Catalyst 6500 シリーズ スイッチの SSL サービス モジュールのコマンド

この章では、Catalyst 6500 シリーズ スイッチの SSL サービス モジュールのコマンドをアルファベット順に一覧表示します。

SSL サービス モジュールの詳細については、次のマニュアルを参照してください。

- 『*Catalyst 6500 Series Switch SSL Services Module Configuration Note*』
- 『*Catalyst 6500 Series Switch SSL Services Module Installation and Verification Note*』

clear ssl-proxy conn

システム全体ですべての TCP 接続を解除するには、**clear ssl-proxy conn** コマンドを使用します。

clear ssl-proxy conn [**service** *name*]

構文の説明

service *name*	（任意）指定したサービスの接続を解除します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

SSL サービス モジュールで維持されるすべての統計情報カウンタをリセットするには、オプションなしで **clear ssl-proxy connection** コマンドを使用します。

例

次の例では、指定したサービスの接続を解除する方法を示します。

```
ssl-proxy# clear ssl-proxy conn service S6
```

次の例では、システム全体ですべての TCP 接続を解除する方法を示します。

```
ssl-proxy# clear ssl-proxy conn
ssl-proxy#
```

clear ssl-proxy session

セッション キャッシュからすべてのエントリをクリアするには、**clear ssl-proxy session** コマンドを使用します。

clear ssl-proxy session [**service** *name*]

構文の説明

service *name*	（任意）指定したサービスのセッション キャッシュをクリアします。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
SSL Services Module Release 1.2(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

すべてのサービスのセッション キャッシュからすべてのエントリをクリアするには、オプションなしで **clear ssl-proxy session** コマンドを使用します。

例

次の例では、SSL サービス モジュールの指定されたサービスのセッション キャッシュからエントリをクリアする方法を示します。

```
ssl-proxy# clear ssl-proxy session service S6
```

次の例では、SSL サービス モジュールで維持されるセッション キャッシュ内のすべてのエントリをクリアする方法を示します。

```
ssl-proxy# clear ssl-proxy session
ssl-proxy#
```

clear ssl-proxy stats

SSL サービス モジュールの複数のシステム コンポーネントで維持されている統計情報カウンタをリセットするには、**clear ssl-proxy stats** コマンドを使用します。

clear ssl-proxy stats [**crypto** | **fdu** | **ipc** | **pki** | **service** | **ssl** | **tcp**]

構文の説明

crypto	（任意）クリプトについての統計情報をクリアします。
fdu	（任意）F6DU についての統計情報をクリアします。
ipc	（任意）Inter-Process Communications（IPC; プロセス間通信）についての統計情報をクリアします。
pki	（任意）Public Key Infrastruture（PKI; 公開キー インフラストラクチャ）についての情報をクリアします。
service *name*	（任意）特定のサービスの統計情報をクリアします。
ssl	（任意）SSL についての統計情報をクリアします。
tcp	（任意）TCP についての統計情報をクリアします。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

SSL サービス モジュールで維持されるすべての統計情報カウンタをリセットするには、オプションなしで **clear ssl-proxy stats** コマンドを使用します。

例

次の例では、SSL サービス モジュールの複数のシステム コンポーネントで維持される統計情報カウンタをリセットする方法を示します。

```
ssl-proxy# clear ssl-proxy stats crypto
ssl-proxy# clear ssl-proxy stats ipc
ssl-proxy# clear ssl-proxy stats pki
ssl-proxy# clear ssl-proxy stats service S6
```

次の例では、SSL サービス モジュールで維持するすべての統計情報カウンタをクリアする方法を示します。

```
ssl-proxy# clear ssl-proxy stats
ssl-proxy#
```

crypto ca export pem

SSL サービス モジュールから Privacy-Enhanced Mail（PEM）ファイルをエクスポートするには、**crypto ca export pem** コマンドを使用します。

crypto ca export *trustpoint_label* **pem** {**terminal** {**des** | **3des**} {**url** *url*}} *pass_phrase*

構文の説明

trustpoint-label	トラストポイントの名前。
terminal	端末上に要求を表示します。
des	56 ビットの DES-CBC 暗号化アルゴリズムを指定します。
3des	168 ビットの DES（3DES）暗号化アルゴリズムを指定します。
url *url*	URL ロケーションを設定します。有効な値は次のとおりです。 • **ftp:** : FTP: ファイル システムにエクスポートする • **null:** : NULL: ファイル システムにエクスポートする • **nvram:** : NVRAM: ファイル システムにエクスポートする • **rcp:** : RCP: ファイル システムにエクスポートする • **scp:** : SCP: ファイル システムにエクスポートする • **system:** : system: ファイル システムにエクスポートする • **tftp:** : TFTP: ファイル システムにエクスポートする
pass-phrase	秘密キーを保護するために使用されるパス フレーズ。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 1.2(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

pass_phrase はスペースおよび句読点を含むフレーズで指定できます。「**?**」は Cisco IOS パーサーに対して特別な意味を持つので使用できません。

パス フレーズ保護では、パス フレーズをキーに関連付けます。パス フレーズは、キーのエクスポート時に暗号化するために使用されます。このキーをインポートする場合、同じパス フレーズを入力して復号化する必要があります。

「unexportable」とマークされたキーはエクスポートできません。

プロンプトが表示される場合は、デフォルトのファイル拡張子を変更できます。デフォルトのファイル拡張子は次のとおりです。

- 公開キー（.pub）
- 秘密キー（.prv）
- 証明書（.crt）
- CA 証明書（.ca）
- 署名キー（-sign）
- 暗号キー（-encr）

（注）　SSL ソフトウェア リリース 1.2 では、秘密キー（.prv）、サーバ証明書（.crt）、およびサーバ証明書の発行元 CA 証明書（.ca）のみがエクスポートされます。すべての CA 証明書を含めて証明書チェーン全体をエクスポートするには、PEM ファイルの代わりに PKCS12 ファイルを使用します。

例

次の例では、SSL サービス モジュールで PEM 形式のファイルをエクスポートする方法を示します。

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

関連コマンド

crypto ca import pem

crypto ca import pem

PEM 形式のファイルを SSL サービス モジュールにインポートするには、**crypto ca import pem** コマンドを使用します。

crypto ca import *trustpoint_label* **pem** [**exportable**] {**terminal** | **url** *url* | **usage-keys**} *pass_phrase*

構文の説明

trustpoint-label	トラストポイントの名前。
exportable	（任意）エクスポート可能なキーを指定します。
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを設定します。有効な値は次のとおりです。 • **ftp:** : FTP: ファイル システムにエクスポートする • **null:** : Null: ファイル システムにエクスポートする • **nvram:** : NVRAM: ファイル システムにエクスポートする • **rcp:** : RCP: ファイル システムにエクスポートする • **scp:** : SCP: ファイル システムにエクスポートする • **system:** : system: ファイル システムにエクスポートする • **tftp:** : TFTP: ファイル システムにエクスポートする
pass_phrase	パス フレーズ。
usage-keys	1 つの汎用キー ペアの代わりに、特別な用途の 2 つのキー ペアを生成する必要があることを指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド履歴

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 1.2(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

パス フレーズを正しく入力しなかった場合、エラーが表示されます。*pass_phrase* はスペースおよび句読点を含むフレーズで指定できます。「**?**」は Cisco IOS パーサーに対して特別な意味を持つので使用できません。

パス フレーズ保護では、パス フレーズをキーに関連付けます。パス フレーズは、キーのエクスポート時に暗号化するために使用されます。このキーをインポートする場合、同じパス フレーズを入力して復号化する必要があります。

RSA キーをインポートする場合、公開キーまたはそれに対応する証明書を使用できます。

crypto ca import pem コマンドでは、秘密キー（.prv）、サーバ証明書（.crt）、発行元の CA 証明書（.ca）のみをインポートします。証明書チェーンに複数のレベルの CA がある場合、認証のためにこのコマンドを発行する前に、ルートおよび下位の CA 証明書をインポートする必要があります。カットアンド ペーストまたは TFTP を使用して、ルートおよび下位の CA 証明書をインポートします。

