電子メール プロキシ

電子メール プロキシを設定すると、リモート電子メール機能をクライアントレス SSL VPN のユーザに拡張できます。ユーザが電子メール プロキシ経由で電子メール セッションを試行すると、電子メール クライアントが SSL プロトコルを使用してトンネルを確立します。

電子メール プロキシ プロトコルは次のとおりです。

POP3S

POP3S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 995 をリッスンし、ポート 995 または設定されたポートとの接続が自動的に許可されます。POP3 プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に POP3 プロトコルが開始され、認証が行われます。POP3S は、電子メール受信用のプロトコルです。

IMAP4S

IMAP4S は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 993 をリッスンし、ポート 993 または設定されたポートとの接続が自動的に許可されます。IMAP4S プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に IMAP4S プロトコルが開始され、認証が行われます。IMAP4S は、電子メール受信用のプロトコルです。

SMTPS

SMTPS は、クライアントレス SSL VPN がサポートする電子メール プロキシの 1 つです。デフォルトでは、セキュリティ アプライアンスがポート 988 をリッスンし、ポート 988 または設定されたポートとの接続が自動的に許可されます。SMTPS プロキシは、SSL 接続だけをそのポートで許可します。SSL トンネルが確立された後に SMTPS プロトコルが開始され、認証が行われます。SMTPS は、電子メール送信用のプロトコルです。

- 電子メール プロキシの設定 （2 ページ）
- AAA サーバ グループの設定 （2 ページ）
- 電子メール プロキシを使用するインターフェイスの識別 （4 ページ）
- 電子メール プロキシの認証の設定 （5 ページ）
- プロキシ サーバの識別 （6 ページ）

• デリミタの設定 （7 ページ）

電子メール プロキシの設定

電子メール プロキシの要件

- 電子メールプロキシを経由してローカルとリモートの両方から電子メールにアクセスするユーザは、電子メール プログラムで、ローカル アクセス用とリモート アクセス用に別々の電子メール アカウントが必要です。
- 電子メール プロキシ セッションでユーザが認証される必要があります。

AAA サーバ グループの設定

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[AAA]** を参照します。

ステップ 2 適切なタブ（[POP3S]、[IMAP4S]、または [SMTPS]）を選択して AAA サーバ グループを関連付け、これらのセッションに適用するデフォルトのグループ ポリシーを設定します。

- [AAA server groups]：[AAA Server Groups] パネル（[Configuration] > [Features] > [Properties] > [AAA Setup] > [AAA Server Groups]）に移動する場合にクリックします。ここでは、AAA サーバ グループを追加または編集できます。
- [group policies]：[Group Policy] パネル（[Configuration] > [Features] > [VPN] > [General] > [Group Policy]）に移動する場合にクリックします。ここでは、グループ ポリシーを追加または編集できます。
- [Authentication Server Group]：ユーザ認証用の認証サーバ グループを選択します。デフォルトでは、認証サーバが設定されていません。AAA を認証方式として設定した場合には（[Configuration] > [Features AAA] > [VPN] > [E-Mail Proxy] > [Authentication] パネル）、AAA サーバを設定してここで選択しないと、常に認証に失敗します。
- [Authorization Server Group]：ユーザ認可用の認可サーバ グループを選択します。デフォルトでは、認可サーバが設定されていません。
- [Accounting Server Group]：ユーザ アカウンティング用のアカウンティング サーバ グループを選択します。デフォルトでは、アカウンティング サーバが設定されていません。
- [Default Group Policy]：AAA が CLASSID 属性を返さない場合にユーザに適用するグループ ポリシーを選択します。長さは、4 ～ 15 文字の英数字です。デフォルトのグループ ポリシーが指定されていない場合や、CLASSID が存在しない場合、ASA はセッションを確立できません。

- [Authorization Settings]：ASA が認可のために識別するユーザ名の値を設定します。この名前は、デジタル証明書を使用して認証し、LDAP または RADIUS 認可を必要とするユーザに適用されます。
  - [Use the entire DN as the username]：認可用の認定者名を使用する場合に選択します。
  - [Specify individual DN fields as the username]：ユーザ認可用に特定の DN フィールドを指定する場合に選択します。

