邮件代理

邮件代理可将远程邮件功能扩展至无客户端 SSL VPN 用户处。用户通过邮件代理尝试进行邮件会话时，邮件客户端将使用 SSL 协议建立一个隧道。

邮件代理协议如下所示：

POP3S

POP3S 是无客户端 SSL VPN 支持的一种邮件代理。默认情况下，安全设备会侦听端口 995，并自动允许连接端口 995 或配置的端口。POP3 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，POP3 协议将会开始工作，然后会进行身份验证。POP3S 用于接收邮件。

IMAP4S

IMAP4S 是无客户端 SSL VPN 支持的一种邮件代理。默认情况下，安全设备会侦听端口 993，并自动允许连接端口 993 或配置的端口。IMAP4S 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，IMAP4S 协议将会开始工作，接着将会进行身份验证。IMAP4S 用于接收邮件。

SMTPS

SMTPS 是无客户端 SSL VPN 支持的一种邮件代理。默认情况下，安全设备会侦听端口 988，并自动允许连接端口 988 或配置的端口。SMTPS 代理仅允许该端口上的 SSL 连接。建立 SSL 隧道后，SMTPS 协议将会开始工作，接着将会进行身份验证。SMTPS 用于接收邮件。

配置邮件代理

邮件代理的要求

- 如果用户从本地和远程位置通过邮件代理存取邮件，用户在他们的邮件程序上需要单独的邮件账户才能进行本地和远程存取。
- 邮件代理会话需要进行用户身份验证。

设置 AAA 服务器组

过程

步骤 1 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **AAA**。

步骤 2 选择适当的选项卡（POP3S、IMAP4S 或 SMTPS）来关联 AAA 服务器组，并为这些会话配置默认的组策略。

- AAA server groups - 点击以便转至 AAA Server Groups 面板 (Configuration > Features > Properties > AAA Setup > AAA Server Groups)，您可以在其中添加或编辑 AAA 服务器组。
- group policies - 点击以便转至 Group Policy 面板 (Configuration > Features > VPN > General > Group Policy)，您可以在其中添加或编辑组策略。
- Authentication Server Group - 选择用于用户身份验证的身份验证服务器组。默认设置为未配置身份验证服务器。如果您将 AAA 设为身份验证方法 (Configuration > Features AAA > VPN > E-Mail Proxy > Authentication panel)，必须配置 AAA 服务器并在此选择，否则身份验证会始终失败。
- Authorization Server Group - 选择用于用户授权的授权服务器组。默认设置为未配置授权服务器。
- Accounting Server Group - 选择用于用户记账的记账服务器组。默认设置为未配置记账服务器。
- Default Group Policy - 选择 AAA 未返回 CLASSID 属性时，应用至用户的组策略。长度必须在 4 至 15 个字母数字字符之间。如果不指定默认组策略，且没有 CLASSID，则 ASA 无法建立会话。
- Authrization Settings - 为 ASA 用于识别授权的用户名设置值。这适用于通过数字证书进行身份验证并需要 LDAP 或 RADIUS 授权的用户。
  - Use the entire DN as the username - 选择以便将可分辨名称用于授权。
  - Specify individual DN fields as the username - 选择以便指定用于用户授权的特定 DN 字段。

    您可以选择两个 DN 字段，主要和辅助。例如，如果您选择 EA，用户将根据其邮件地址进行身份验证。这样，使用公用名 (CN) John Doe 和邮件地址 johndoe@cisco.com 的用户无法

作为 John Doe 或 johndoe 进行身份验证。他必须作为 johndoe@cisco.com 进行身份验证。如果选择 EA 和 O，John Doe 的身份必须验证为 johndoe@cisco.com 和 Cisco Systems, Inc。

- Primary DN Field - 选择您要配置用于授权的主要 DN 字段。默认设置为 CN。选项包括以下内容：

DN 字段	**定义**
Country (C)	所在国家/地区的双字母缩写。这些代码符合 ISO 3166 国家/地区缩写。
Common Name (CN)	人员、系统或者其他实体的名称。这是标识层次结构中的最低（最具体）级别。
DN Qualifier (DNQ)	特定 DN 属性。
E-mail Address (EA)	拥有此证书的人员、系统或实体的邮件地址。
Generational Qualifier (GENQ)	辈分词，例如 Jr.、Sr. 或 III。
Given Name (GN)	证书所有者的名字。
Initials (I)	证书所有者姓名的每个部分的第一个字母。
Locality (L)	组织所在的城市或城镇。
Name (N)	证书所有者的姓名。
Organization (O)	公司、机构、代理、协会或其他实体的名称。
Organizational Unit (OU)	组织内的子组。
Serial Number (SER)	证书的序列号。
Surname (SN)	证书所有者的姓氏。
State/Province (S/P)	组织所在的省、自治区或直辖市。
Title (T)	证书所有者的头衔，例如博士。
User ID (UID)	证书所有者的标识号。

- Secondary DN Field -（可选）选择您要配置用于授权的辅助 DN 字段。默认设置为 OU。选项包括以前表中的所有选项，加上 **None**，如果您不想包括辅助字段可选择此选项。

标识邮件代理接口

Email Proxy Access 屏幕允许您标识在其上配置邮件代理的接口。您可以在各个接口上配置和编辑邮件代理，而且您可以为一个接口配置和编辑邮件代理，然后将设置应用至所有接口。您无法为管理专用接口或子接口配置邮件代理。