例

次の例では、SSL サービス モジュールから PEM 形式のファイルをインポートする方法を示します。

```
ssl-proxy(config)# crypto ca import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
ssl-proxy(config)# end
ssl-proxy#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

関連コマンド

crypto ca export pem

crypto ca export pkcs12

SSL サービス モジュールから PKCS12 ファイルをエクスポートするには、**crypto ca export pkcs12** コマンドを使用します。

crypto ca export *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

構文の説明

trustpoint_label	トラストポイント ラベルを指定します。
file_system	ファイル システムを指定します。有効な値は、**scp:**、**ftp:**、**nvram:**、**rcp:**、および **tftp:** です。
pkcs12_filename	（任意）インポートする PKCS12 ファイル名を指定します。
pass_phrase	PKCS12 ファイルのパス フレーズを指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

インポートしたキー ペアはエクスポートできません。

SSH を使用する場合、PKCS12 ファイルをエクスポートする場合は、Secure File Transfer（SCP; セキュア ファイル転送）を使用することを推奨します。SCP はホストを認証し、転送セッションを暗号化します。

pkcs12_filename を指定しない場合、デフォルトのファイル名（デフォルトのファイル名は *trustpoint_label*）を受け入れるか、ファイル名を入力するように求められます。値が **ftp:** または **tftp:** の場合、*pkcs12_filename* にフル パスを含めます。

パス フレーズを正しく入力しなかった場合、エラーが表示されます。

複数のレベルの CA がある場合、ルート CA とすべての下位 CA 証明書が PKCS12 ファイルにエクスポートされます。

例

次の例では、SCP を使用して PKCS12 ファイルをエクスポートする方法を示します。

```
ssl-proxy(config)# crypto ca export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:

Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
ssl-proxy(config)#
```

crypto ca import pkcs12

PKCS12 ファイルを SSL サービス モジュールにインポートするには、**crypto ca import** コマンドを使用します。

crypto ca import *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

構文の説明

trustpoint_label	トラストポイント ラベルを指定します。
file_system	ファイル システムを指定します。有効な値は次のとおりです。 • **ftp:** : FTP: ファイル システムからインポートする • **nvram:** : NVRAM: ファイル システムからインポートする • **rcp:** : RCP: ファイル システムからインポートする • **scp:** : SCP: ファイル システムからインポートする • **tftp:** : TFTP: ファイル システムからインポートする
pkcs12_filename	（任意）インポートする PKCS12 ファイル名を指定します。
pass_phrase	PKCS12 ファイルのパス フレーズを指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

コマンド モード

SSH を使用する場合、PKCS12 ファイルをインポートするときに、Secure File Transfer（SCP; セキュア ファイル転送）を使用することを推奨します。SCP はホストを認証し、転送セッションを暗号化します。

pkcs12_filename を指定しない場合、デフォルトのファイル名（デフォルトのファイル名は *trustpoint_label*）を受け入れるか、ファイル名を入力するように求められます。値が **ftp:** または **tftp:** の場合、*pkcs12_filename* にフル パスを含めます。

パス フレーズを正しく入力しなかった場合、エラーが表示されます。

複数のレベルの CA がある場合、ルート CA とすべての下位 CA 証明書が PKCS12 ファイルにエクスポートされます。

例

次の例では、SCP を使用して PKCS12 ファイルをインポートする方法を示します。

```
ssl-proxy(config)# crypto ca import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
ssl-proxy(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
ssl-proxy(config)#
```

crypto key export rsa pem

PEM 形式の RSA キーを SSL サービス モジュールにエクスポートするには、**crypto key export rsa pem** コマンドを使用します。

crypto key export rsa *keylabel* **pem** {**terminal** | **url** *url*} {{**3des** | **des**} [**exportable**] *pass_phrase*}

構文の説明

keylabel	キーの名前。
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを設定します。有効な値は次のとおりです。 • **ftp:** : FTP: ファイル システムにエクスポートする • **null:** : Null: ファイル システムにエクスポートする • **nvram:** : NVRAM: ファイル システムにエクスポートする • **rcp:** : RCP: ファイル システムにエクスポートする • **scp:** : SCP: ファイル システムにエクスポートする • **system:** : system: ファイル システムにエクスポートする • **tftp:** : TFTP: ファイル システムにエクスポートする
des	56 ビットの DES-CBC 暗号化アルゴリズムを指定します。
3des	168 ビットの DES（3DES）暗号化アルゴリズムを指定します。
exportable	（任意）エクスポート可能なキーを指定します。
pass_phrase	パス フレーズ。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 1.2(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

パス フレーズはスペースおよび句読点を含むフレーズで指定できます。「**?**」は Cisco IOS パーサーに対して特別な意味を持つので使用できません。

パス フレーズ保護では、パス フレーズをキーに関連付けます。パス フレーズは、キーのエクスポート時に暗号化するために使用されます。このキーをインポートする場合、同じパス フレーズを入力して復号化する必要があります。

例

次の例では、SSL サービス モジュールからキーをエクスポートする方法を示します。

```
ssl-proxy(config)# crypto key export rsa test-keys pem url scp: 3des password
% Key name:test-keys
   Usage:General Purpose Key
Exporting public key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.pub]?

Password:

Writing test-keys.pub Writing file to scp://lab@7.0.0.7/test-keys.pub
Password:
!
Exporting private key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.prv]?

Password:

Writing test-keys.prv Writing file to scp://lab@7.0.0.7/test-keys.prv
Password:
ssl-proxy(config)#
```

crypto key import rsa pem

外部システムから PEM 形式の RSA キーをインポートするには、**crypto key import rsa pem** コマンドを使用します。

crypto key import rsa *keylabel* **pem** [**usage-keys**] {**terminal** | **url** *url*} [**exportable**] *passphrase*}

構文の説明

keylabel	キーの名前。
usage-keys	（任意）1 つの汎用キー ペアの代わりに、特別な用途の 2 つのキー ペアを生成する必要があることを指定します。
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを設定します。有効な値は次のとおりです。 • **ftp:** : FTP: ファイル システムからインポートする • **null:** : null: ファイル システムからインポートする • **nvram:** : NVRAM: ファイル システムからインポートする • **rcp:** : RCP: ファイル システムからインポートする • **scp:** : SCP: ファイル システムからインポートする • **system:** : system: ファイル システムからインポートする • **tftp:** : TFTP: ファイル システムからインポートする
exportable	（任意）エクスポート可能なキーを指定します。
passphrase	パス フレーズ。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 1.2(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

パス フレーズはスペースおよび句読点を含むフレーズで指定できます。「**?**」は Cisco IOS パーサーに対して特別な意味を持つので使用できません。

パス フレーズ保護では、パス フレーズをキーに関連付けます。パス フレーズは、キーのエクスポート時に暗号化するために使用されます。このキーをインポートする場合、同じパス フレーズを入力して復号化する必要があります。

例

次の例では、外部システムから PEM 形式の RSA キーをインポートし、PEM 形式の RSA キーを SSL サービス モジュールにエクスポートする方法を示します。

```
ssl-proxy(config)# crypto key import rsa newkeys pem url scp: password
% Importing public key or certificate PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.pub]? test-keys.pub

Password:
Sending file modes:C0644 272 test-keys.pub
Reading file from scp://lab@7.0.0.7/test-keys.pub!
% Importing private key PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.prv]? test-keys.prv

Password:
Sending file modes:C0644 963 test-keys.prv
Reading file from scp://lab@7.0.0.7/test-keys.prv!% Key pair import succeeded.

