for

one interface and then apply your settings to all interfaces. You cannot configure email proxies for management-only interfaces, or for subinterfaces.

Procedure

Step 1 Browse to **Configuration** > **VPN** > **E-Mail Proxy** > **Access** to show what is enabled for the interfaces.

- Interface—Displays the names of all configured interfaces.
- POP3S Enabled—Shows whether POP3S is enabled for the interface.
- IMAP4s Enabled—Shows whether IMAP4S is enabled for the interface.
- SMTPS Enabled—Shows whether SMTPS is enabled for the interface.

Step 2 Click **Edit** to change the email proxy settings for the highlighted interface.

Configure Authentication for Email Proxy

Configure the authentication methods for each of the email proxy types.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Authentication.**

Step 2 Choose from the multiple methods of authentication:

- AAA—Select to require AAA authentication. This option requires a configured AAA server. The user presents a username, server, and password. Users must present both the VPN username and the email username, separated by the VPN Name Delimiter, only if the usernames are different from each other.
- Certificate—Select to require certificate authentication.

  Note
  Certificate authentication does not work for email proxies in the current ASA software release.

  Certificate authentication requires that users have a certificate that the ASA can validate during SSL negotiation. You can use certificate authentication as the only method of authentication, for SMTPS proxy. Other email proxies require two authentication methods.

  Certificate authentication requires three certificates, all from the same CA:

  - A CA certificate on the ASA.

  - A CA certificate on the client PC.

  - A Web Browser certificate on the client PC, sometimes called a Personal certificate or a Web Browser certificate.
- Piggyback HTTPS—Select to require piggyback authentication.

This authentication scheme requires a user to have already established a Clientless SSL VPN session. The user presents an email username only. No password is required. Users must present both the VPN username and the email username, separated by the VPN Name Delimiter, only if the usernames are different from each other.

IMAP generates a number of sessions that are not limited by the simultaneous user count but do count against the number of simultaneous logins allowed for a username. If the number of IMAP sessions exceeds this maximum and the Clientless SSL VPN connection expires, a user cannot subsequently establish a new connection. There are several solutions:

SMTPS email most often uses piggyback authentication because most SMTP servers do not allow users to log in.

Note
IMAP generates a number of sessions that are not limited by the simultaneous user count but do count against the number of simultaneous logins allowed for a username. If the number of IMAP sessions exceeds this maximum and the Clientless SSL VPN connection expires, a user cannot subsequently establish a new connection. There are several solutions:

- The user can close the IMAP application to clear the sessions with the ASA, and then establish a new Clientless SSL VPN connection.

- The administrator can increase the simultaneous logins for IMAP users (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General).

- Disable HTTPS/Piggyback authentication for email proxy.

- Mailhost—(SMTPS only) Select to require mailhost authentication. This option appears for SMTPS only because POP3S and IMAP4S always perform mailhost authentication. It requires the user's email username, server, and password.

Identify Proxy Servers

This Default Server panel lets you identify proxy servers to the ASA and configure a default server, port, and non-authenticated session limit for email proxies.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Default Servers.**

Step 2 Configure the following fields:

- Name or IP Address—Type the DNS name or IP address for the default email proxy server.
- Port—Type the port number on which the ASA listens for email proxy traffic. Connections are automatically allowed to the configured port. The email proxy allows only SSL connections on this port. After the SSL tunnel is established, the email proxy starts, and then authentication occurs.

  The defaults are as follows:

  - 995 (for POP3S)

- 993 (for IMAP4S)
- 988 (for SMTPS)

- Enable non-authenticated session limit—Select to restrict the number of non-authenticated email proxy sessions. Lets you set a limit for session in the process of authenticating, thereby preventing DOS attacks. When a new session exceeds the set limit, the ASA terminates the oldest non-authenticating connection. If no non-authenticating connection exist, the oldest authenticating connection is terminated without terminating the authenticated sessions.

Email proxy connections have three states:

- Unauthenticated—State of new email connections.
- Authenticating—State when the connection presents a username.
- Authenticated—State when the ASA authenticates the connection.

Configure Delimiters

This panel configures username/password delimiters and server delimiters for email proxy authentication.

Procedure

Step 1 Browse to **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Delimiters.**

Step 2 Configure the following fields:

- Username/Password Delimiter—Select a delimiter to separate the VPN username from the email username. Users need both usernames when using AAA authentication for email proxy, and the VPN username and email username are different. When they log in to an email proxy session, users enter both usernames, separated by the delimiter you configure here, and also the email server name.

  Note
  Passwords for Clientless SSL VPN email proxy users cannot contain characters that are used as delimiters.

- Server Delimiter—Select a delimiter to separate the username from the name of the email server. It must be different from the VPN Name Delimiter. Users enter both their username and server in the username field when they log in to an email proxy session.

  For example, using : as the VPN Name Delimiter and @ as the Server Delimiter, when logging in to an email program via email proxy, users would enter their username in the following format: vpn_username:e-mail_username@server.