    [DN] フィールドは、プライマリとセカンダリの 2 つを選択できます。たとえば、EA を選択した場合には、ユーザは電子メールアドレスによって認証されます。John Doe という一般名（CN）と johndoe@cisco.com という電子メール アドレスを持つユーザは、John Doe または johndoe として認証されません。彼は johndoe@cisco.com として認証される必要があります。EA および O を選択した場合、John Doe は johndoe@cisco.com および Cisco Systems, Inc. として認証される必要があります。
  - [Primary DN Field]：認可用に設定するプライマリ DN フィールドを選択します。デフォルトは [CN] です。オプションには、次のものが含まれます。

DN フィールド	定義
Country（C）	2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。
Common Name（CN）	ユーザ、システム、その他のエンティティの名前。これは、ID 階層の最下位（最も固有性の高い）レベルです。
DN Qualifier（DNQ）	特定の DN 属性。
E-mail Address（EA）	証明書を所有するユーザ、システム、またはエンティティの電子メール アドレス。
Generational Qualifier（GENQ）	Jr.、Sr.、または III などの世代修飾子。
Given Name（GN）	証明書所有者の名前（名）。
Initials（I）	証明書所有者の姓と名の最初の文字。
Locality（L）	組織が所在する市町村。
Name（N）	証明書所有者の名前。
Organization（O）	会社、団体、機関、協会、その他のエンティティの名前。
Organizational Unit（OU）	組織内のサブグループ。
Serial Number（SER）	証明書のシリアル番号。

DN フィールド	定義
Surname（SN）	証明書所有者の姓。
State/Province（S/P）	組織が所在する州や県。
Title（T）	証明書所有者の役職（Dr. など）。
User ID（UID）	証明書所有者の ID 番号。

- [Secondary DN Field]：（オプション）認可用に設定するセカンダリ DN フィールドを選択します。デフォルトは [OU] です。オプションには、上記の表に記載されているものすべてに加えて、[None] があります。これは、セカンダリ フィールドを指定しない場合に選択します。

電子メールプロキシを使用するインターフェイスの識別

[Email Proxy Access] 画面では、電子メール プロキシを設定するインターフェイスを識別できます。電子メール プロキシは、個々のインターフェイスで設定および編集できます。また、1つのインターフェイスで電子メールプロキシを設定および編集すれば、その設定をすべてのインターフェイスに適用できます。管理専用のインターフェイスやサブインターフェイスに対して電子メール プロキシは設定できません。

手順

ステップ 1 **[Configuration]** > **[VPN]** > **[E-Mail Proxy]** > **[Access]** を参照して、インターフェイスでイネーブルになっている電子メール プロキシを表示します。

- [Interface]：設定されているすべてのインターフェイスの名前を表示します。
- [POP3S Enabled]：そのインターフェイスで POP3S がイネーブルかどうかを示します。
- [IMAP4s Enabled]：そのインターフェイスで IMAP4S がイネーブルかどうかを示します。
- [SMTPS Enabled]：そのインターフェイスで SMTPS がイネーブルかどうかを示します。

ステップ 2 [Edit] をクリックし、強調表示されているインターフェイスの電子メール プロキシ設定を変更します。

電子メール プロキシの認証の設定

電子メール プロキシのタイプごとに認証方式を設定します。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Authentication]** を参照します。

ステップ 2 複数の認証方式から選択できます。

- [AAA]：AAA認証を必須にする場合に選択します。このオプションを使用するには、AAAサーバを設定する必要があります。ユーザは、ユーザ名、サーバ、およびパスワードを入力します。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN名デリミタによって区切ります。
- [Certificate]：証明書認証を必須にする場合に選択します。

  （注） 現在の ASA ソフトウェア リリースでは、証明書認証は電子メール プロキシに対して機能しません。

  証明書認証を使用する場合、ユーザは、ASA が SSL ネゴシエーション時に検証できる証明書を持っている必要があります。SMTPS プロキシでは、証明書認証を唯一の認証方式として使用できます。その他の電子メール プロキシでは 2 種類の認証方式が必要です。

  証明書認証には、すべて同じ CA から発行された 3 種類の証明書が必要です。

  - ASA の CA 証明書。

  - クライアント PC の CA 証明書。

  - クライアント PC の Web ブラウザ証明書。個人証明書または Web ブラウザ証明書とも呼ばれます。

- [Piggyback HTTPS]：ピギーバック認証を必須にする場合に選択します。

  この認証スキームは、ユーザがすでにクライアントレス SSL VPN セッションを確立していることを必須とします。ユーザは電子メールユーザ名だけを入力します。パスワードは不要です。ユーザは、VPN ユーザ名と電子メール ユーザ名の両方を入力する必要があります。そのとき、互いのユーザ名が異なる場合にだけ、VPN名デリミタによって区切ります。