ssl-proxy(config)#
```

debug ssl-proxy

複数のシステム コンポーネントでデバッグ フラグをオンにするには、**debug ssl-proxy** コマンドを使用します。このコマンドの **no** 形式を使用して、デバッグ フラグをオフにします。

debug ssl-proxy {**app** | **fdu** [*type*] | **ipc** | **pki** [*type*] | **ssl** [*type*] | **tcp** [*type*]}

構文の説明

app	App デバッグをオンにします。
fdu *type*	FDU デバッグをオンします。（任意）*type* の有効な値は **cli**、**hash**、**ipc**、および **trace** です。詳細については、「使用上のガイドライン」を参照してください。
ipc	IPC デバッグをオンにします。
pki *type*	PKI デバッグをオンにします。（任意）*type* の有効な値は **cert**、**events**、**history**、**ipc**、および **key** です。詳細については、「使用上のガイドライン」を参照してください。
ssl *type*	SSL デバッグをオンにします。（任意）*type* の有効な値は **alert**、**error**、**handshake**、および **pkt** です。詳細については、「使用上のガイドライン」を参照してください。
tcp *type*	TCP デバッグをオンにします。（任意）*type* の有効な値は **event**、**packet**、**state**、および **timers** です。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

fdu *type* には次の値があります。

- **cli**：FDU CLI をデバッグします。
- **hash**：FDU ハッシュをデバッグします。
- **ipc**：FDU IPC をデバッグします。
- **trace**：FDU トレースをデバッグします。

pki *type* には次の値があります。

- **certs**：証明書の管理をデバッグします。
- **events**：イベントをデバッグします。
- **history**：証明書の履歴をデバッグします。
- **ipc**：IPC メッセージおよびバッファをデバッグします。
- **key**：キーの管理をデバッグします。

ssl *type* には次の値があります。

- **alert**：SSL アラート イベントをデバッグします。
- **error**：SSL エラー イベントをデバッグします。
- **handshake**：SSL ハンドシェイク イベントをデバッグします。
- **pkt**：送受信された SSL パケットをデバッグします。

（注） TCP デバッグ コマンドは、負荷がほとんどないか、またはまったくない状態で基本的な接続問題（たとえば、仮想サーバまたは実際のサーバとの間で接続が確立されない場合）をトラブルシューティングする場合だけに使用します。

TCP デバッグ コマンドを実行する場合、コンソール上に TCP モジュールに大量のデバッグ情報が表示され、それによってモジュールのパフォーマンスが大幅に低下する可能性があります。モジュールのパフォーマンスが低いと、TCP 接続タイマー、パケット、および状態遷移の処理が遅延する可能性があります。

tcp *type* には次の値があります。

- **events**：TCP イベントをデバッグします。
- **pkt**：送受信された TCP パケットをデバッグします。
- **state**：TCP 状態をデバッグします。
- **timers**：TCP タイマーをデバッグします。

例

次の例では、App デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy app
ssl-proxy#
```

次の例では、FDU デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy fdu
ssl-proxy#
```

次の例では、IPC デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy ipc
ssl-proxy#
```

次の例では、PKI デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy pki
ssl-proxy#
```

次の例では、SSL デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy ssl
```

```
ssl-proxy#
```

次の例では、TCP デバッグをオンにする方法を示します。

```
ssl-proxy# debug ssl-proxy tcp
ssl-proxy#
```

次の例では、TCP デバッグをオフにする方法を示します。

```
ssl-proxy# no debug ssl-proxy tcp
ssl-proxy#
```

do

グローバル コンフィギュレーション モードまたはその他のコンフィギュレーション モードあるいはサブモードから EXEC レベルのコマンドを実行するには、**do** コマンドを使用します。

do *command*

構文の説明

command	実行する EXEC レベルのコマンド。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC レベルのコマンドを実行するグローバル コンフィギュレーションまたはその他のコンフィギュレーション モードあるいはサブモード。

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

注意　EXEC モードでは **do** コマンドを入力しないでください。サービスの中断が発生する可能性があります。

do コマンドを使用して **configure terminal** コマンドを実行できません。これは、**configure terminal** コマンドを入力すると、モードがコンフィギュレーション モードに変更されるためです。

do コマンドを使用して、グローバル コンフィギュレーション モードまたはその他のコンフィギュレーション モードあるいはサブモードで **copy** または **write** コマンドを実行できません。

例

次の例では、グローバル コンフィギュレーション モードで EXEC レベルの **show interfaces** コマンドを実行する方法を示します。

```
ssl-proxy(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
ssl-proxy(config)#
```

show ssl-proxy admin-info

管理 VLAN とそれに関連する IP およびゲートウェイ アドレスを表示するには、**show ssl-proxy admin-info** コマンドを使用します。

show ssl-proxy admin-info

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、管理 VLAN とそれに関連する IP およびゲートウェイ アドレスを表示する方法を示します。

```
ssl-proxy# show ssl-proxy admin-info
STE administration VLAN: 2
STE administration IP address: 207.57.100.18
STE administration gateway: 207.0.207.5
ssl-proxy#
```

関連コマンド

ssl-proxy vlan

show ssl-proxy buffers

TCP バッファの使用状況についての情報を表示するには、**show ssl-proxy buffers** コマンドを使用します。

show ssl-proxy buffers

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、TCP サブシステムのバッファの使用状況とその他の情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy buffers
Buffers info for TCP module 1
TCP data buffers used 2816 limit 112640
TCP ingress buffer pool size 56320 egress buffer pool size 56320
TCP ingress data buffers min-thresh 7208960 max-thresh 21626880
TCP ingress data buffers used Current 0 Max 0
TCP ingress buffer RED shift 9 max drop prob 10
Conns consuming ingress data buffers 0
Buffers with App 0
TCP egress data buffers used Current 0 Max 0
Conns consuming egress data buffers 0
In-sequence queue bufs 0 OOO bufs 0
ssl-proxy#
```

関連コマンド

ssl-proxy policy tcp

show ssl-proxy certificate-history

証明書のイベント履歴についての情報を表示するには、**show ssl-proxy certificate-history** コマンドを使用します。

show ssl-proxy certificate-history [**service** [*name*]]

構文の説明

service *name*	プロキシ サービスのすべての証明書レコードおよび（任意で）特定のプロキシ サービスの証明書レコードを表示します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

show ssl-proxy certificate-history コマンドでは、次のレコードが表示されます。

- サービス名
- キー ペア名
- 生成時刻およびインポート時刻
- トラストポイント名
- 証明書の件名
- 証明書の発行元名
- シリアル番号
- 日付

各レコードに対して Syslog メッセージが生成されます。制限値の 512 レコードに達した後は、最も古いレコードが削除されます。

例

次の例では、証明書の処理のすべてのイベント履歴を表示する方法を示します。

```
ssl-proxy# show ssl-proxy certificate-history
Record 1, Timestamp:00:00:51, 16:36:34 UTC Oct 31 2002
    Installed Server Certificate, Index 5
    Proxy Service:s1,  Trust Point:t3
    Key Pair Name:k3,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:12:27:58 UTC Oct 30 2002
    Subject Name:OID.1.2.840.113549.1.9.2 = simpson5-2-ste.cisco.com,
OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5D3D1931000100000D99
    Validity Start Time:21:58:12 UTC Oct 30 2002
    End Time:22:08:12 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 2, Timestamp:00:01:06, 16:36:49 UTC Oct 31 2002
    Installed Server Certificate, Index 6
    Proxy Service:s5,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
% Total number of certificate history records displayed = 4
ssl-proxy#
```

次の例では、特定のプロキシ サービスの証明書レコードを表示する方法を示します。