过程

步骤 1 浏览至**配置** > **VPN** > **邮件代理** > **访问**，显示为接口启用的内容。

- Interface - 显示所有已配置接口的名称。
- POP3S Enabled - 显示是否为接口启用 POP3S。
- IMAP4s Enabled - 显示是否为接口启用 IMAP4S。
- SMTPS Enabled - 显示是否为接口启用 SMTPS。

步骤 2 点击**编辑**可更改突出显示的接口的邮件代理设置。

配置邮件代理的身份验证

为每种邮件代理类型配置身份验证方法。

过程

步骤 1 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **身份验证**。

步骤 2 从多种身份验证方法中选择：

- AAA - 选择此项表示需要 AAA 身份验证。此选项需要一个配置的 AAA 服务器。用户要提供用户名、服务器和密码。用户必须同时提供 VPN 用户名和邮件用户名，其以 VPN 名称分隔符分隔（仅当用户名各不相同时）。
- Certificate - 选择此选项表示需要进行证书身份验证。

  注释 证书身份验证对于当前 ASA 软件版本中的邮件代理不起作用。

  证书身份验证要求用户拥有 ASA 可在 SSL 协商期间验证的证书。您可以将证书身份验证用作唯一的身份验证方法，如 SMTPS 代理。其他邮件代理需要两种身份验证方法。

  证书身份验证需要均来自相同 CA 的三个证书：

  - ASA 上的 CA 证书。

- 客户端 PC 上的一个 CA 证书。

- 客户端 PC 上的网络浏览器证书，有时称为个人证书或网络浏览器证书。

- Piggyback HTTPS - 选择以便要求进行 Piggyback 身份验证。

  此身份验证方案要求用户已建立无客户端 SSL VPN 会话。用户只提供邮件用户名。不需要密码。用户必须同时提供 VPN 用户名和邮件用户名，其以 VPN 名称分隔符分隔（仅当用户名各不相同时）。

  IMAP 可生成不受同时用户计数限制的一些会话，但会对某个用户名允许的同时登录数量进行计数。如果 IMAP 会话数超过此最大数量，且无客户端 SSL VPN 连接到期，则用户随后无法建立新连接。有多种解决方案：

  因为大多数 SMTP 服务器不允许用户登录，所以 SMTPS 邮件最常使用 Piggyback 身份验证。

  注释 IMAP 可生成不受同时用户计数限制的一些会话，但会对某个用户名允许的同时登录数量进行计数。如果 IMAP 会话数超过此最大数量，且无客户端 SSL VPN 连接到期，则用户随后无法建立新连接。有多种解决方案：

  - 用户可以关闭 IMAP 应用以便通过 ASA 清除会话，然后建立新的无客户端 SSL VPN 连接。

  - 管理员可增加 IMAP 用户的同时登录 (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General)。

  - 为邮件代理禁用 HTTPS/Piggyback 身份验证。

- Mailhost -（仅 SMTPS）选择以便要求进行邮件主机身份验证。此选项只面向 SMTPS 显示，因为 POP3S 和 IMAP4S 始终进行邮件主机身份验证。它需要用户的邮件用户名、服务器和密码。

标识代理服务器

通过此“默认服务器”面板，您可以向ASA标识代理服务器，并为邮件代理配置默认服务器、端口和未经身份验证的会话的限制。

过程

步骤 1 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **默认服务器**。

步骤 2 配置以下字段：

- Name or IP Address - 为默认邮件代理服务器键入 DNS 名称或 IP 地址。
- “端口”- 键入 ASA 在其上侦听邮件代理流量的端口号。允许自动建立到已配置端口的连接。邮件代理只允许该端口上的 SSL 连接。建立 SSL 隧道后，此邮件代理将会开始工作，接着将会进行身份验证。

默认值如下：

- 995（用于 POP3S）
- 993（用于 IMAP4S）
- 988（用于 SMTPS）

- Enable non-authenticated session limit - 选择以便限制未经身份验证的邮件代理会话的数量。允许您为正处于身份验证过程中的会话设置限制，从而防止DOS攻击。当新会话超过设置限制时，ASA 将会终止最早的未进行身份验证的连接。如果不存在未进行身份验证的连接，最早的正进行身份验证的连接会被终止，而不会终止已完成身份验证的会话。

邮件代理连接有三个状态：

- Unauthenticated - 新邮件连接的状态。
- Authenticating - 连接提供用户名时的状态。
- Authenticated - ASA 已完成连接的身份验证时的状态。

配置分隔符

此面板用于为邮件代理身份验证配置用户名/密码分隔符和服务器分隔符。

过程

步骤 1 浏览至**配置** > **功能** > **VPN** > **邮件代理** > **分隔符**。

步骤 2 配置以下字段：

- Username/Password Delimiter - 选择用于分隔 VPN 用户名与邮件用户名的分隔符。将 AAA 身份验证用于邮件代理，并且VPN用户名和邮件用户名不同时，用户需要两个用户名。当用户登录至邮件代理会话时，会输入两个用户名，以您在此处配置的分隔符分隔，另外还有邮件服务器名称。

  注释 无客户端 SSL VPN 邮件代理用户的密码不能包含用作分隔符的字符。

- Server Delimiter - 选择用于分隔用户名与邮件服务器的名称的分隔符。它必须不同于 VPN 名称分隔符。当用户登录至邮件代理会话时，会在用户名字段中同时输入其用户名和服务器。

  例如，使用 : 作为 VPN 名称分隔符，使用 @ 作为服务器分隔符，通过邮件代理登录邮件程序时，用户会以如下格式输入其用户名：vpn_username:e-mail_username@server。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。