  IMAP は、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えません。IMAP セッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

  SMTPS 電子メールは、最も頻繁にピギーバックを使用します。ほとんどの SMTP サーバが、ユーザがログインすることを許可していないためです。

（注） IMAPは、同時ユーザ数によって制限されない多数のセッションを生成しますが、ユーザ名に対して許可されている同時ログインの数を数えません。IMAPセッションの数がこの最大値を超え、クライアントレス SSL VPN 接続の有効期限が切れた場合には、その後ユーザが新しい接続を確立できません。以下の解決策があります。

- ユーザはIMAPアプリケーションを終了してASAとのセッションをクリアしてから、新しいクライアントレス SSL VPN 接続を確立できる。

- 管理者が IMAP ユーザの同時ログイン数を増やす（[Configuration] > [Features] > [VPN] > [General] > [Group Policy] > [Edit Group Policy] > [General]）。

- 電子メール プロキシの HTTPS/ピギーバック認証をディセーブルにする。

- [Mailhost]：（SMTPS のみ）メールホスト認証を必須にする場合に選択します。POP3S とIMAP4Sは必ずメールホスト認証を実行するため、このオプションは、SMTPSの場合にだけ表示されます。この認証方式では、ユーザの電子メールユーザ名、サーバ、およびパスワードが必要です。

プロキシ サーバの識別

この [Default Server] パネルでは、ASA のプロキシ サーバを識別し、電子メール プロキシに対してデフォルト サーバ、ポート、および非認証セッション制限を設定することができます。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Default Servers]** を参照します。

ステップ 2 次のフィールドを設定します。

- [Name or IP Address]：デフォルトの電子メール プロキシ サーバの DNS 名または IP アドレスを入力します。

- [Port]：ASA が電子メール プロキシ トラフィックをリッスンするポート番号を入力します。設定されたポートに対する接続が自動的に許可されます。電子メール プロキシは、SSL接続だけをこのポートで許可します。SSLトンネルが確立された後に電子メールプロキシが開始され、認証が行われます。

  デフォルトの設定は次のとおりです。

  - 995（POP3S の場合）
  - 993（IMAP4S の場合）
  - 988（SMTPS の場合）

- [Enable non-authenticated session limit]：非認証電子メール プロキシ セッションの数を制限する場合に選択します。認証プロセスでのセッションの制限を設定でき、それによって DOS 攻撃を防ぎます。新しいセッションが、設定された制限を超えると、ASA が最も古い非認証接続を終了します。非認証接続が存在しない場合には、最も古い認証接続が終了します。それによって認証済みのセッションが終了することはありません。

電子メール プロキシ接続には、3 つの状態があります。

- 新規に電子メール接続が確立されると、「認証されていない」状態になります。
- この接続でユーザ名が提示されると、「認証中」状態になります。
- ASA が接続を認証すると、「認証済み」状態になります。

デリミタの設定

このパネルでは、電子メール プロキシ認証で使用するユーザ名/パスワード デリミタとサーバ デリミタを設定します。

手順

ステップ 1 **[Configuration]** > **[Features]** > **[VPN]** > **[E-mail Proxy]** > **[Delimiters]** を参照します。

ステップ 2 次のフィールドを設定します。

- [Username/Password Delimiter]：VPN ユーザ名と電子メール ユーザ名を区切るためのデリミタを選択します。電子メール プロキシで AAA 認証を使用する場合、および VPN ユーザ名と電子メール ユーザ名が異なる場合に両方のユーザ名を使用します。電子メール プロキシセッションにログインするときに、ユーザは両方のユーザ名を入力し、ここで設定したデリミタで区切ります。また、電子メール サーバ名も入力します。

  （注） クライアントレス SSL VPN 電子メール プロキシ ユーザのパスワードに、デリミタとして使用されている文字を含めることはできません。

- [Server Delimiter]：ユーザ名と電子メール サーバ名を区切るためのデリミタを選択します。このデリミタは、VPN 名デリミタとは別にする必要があります。電子メール プロキシセッションにログインする場合には、ユーザ名フィールドにユーザ名とサーバの両方を入力します。

  たとえば、VPN 名デリミタとして : を使用し、サーバ デリミタとして @ を使用する場合には、電子メール プロキシ経由で電子メール プログラムにログインするときに、vpn_username:e-mail_username@server という形式でユーザ名を入力します。