```
ssl-proxy# show ssl-proxy certificate-history service s6
Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
Total number of certificate history records displayed = 2
```

関連コマンド

ssl-proxy service

show ssl-proxy conn

SSL サービス モジュールから TCP 接続を表示するには、**show ssl-proxy conn** コマンドを使用します。

show ssl-proxy conn 4tuple [**local** {**ip** *local-ip-addr local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**port** *local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [**local** {**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]

show ssl-proxy conn service *name*

構文の説明

4tuple	特定のアドレスの TCP 接続を表示します。
local	（任意）特定のローカル デバイスの TCP 接続を表示します。
ip *local-ip-addr*	ローカル デバイスの IP アドレス。
local-port	ローカル デバイスのポート番号。
remote	（任意）特定のリモート デバイスの TCP 接続を表示します。
ip *remote-ip-addr*	リモート デバイスの IP アドレス。
port *remote-port*	リモート デバイスのポート番号。
port *local-port*	（任意）特定のローカル ポートの TCP 接続を表示します。
service *name*	特定のプロキシ サービスの TCP 接続を表示します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

show ssl-proxy conn コマンドでは、次のレコードが表示されます。

- Local Address
- Remote Address
- VLAN
- Conid
- Send-Q
- Recv-Q
- State

  State レコードは、SSL サービス モジュールとリモート デバイスの間の接続の TCP 状態を示します。TCP 状態については、次の表で説明します。

表 2-1　TCP 接続状態の説明

LISTEN	このモジュールは、TCP 接続を開始する要求を待機しています。
SYN_SEND	このモジュールは、TCP 接続を開くために、SYN パケットを別のデバイスに送信しました。
SYN_RECEIVED	このモジュールは、TCP 接続を開くことを要求している別のデバイスから SYN パケットを受信しました。
ESTABLISHED **または ESTAB**	スリーウェイ TCP ハンドシェイク（SYN、SYN/ACK、ACK）が完了し、このモジュールと別のデバイスの間で TCP 接続が確立します。
FIN_WAIT_1	このモジュールは、TCP 接続を閉じるために、FIN パケットを接続先のデバイスに送信しました。
TIME_WAIT **または TWAIT**	このモジュールは FIN シーケンスを正常に完了し、接続先のデバイスで TCP 接続を閉じます。遅延パケットを受信するために、30 ～ 120 秒間、接続がこの状態で保持されます。
CLOSE_WAIT	このモジュールは、TCP 接続を閉じることを要求している接続先のデバイスから FIN パケットを受信しました。
FIN_WAIT_2	TCP 接続を閉じるために FIN パケットを接続先のデバイスに送信した後、このモジュールは ACK パケットを受信し、FIN パケットを待機します。
LAST_ACK	接続先のデバイスの要求により、このモジュールは TCP 接続を閉じ、他のデバイスからの最後の ACK を待機します。
CLOSING	このモジュールは TCP 接続をアクティブに閉じ、TIME_WAIT 状態に入る前に、他のデバイスからの最後の ACK を待機します。
CLOSED	TCP 接続が閉じられ、すべての待機時間と確認応答が完了します。

例

次の例では、SSL サービス モジュールから確立された TCP 接続を表示するさまざまな方法を示します。

```
ssl-proxy# show ssl-proxy conn
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.0.0.10:4430         1.200.200.14:48582    2    0      0      0      ESTAB
1.200.200.14:48582    2.100.100.72:80       2    1      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48583    2    2      0      0      ESTAB
1.200.200.14:48583    2.100.100.72:80       2    3      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48584    2    4      0      0      ESTAB
1.200.200.14:48584    2.100.100.72:80       2    5      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48585    2    6      0      0      ESTAB
1.200.200.14:48585    2.100.100.72:80       2    7      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48586    2    8      0      0      ESTAB
1.200.200.14:48586    2.100.100.72:80       2    9      0      0      ESTAB

ssl-proxy# show ssl-proxy conn 4tuple local port 443
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.133:443       1.200.200.12:39728    2    113676 0      0      TWAIT
No Bound Connection

2.50.50.133:443       1.200.200.12:39729    2    113680 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:40599    2    113684 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48031    2    114046 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48032    2    114048 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48034    2    114092 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48035    2    114100 0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn 4tuple remote ip 1.200.200.14
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:38814    2    58796  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38815    2    58800  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38817    2    58802  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38818    2    58806  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38819    2    58810  0      0      TWAIT
No Bound Connection
```

```
2.50.50.131:443       1.200.200.14:38820    2    58814  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38821    2    58818  0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn service iis1
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:41217    2    121718 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41218    2    121722 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41219    2    121726 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41220    2    121794 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41221    2    121808 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41222    2    121940 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41223    2    122048 0      0      TWAIT
No Bound Connection
```

show ssl-proxy crash-info

SSL サービス モジュールからのソフトウェアによって強制されたリセットについての情報を収集するには、**show ssl-proxy crash-info** コマンドを使用します。

show ssl-proxy crash-info [**brief** | **details**]

構文の説明

brief	（任意）プロセッサのレジスタに制限された、ソフトウェアによって強制されたリセット情報の小規模なサブセットを収集します。
details	（任意）ソフトウェアによって強制されたリセット情報のすべてを、例外スタックと割り込みスタックのダンプも含めて収集します（出力が完了するまでに最大 10 分かかる可能性があります）。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、ソフトウェアによって強制されたリセットについての情報を収集する方法を示します。

```
ssl-proxy# show ssl-proxy crash-info

===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

NVRAM CHKSUM:0xEB28
NVRAM MAGIC:0xC8A514F0
NVRAM VERSION:1

++++++++++ CORE 0 (FDU) ++++++++++++++++++++++

   CID:0
   APPLICATION VERSION:2003.04.15 14:50:20 built for cantuc
   APPROXIMATE TIME WHEN CRASH HAPPENED:14:06:04 UTC Apr 16 2003
   THIS CORE DIDN'T CRASH
   TRACEBACK:222D48 216894
   CPU CONTEXT  ------------------------------

$0 :00000000, AT :00240008, v0 :5A27E637, v1 :000F2BB1
a0 :00000001, a1 :0000003C, a2 :002331B0, a3 :00000000
t0 :00247834, t1 :02BFAAA0, t2 :02BF8BB0, t3 :02BF8BA0
t4 :02BF8BB0, t5 :00247834, t6 :00000000, t7 :00000001
```

```
s0 :00000000, s1 :0024783C, s2 :00000000, s3 :00000000
s4 :00000001, s5 :0000003C, s6 :00000019, s7 :0000000F
t8 :00000001, t9 :00000001, k0 :00400001, k1 :00000000
gp :0023AE80, sp :031FFF58, s8 :00000019, ra :00216894
LO :00000000, HI :0000000A, BADVADDR :828D641C
EPC :00222D48, ErrorEPC :BFC02308, SREG :34007E03
Cause 0000C000 (Code 0x0):Interrupt exception

CACHE ERROR registers  -------------------

CacheErrI:00000000, CacheErrD:00000000
ErrCtl:00000000, CacheErrDPA:0000000000000000

   PROCESS STACK -----------------------------
      stack top:0x3200000

   Process stack in use:

   sp is close to stack top;

   printing 1024 bytes from stack top:

031FFC00:06405DE0 002706E0 0000002D 00000001  .@]`.'.`...-....
031FFC10:06405DE0 002706E0 00000001 0020B800  .@]`.'.`..... 8.
031FFC20:031FFC30 8FBF005C 14620010 24020004  ..|0.?.\.b..$...
...........
...........
...........
FFFFFFD0:00000000 00000000 00000000 00000000 ................
FFFFFFE0:00627E34 00000000 00000000 00000000 .b~4............
FFFFFFF0:00000000 00000000 00000000 00000006 ................


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

次の例では、ソフトウェアによって強制されたリセットについての情報の小規模なサブセットを収集する方法を示します。

```
ssl-proxy# show ssl-proxy crash-info brief


===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

SKE CRASH INFO Error: wrong MAGIC # 0

CLI detected an error in FDU_IOS crash-info; wrong magic.

------------- COMPLEX 1 [TCP_SSL] ----------------------


Crashinfo fragment #0 from core 2 at offset 0 error:
Remote system reports wrong crashinfo magic.
Bad fragment received. Reception abort.

CLI detected an error in TCP_SSL crash-info;


===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

show ssl-proxy mac address

現在の MAC アドレスを表示するには、**show ssl-proxy mac address** コマンドを使用します。

show ssl-proxy mac address

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SSL サービス モジュールで使用される現在の MAC アドレスを表示する方法を示します。

```
ssl-proxy# show ssl-proxy mac address
STE MAC address: 00e0.b0ff.f232
ssl-proxy#
```

show ssl-proxy natpool

NAT プールについての情報を表示するには、**show ssl-proxy natpool** コマンドを使用します。

show ssl-proxy natpool [*name*]

構文の説明

name	（任意）NAT プール名。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SSL サービス モジュールで設定される特定の NAT アドレス プールについての情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy natpool NP1
Start ip: 207.57.110.1
End ip: 207.57.110.8
netmask: 255.0.0.0
vlan associated with natpool: 2
SSL proxy services using this natpool:
S2
S3
S1
S6
Num of proxies using this natpool: 4
ssl-proxy#
```

関連コマンド

ssl-proxy natpool

show ssl-proxy policy

設定された SSL プロキシ ポリシーを表示するには、**show ssl-proxy policy** コマンドを使用します。

show ssl-proxy policy {**http-header** | **ssl** | **tcp** | **url-rewrite**} [*name*]

構文の説明

http-header	設定された HTTP ヘッダー ポリシーを表示します。
ssl	設定された SSL ポリシーを表示します。
tcp	設定された TCP ポリシーを表示します。
url-rewrite	設定された URL 書き換えポリシーを表示します。
name	（任意）ポリシー名。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 2.1(1)	このコマンドは、**http-header** キーワードおよび **url-rewrite** キーワードを含めるように変更されました。

例

次の例では、HTTP ヘッダー ポリシーについての情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy policy http-header httphdr-policy
 Client Certificate Insertion Header Only
 Session Header Insertion All
 Client IP/Port Insertion Client IP and Port
 Hdr # Custom Header
  0 SSL-Frontend:Enable

>Usage count of this policy: 0
ssl-proxy#
```

次の例では、SSL サービス モジュールで設定される特定の SSL ポリシーについてのポリシー情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy policy ssl ssl-policy1
Cipher suites: (None configured, default ciphers included)
     rsa-with-rc4-128-md5
     rsa-with-rc4-128-sha
     rsa-with-des-cbc-sha
     rsa-with-3des-ede-cbc-sha
SSL Versions enabled:SSL3.0, TLS1.0
strict close protocol:disabled
Session Cache:enabled
```

```
Handshake timeout not configured (never times out)
Num of proxies using this policy:0
```

次の例では、SSL サービス モジュールで設定される特定の TCP ポリシーについてのポリシー情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy policy tcp tcp-policy1
 MSS                 1250
 SYN timeout         75
 Idle timeout        600
 FIN wait timeout    75
 Reassembly timeout  60
 Rx Buffer Share     32768
 Tx Buffer Share     32768
 TOS Carryover       Enabled

 Usage count of this policy:0
ssl-proxy#
```

次の例では、URL 書き換えポリシーについての情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy policy url-rewrite urlrw-policy
 >Rule URL Clearport SSLport
  1 wwwin.cisco.com 80 443
  2 www.cisco.com 8080 444
>
>Usage count of this policy: 0
ssl-proxy#
```

関連コマンド

ssl-proxy policy http-header
ssl-proxy policy ssl
ssl-proxy policy tcp
ssl-proxy policy url-rewrite

show ssl-proxy service

設定された SSL 仮想サービスについての情報を表示するには、**show ssl-proxy service** コマンドを使用します。

show ssl-proxy service [*name*]

構文の説明

name	（任意）サービス名。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SSL サービス モジュールで設定されるすべての SSL 仮想サービスを表示する方法を示します。

```
ssl-proxy# show ssl-proxy service
Proxy Service Name Admin Operation Events
status status
S2 up up
S3 up up
S1 up up
S6 down down
ssl-proxy#
```

次の例では、SSL サービス モジュールで設定される特定の SSL 仮想サービスを表示する方法を示します。

```
ssl-proxy# show ssl-proxy service S6
Service id: 0, bound_service_id: 256
Virtual IP: 10.10.1.104, port: 443
Server IP: 10.10.1.100, port: 80
Virtual SSL Policy: SSL1_PLC
rsa-general-purpose certificate trustpoint: tptest
  Certificate chain for new connections:
    Server Certificate:
       Key Label: tptest
       Serial Number: 01
    Root CA Certificate:
       Serial Number: 00
  Certificate chain complete
Admin Status: up
Operation Status: down
Proxy status: No Client VLAN, No Server VLAN
ssl-proxy#
```

show ssl-proxy stats

統計情報カウンタについての情報を表示するには、**show ssl-proxy stats** コマンドを使用します。

show ssl-proxy stats [*type*]

構文の説明

type	（任意）情報のタイプ。有効な値は **crypto**、**ipc**、**pki**、**service**、**ssl**、および **tcp** です。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 1.2(1)	**show ssl-proxy stats** コマンドの出力が、セッション割り当ての失敗およびセッションの制限を超えたテーブルについての情報を含めるように変更されました。

使用上のガイドライン

type 値は次のように定義されています。

- **crypto**：クリプトについての統計情報を表示します。
- **ipc**：IPC 統計情報を表示します。
- **pki**：PKI 統計情報を表示します。
- **service**：プロキシ サービス統計情報を表示します。
- **ssl**：SSL の詳細な統計情報を表示します。
- **tcp**：TCP の詳細な統計情報を表示します。

例

次の例では、SSL サービス モジュールで収集されるすべての統計情報カウンタを表示する方法を示します。

```
ssl-proxy# show ssl-proxy stats
TCP Statistics:
    Conns initiated     : 1970288       Conns accepted       : 1970288
    Conns established   : 3797817       Conns dropped        : 2481867
    Conns Allocated     : 1970288       Conns Deallocated    : 1970288
    Conns closed        : 3940576       SYN timeouts         : 141865
    Idle timeouts       : 0             Total pkts sent      : 2499818678
    Data packets sent   : 2034445802    Data bytes sent      : 2837513871
```

```
    Total Pkts rcvd     : 2055992562    Pkts rcvd in seq     : 1365961238
    Bytes rcvd in seq   : 464953685

SSL Statistics:
    conns attempted     : 1970288       conns completed     : 1970288
    full handshakes     : 1968370       resumed handshakes  : 0
    active conns        : 0             active sessions     : 0
    renegs attempted    : 0             conns in reneg      : 0
    handshake failures  : 1918          data failures       : 0
    fatal alerts rcvd   : 0             fatal alerts sent   : 1918
    no-cipher alerts    : 0             ver mismatch alerts : 0
    no-compress alerts  : 0             bad macs received   : 0
    pad errors          : 0             session fails       : 0

FDU Statistics:
    IP Frag Drops       : 0             IP Version Drops    : 0
    IP Addr Discards    : 0             Serv_Id Drops       : 27
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             TCP Checksum Drops  : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 3940576       Flow Deletes        : 3940576
    Conn Id allocs      : 1970288       Conn Id deallocs    : 1970288
    Tagged Pkts Drops   : 0             Non-Tagg Pkts Drops : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 0             Enable ipcs         : 0
    Unsolicited ipcs    : 0             Duplicate Add ipcs  : 0
    IOS Broadcast Pkts  : 82820         IOS Unicast Pkts    : 1360
    IOS Multicast Pkts  : 0             IOS Total Pkts      : 84180
    IOS Congest Drops   : 0             SYN Discards        : 0
    TCP 5-tuple reuse   : 0

ssl-proxy#
```

次に、SSL の統計情報を表示する例を示します。

```
ssl-proxy# show ssl-proxy stats ssl
SSL Statistics:
    conns attempted     : 1970288       conns completed     : 1970288
    conns in handshake  : 0             conns in data       : 0
    renegs attempted    : 0             conns in reneg      : 0
    active sessions     : 0             max handshake conns : 472
    rand bufs allocated : 114801        cached rand buf miss: 0
    current device q len: 0             max device q len    : 144
    sslv2 forwards      : 0             cert reqs processed : 1897
    fatal alerts rcvd   : 0             fatal alerts sent   : 1918
    stale packet drops  : 0             service_id discards : 0
    session reuses      : 0             hs handle in use    : 0
    bad clnt session id : 0             expired session id  : 0
    available ctx count : 64            ctx cleanup count   : 22
    device reset count  : 22

    SSL3 Statistics:
      full handshakes    : 0             resumed handshakes : 0
      handshake failures : 0             data failures      : 0
      bad macs received  : 0             pad errors         : 0
      conns established with cipher rsa-with-rc4-128-md5        : 0
      conns established with cipher rsa-with-rc4-128-sha        : 0
      conns established with cipher rsa-with-des-cbc-sha        : 0
      conns established with cipher rsa-with-3des-ede-cbc-sha   : 0

    TLS1 Statistics:
      full handshakes    : 1968370       resumed handshakes : 0
      handshake failures : 1918          data failures      : 0
      bad macs received  : 0             pad errors         : 0
```

```
      conns established with cipher rsa-with-rc4-128-md5        : 1968369
      conns established with cipher rsa-with-rc4-128-sha        : 0
      conns established with cipher rsa-with-des-cbc-sha        : 0
      conns established with cipher rsa-with-3des-ede-cbc-sha   : 1

SSL error statistics:
    session alloc fails : 0             session limit exceed: 0
    handshake init fails: 0             renegotiation fails : 0
    no-cipher alerts    : 0             ver mismatch alerts : 0
    no-compress alerts  : 0             multi buf rec errors: 0
    ssl peer closes     : 0             non-ssl peer closes : 0
    unexpected record   : 0             rec formatting error: 0
    rsa pkcs pad errors : 0             premaster errors    : 0
    failed rsa reqs     : 0             failed random reqs  : 0
    failed key-material : 0             failed master-secret: 0
    failed update hash  : 0             failed finish hash  : 0
    failed encrypts     : 0             failed decrypts     : 0
    bad record version  : 0             bad record size     : 0
    cert verify errors  : 1896          unsupported certs   : 0
    conn aborted        : 0
    overload drops      : 0             hs limit exceeded   : 0
    hs handle mem fails : 0             conn reuse error    : 0
    dev invalid params  : 0             dev failed requests : 0
    dev timeout         : 0             dev busy            : 0
    dev cancelled       : 0             no dev fails        : 0
    dev resource fails  : 0             dev unknown errors  : 0
    dev conn ctx fails  : 0             dev cmd ctx fails   : 0
    mem alloc fails     : 0             buf alloc fails     : 0
    invalid cipher algo : 0             invalid hash algo   : 0
    unaligned buf addr  : 0             unaligned buf len   : 0
    internal error      : 0             unknown ipcs        : 0
    double free attempts: 0             alert-send fails    : 0

SSL Crypto Statistics:
    blocks encrypted    : 89226334      blocks decrypted    : 4864649
    bytes encrypted     : 1500039492    bytes decrypted     : 314938656
    crypto failures     : 0
    IKECount            : 128270        IKEFailedCount      : 0
    DHPublicCount       : 0             DHSharedCount       : 0
    rsa public key ops  : 1             rsa private key ops : 128269
    dsa_signs           : 0             dsa_verifies        : 0
    device dma errors   : 0
    PushMCR_nopkts      : 472328917     PushMCR_pushed      : 0
    PushMCR1_full       : 160504926     PushMCR2_full       : 0
    PushMCR_push        : 13277229
    GetFreeMCR_busy     : 0             GetFreeMCR_dma_error: 0
    GetFreeMCR_no_rsrc  : 0             GetFreeMCR_success  : 103511789

SSL last 5 sec average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL last 1 min average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL last 5 min average Statistics:
    full handshakes     : 0             resumed handshakes  : 0
    handshake failures  : 0             data failures       : 0
    bytes encrypted     : 0             bytes decrypted     : 0

SSL PKI Statistics:
```

```
    number of malloc    : 245           number of free      : 202
    ssl buf allocated   : 8             ssl buf freed       : 1

    Peer Certificate Verify Statistics:
    cert approved       : 1             cert disapproved    : 0
    peer cert empty     : 1896          total num of request: 1897
    req being processed : 0             req pending         : 0
    longest queue       : 1             longest pending     : 0
    verify congestion   : 0             req dropped, q full : 0
    no memory for verify: 0             verify data error   : 0
    verify context error: 0             context delete error: 0
    timer expired error : 0             timer expired count : 0
    late verify result  : 0             timer turned on     : 1
    timer turned off    : 1             context created     : 1
    context deleted     : 1

    High Priority IPC:
    ipc request received: 18            ipc request dropped : 0
    ipc req duplicated  : 0             ipc req fragment err: 0
    ipc req parm len err: 0             ipc req op code err : 0
    ipc req cert len err: 0             ipc response sent   : 18
    ipc resp no memory  : 0             ipc resp no ssl buf : 0
    ipc buffer allocated: 0             ipc buffer freed    : 0
    ipc buf alloc failed: 0             ipc send msg failed : 0

    Normal Priority IPC:
    ipc buffer allocated: 1             ipc buffer freed    : 1
    ipc request sent    : 1             ipc request received: 3
    ipc buf alloc failed: 0             ipc send msg failed : 0
    ipc requests dropped: 0

SSL Queue Sizes:
    bcm_cmd_ctx_pool_size   : 64            bcm_asym_cmd_ctx_pool_sz: 9000
    bcm_info_pool_size      : 65538         buf_desc_free_q_size    : 94709
    cert_result_free_q_size : 11048         delete_conn_q_size      : 0
    event_q_size            : 0             free_conn_q_size        : 65536
    free_sess_q_size        : 262144        free_sess_active_tmr_qsz: 0
    global_pending_q_size   : 0             to_app_ctx_pool_size    : 512
    ste_asym_req_q_size     : 0             ste_free_req_ctx_pool_sz: 20480
    ste_sym_req_q_size      : 0

SSL Random Buffer Info:
    psuedo_rand_req_pending : 0             rand_req_pending        : 0
    pseudo_rand_req_count   : 71
    curr_psuedo_rand_buf    : 0x0ACB5264    curr_rand_buf           : 0x0ACB520C
    psuedo_rand_buf_a       : 0x0ACB5238    psuedo_rand_buf_a_rx_sz : 2984
    psuedo_rand_buf_b       : 0x0ACB5264    psuedo_rand_buf_b_rx_sz : 3464
    rand_buf_a              : 0x0ACB51E0    rand_buf_a_rx_size      : 4064
    rand_buf_b              : 0x0ACB520C    rand_buf_b_rx_size      : 4064
```

次に、TCP の統計情報を表示する例を示します。

```
ssl-proxy# show ssl-proxy stats tcp
TCP Statistics:
 Connection related :
    Initiated             : 1970288    Accepted             : 1970288
    Established           : 3797817    Dropped              : 2481867
    Dropped before est    : 142324     Closed               : 3940576
    Persist timeout drops : 0          Rxmt timeout drops   : 0
    Current TIME-WAIT     : 0          Current ESTABLISHED  : 0
    Maximum TIME-WAIT     : 1027       Maximum ESTABLISHED  : 1961
    Conns Allocated       : 1970288    Conns Deallocated    : 1970288
    Conn Deletes sent     : 3940576    Probe resets         : 0
 Timer related :
```

```
    RTT estimates          : 684903022  RTT est. updates     : 684060502
    delayed acks sent      : 1760943    FIN-WAIT2 timeouts   : 0
    Retransmit timeouts    : 1855840    Persist Timeouts     : 0
    SYN timeouts           : 141865     Idle Timeouts        : 0
    Reassembly timeouts    : 0
 Packet Transmit related :
    Total packets          : 2499818678 Data packets         : 2034445802
    Data bytes sent        : 2837513871 Retransmitted pkts   : 1283476
    Retransmitted bytes    : 311746077  Ack only pkts        : 5444907
    Window probes          : 0          URG only pkts        : 0
    Window Update pkts     : 452160292  Cntrl pkts (S/F/R)   : 6482745
    Tx TOS - normal        : 2499817222 Tx TOS - Min. Cost   : 0
    Tx TOS - max. rel.     : 0          Tx TOS - Max. thru.  : 0
    Tx TOS - min. delay    : 0          Tx TOS - invalid     : 0
 Packet Receive related :
    Total packets          : 2055992562 In seq data pkts     : 1365961238
    In seq data bytes      : 464953685  Bad Offset           : 0
    Too short              : 0          Dup-only data pkts   : 540520
    Dup-only data bytes    : 37642208   Part. dup. data pkts : 0
    Part. Dup. data bytes  : 0          OOO data pkts        : 0
    OOO data bytes rcvd    : 0          Pkts after rx win    : 0
    Bytes after rx window  : 0          Pkts after close     : 0
    Window Probes          : 0          Duplicate ACKs       : 1197303
    ACKs for unsent data   : 0          ACK-only pkts        : 690294070
    Bytes acked by acks    : 1974287219 Window Update pkts   : 0
    PAWS dropped pkts      : 0          Hdr pred. ACKs       : 664831275
    Hdr pred. data pkts    : 1360706633 TCB cache misses     : 1322565191
    3 dup-only pkts        : 35         Partial Acks         : 0
    Rx TOS - normal        : 2055337650 Rx TOS - Min. Cost   : 0
    Rx TOS - max. rel.     : 0          Rx TOS - Max. thru.  : 0
    Rx TOS - min. delay    : 0          Rx TOS - invalid     : 0
    Unrecognized Options   : 0          Unaligned MSS        : 0
    Unaligned Timestamp    : 0          Unaligned SACK       : 0
    RST ACK's sent         : 0

 Packet Drop statistics :
    Per-flow limit drops   : 0          Aggregate tail drops : 0
    Aggregate random drps  : 0          Egress Bufpool drops : 0

 Connection Drop/Close statistics :
    Active                 : 659122     Passive              : 656828
    App closed early       : 435        Client Reuse         : 0
    RST Rcvd               : 1169301    Unexp. Data Rcvd     : 0
    Server Reuse           : 0          App initiated abort  : 1313025
    Unexp. SYNs            : 0          Server Refused       : 0
    Other Drops            : 0          Conn Pool Fails      : 0
    Conn Bufpool Drops     : 0          Invalid MSS Drops    : 0
    User clear Drops       : 0          Conn Init Failures   : 0

 Debug Statistics :
    Unaccounted Buffers    : 0          Invalid Conns        : 0
    Output Failures        : 0          Header Bufpool Fails : 0
    MAC channel Fails      : 0          DM Channel Fails     : 0
    Invalid App Opcodes    : 0          MAC Bufpool Fails    : 0
    MAC BufDesc Fails      : 0          Recycle Conn Fails   : 0
    DM chan congested      : 0          MAC chan congested   : 0

ssl-proxy#
```

次に、PKI の統計情報を表示する例を示します。

```
ssl-proxy# show ssl-proxy stats pki
Authentication request timeout: 180 seconds
Max in process: 50 (requests)
```

```
Max queued before dropping: 500 (requests)
Certificate Authentication & Authorization Statistics:
  Requests started: 1
  Requests finished: 1
  Requests pending to be processed: 0
  Requests waiting for CRL: 0
  Signature only requests: 1
  Valid signature: 0
  Invalid signature: 0
  Total number of invalid certificates: 0
  Approved with warning (no crl check): 1
  Number of times polling CRL: 0
  No certificates present: 0
  Failed to get CRL: 0
  Not authorized (e.g. denied by ACL): 0
  Root certificates not self-signed: 0
  Verify requests failed (e.g. expired or CRL operation failed): 0
  Unknown failure: 0
  Empty certificate chain: 0
  No memory to process requests: 0
  DER encoded certificates missing: 0
  Bad DER certificate length: 0
  Failed to get key from certificate: 0
  Issuer CA not in trusted CA pool: 0
  Issuer CA certificates not valid yet: 0
  Expired issuer CA certificates: 0
  Peer certificates not valid yet: 0
  Expired peer certificates: 0
Peer certificate cache size: 0 (entries), aging timeout: 15 (minutes)
Peer certificate cache statistics:
  In use: 0 (entries)
  Cache hit: 0
  Cache miss: 0
  Cache allocated: 0
  Cache freed: 0
  Cache entries expired: 0
  Cache error: 0
  Cache full (wrapped around): 0
  No memory for caching: 0
Certificate Expiration Warning statistics:
  Proxy service certificates expiring: 0
  CA certificates expiring: 0
  CA pool certificates expiring: 0
  Proxy service certificates expiring SNMP traps sent: 0
Certificate headers statistics:
  Certificate headers formed: 1
  Errors in forming headers: 0
  Prefix error: 0
Key Certificate Table Current Usage (cannot be cleared):
  Total number of entries in table: 8192
  Entries in use: 6
  Free entries: 8186
  Complete service entries: 4
  Incomplete new/renew service entries: 0
  Retiring service entries: 0
  Obsolete service entries: 0
  Complete intermediate CA cert: 1
  Complete root CA cert: 1
  Obsolete intermediate CA cert: 0
  Obsolete root CA cert: 0
PKI Accumulative Counters (cannot be cleared):
  Proxy service trustpoint added: 4
  Proxy service trustpoint deleted: 0
  Proxy service trustpoint modified: 0
```

```
  Keypair added: 4
  Keypair deleted: 0
  Wrong key type: 0
  Service certificate added: 4
  Service certificate deleted: 0
  Service certificate rolled over: 0
  Service certificate completed: 4
  Intermediate CA certificate added: 1
  Intermediate CA certificate deleted: 0
  Root CA certificate added: 1
  Root CA certificate deleted: 0
  Certificate overwritten: 0
  No free table entries: 0
  Rollover failed: 0
Certificate History Statistics (cannot be cleared):
  History records written: 0
  History records deleted: 0
  History records malloc: 0
  History records free: 0
  History records errors: 0
  History records currently kept in memory: 0
  History records have been cleared: 0 times
PKI IPC Counters for normal priority messages:
  Request buffer sent: 3
  Request buffer received: 1
  Request duplicated: 0
  Request send failed: 0
  Response buffer sent: 0
  Response buffer received: 0
  Response timeout: 0
  Response failed: 0
  Response with error reported by SSL Processor: 0
  Response with no request: 0
  Response duplicated: 0
  Message type error: 0
  Message length error: 0
PKI IPC Counters for high priority messages:
  Request buffer sent: 18
  Request buffer received: 0
  Request duplicated: 0
  Request send failed: 0
  Response buffer sent: 0
  Response buffer received: 18
  Response timeout: 0
  Response failed: 0
  Response with error reported by SSL Processor: 0
  Response with no request: 0
  Response duplicated: 0
  Message type error: 0
  Message length error: 0
PKI Memory Usage Counters:
  Malloc count: 237
  Free count: 178
  Malloc failed: 0
  High Priority IPC:
  Ipc alloc count: 36
  Ipc free count: 54
  Ipc alloc failed: 0
  Normal Priority IPC:
  Ipc alloc count: 3
  Ipc free count: 1
  Ipc alloc failed: 0
ssl-proxy#
```

次に、FDU の統計情報を表示する例を示します。

```
ssl-proxy# show ssl-proxy stats fdu
FDU Statistics:
    IP Frag Drops       : 0             IP Version Drops    : 0
    IP Addr Discards    : 0             Serv_Id Drops       : 27
    Conn Id Drops       : 0             Bound Conn Drops    : 0
    Vlan Id Drops       : 0             TCP Checksum Drops  : 0
    Hash Full Drops     : 0             Hash Alloc Fails    : 0
    Flow Creates        : 3940576       Flow Deletes        : 3940576
    Conn Id allocs      : 1970288       Conn Id deallocs    : 1970288
    Tagged Pkts Drops   : 0             Non-Tagg Pkts Drops : 0
    Add ipcs            : 3             Delete ipcs         : 0
    Disable ipcs        : 0             Enable ipcs         : 0
    Unsolicited ipcs    : 0             Duplicate Add ipcs  : 0
    IOS Broadcast Pkts  : 83551         IOS Unicast Pkts    : 1562
    IOS Multicast Pkts  : 0             IOS Total Pkts      : 85113
    IOS Congest Drops   : 0             SYN Discards        : 0
    TCP 5-tuple reuse   : 0


FDU Debug Counters:
    Inv. Conn Drops     : 0             Inv. Conn Pkt Drops : 0
    Inv. TCP opcodes    : 0

ssl-proxy#
```

次の例では、すべての HTTP ヘッダー挿入の統計情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy stats hdr
Header Insert Statistics:
    Session Headers Inserted : 0          Custom Headers Inserted : 1826046
    Session Id's Inserted    : 1826046    Client Cert. Inserted   : 1
    Client IP/Port Inserted  : 0          Req. boundry found      : 1826046
    Content Length Headers   : 0          Chunked Headers         : 0
    Content Length Splt Bufs : 0          Content Length Read Errs: 0
    Buffers allocated        : 0          Buffers Scanned         : 1826049
    Insertion Points Found   : 1826046    Header Overflow         : 3
    End of Header Found      : 1826046    Buffers Accumulated     : 1826049
    Multi-buffer IP Port     : 0          Multi-buffer Session Id : 0
    Multi-buffer Session Hdr : 0          Multi-buffer Custom Hdr : 0
    HTTP Struct Allocs       : 1826046    HTTP Struct Frees       : 1826046
    No End of Hdr Detected   : 0          Payload no HTTP header  : 0
    Desc Alloc Failed        : 0          Buffer Alloc Failed     : 0
    Client Cert Errors       : 1826045    Malloc failed           : 0
    Service Errors           : 0          Conn Entry Invalid      : 0
    Scan Internal Error      : 0          Database Not Initialized: 0
    Unsupported headers      : 0          Chunk Parse Errors      : 0
    Http headers removed     : 0          Http header removal errs: 0
```

次の例では、URL 書き換えの統計情報を表示する方法を示します。

```
ssl-proxy# show ssl-proxy stats url
ssl-proxy#show ssl-pro stats url
URL Rewrite Statistics:
    Rewrites Succeeded   : 0          Rewrites Failed      : 0
    Rsp Scan Incomplete  : 0          URL Scan Incomplete  : 0
    Invalid Conn Entry   : 0          URL Mismatch         : 0
    URL Object Error     : 0          Dbase not initialized: 0
    Scan Internal Error  : 0          Scan Dbase not Init. : 0
    Slash Delim not found: 0
```

次に、コンテンツの統計情報を表示する例を示します。

```
ssl-proxy# show ssl-proxy stats content
```

```
Scan object statistics in CPU: SSL1
    Objects in use       : 0
    Obj alloc failures   : 0
    Max obj in use       : 5
```

show ssl-proxy status

SSL サービス モジュールのプロキシ ステータスについての情報を表示するには、**show ssl-proxy status** コマンドを使用します。

show ssl-proxy status

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 1.2(1)	**show ssl-proxy status** コマンドの出力が、1 秒、1 分、5 分のあたりの CPU 使用率のトラフィック レートで表示される統計情報を含めるように変更されました。

例

次の例では、SSL サービス モジュールのステータスを表示する方法を示します。

```
ssl-proxy# show ssl-proxy status
FDU cpu is alive!
FDU cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0x4D52D1B7         int cycles  : 0x6B6C9937
    total cycles: 0xB954D5BEB6FA
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0


TCP cpu is alive!
TCP cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0xA973D74D         int cycles  : 0xAA03E1D89A
    total cycles: 0xB958C8FF0E73
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0
```

```
SSL cpu is alive!
SSL cpu utilization:
    % process util   : 0             % interrupt util : 0

    proc cycles : 0xD475444          int cycles  : 0x21865088E
    total cycles: 0xB958CCEB8059
    % process util (5 sec)   : 0             % interrupt util (5 sec) : 0

    % process util (1 min)  : 0             % interrupt util (1 min): 0
    % process util (5 min)  : 0             % interrupt util (5 min) : 0
```

show ssl-proxy version

現在のイメージ バージョンを表示するには、**show ssl-proxy version** コマンドを使用します。

show ssl-proxy version

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SSL サービス モジュールで現在実行しているイメージ バージョンを表示する方法を示します。

```
ssl-proxy# show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SSL(0.19)  INTERIM TEST
SOFTWARE
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 10-Apr-03 03:03 by integ
Image text-base: 0x00400078, data-base: 0x00ABE000

ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE

ssl-proxy uptime is 3 days, 22 hours, 22 minutes
System returned to ROM by power-on
System image file is "tftp://10.1.1.1/unknown"
AP Version 1.2(1)

ssl-proxy#
```

show ssl-proxy vlan

VLAN 情報を表示するには、**show ssl-proxy vlan** コマンドを使用します。

show ssl-proxy vlan [*vlan-id* | **debug**]

構文の説明

vlan-id	（任意）VLAN ID です。特定の VLAN の情報を表示します。有効な値は 1 ～ 1005 です。
debug	（任意）デバッグ情報を表示します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SSL サービス モジュールで設定されるすべての VLAN を表示する方法を示します。

```
ssl-proxy# show ssl-proxy vlan
VLAN index 2 (admin VLAN)
   IP addr 10.1.1.1 NetMask 255.0.0.0 Gateway 10.1.1.5
   Network 10.1.1.2 Mask 255.0.0.0 Gateway 10.1.1.6
VLAN index 3
   IP addr 10.1.1.3 NetMask 255.0.0.0 Gateway 10.1.1.6
VLAN index 6
   IP addr 10.1.1.4 NetMask 255.0.0.0

ssl-proxy#
```

関連コマンド

ssl-proxy vlan

snmp-server enable

SNMP トラップおよび通知を設定するには、**snmp-server enable** コマンドを使用します。SNMP トラップおよび通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

no snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | {**ssl-proxy** [**cert-expiring**] [**oper-status**]}}}

構文の説明

informs	SNMP 通知をイネーブルにします。
traps	SNMP トラップをイネーブルにします。
ipsec	IPSec トラップをイネーブルにします。
isakmp	ISAKMP トラップをイネーブルにします。
snmp	SNMP トラップをイネーブルにします。
ssl-proxy	SNMP SSL プロキシ通知トラップをイネーブルにします。
cert-expiring	（任意）SSL プロキシ証明書の期限切れ通知トラップをイネーブルにします。
oper-status	（任意）SSL プロキシ証明書の動作ステータス通知トラップをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、SNMP 通知をイネーブルにする方法を示します。

```
ssl-proxy (config)# snmp-server enable informs
ssl-proxy (config)#
```

次の例では、SSL プロキシ トラップをイネーブルにする方法を示します。

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy
ssl-proxy (config)#
```

次の例では、SSL プロキシ通知トラップをイネーブルにする方法を示します。

```
ssl-proxy (config)# snmp-server enable traps ssl-proxy cert-expiring oper-status
ssl-proxy (config)#
```

ssl-proxy crypto selftest

暗号形式セルフテストを開始するには、**ssl-proxy crypto selftest** コマンドを使用します。テストをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssl-proxy crypto selftest [**time-interval** *seconds*]

no ssl-proxy crypto selftest

構文の説明

time-interval *seconds*	（任意）テスト ケースの間隔を設定します。有効な値は 1 ～ 8 秒です。

デフォルト

3 秒

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

ssl-proxy crypto selftest コマンドでは、バックグラウンドの SSL プロセッサ上で実行するクリプト アルゴリズム テストのセットをイネーブルにします。乱数生成、ハッシュ、暗号化および復号化、および MAC 生成が、テスト ケースの間隔でテストされます。

このテストは、トラブルシューティングの目的のみで実行します。このテストを実行すると、実行時のパフォーマンスに影響します。

セルフテストの結果を表示するには、**show ssl-proxy stats crypto** コマンドを入力します。

例

次の例では、暗号形式セルフテストを開始する方法を示します。

```
ssl-proxy (config)# ssl-proxy crypto selftest
ssl-proxy (config)#
```

ssl-proxy device-check

クリプト デバイスのヘルスを確認するには、**ssl-proxy device-check** コマンドを使用します。

ssl-proxy device-check interval *milliseconds* **reset-limit** *number*

構文の説明

interval *milliseconds*	デバイス チェックの間隔（ミリ秒単位）。指定できる範囲は 10 ～ 60000 です。 0 の場合、デバイス チェックがディセーブルになります。
reset-limit *number*	再起動の前にリセットが繰り返される回数。指定できる範囲は 0 ～ 60 です。 0 の場合、無制限です。

デフォルト

デバイス チェックがディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(13)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

このコマンドは通常、ディセーブルになっています（デバイス チェックの間隔は 0）。このコマンドがイネーブルの場合、SSLM は各間隔でクリプト デバイスが正常に動作しているかどうかをチェックします。要求間隔よりも古い未処理の要求がある場合、クリプト デバイスがリセットされ、動作ステータスに戻ります。リセットの制限も設定できます。リセットの制限がデフォルト（0）に設定されている場合、制限はありません。リセットの制限が 0 以外に設定されている場合、繰り返されるポール間隔のリセットの制限回数より多くデバイスがリセットされると、SSLM が再起動されます。

例

次の例では、デバイス チェックの間隔を 20 ミリ秒に設定し、リセットの制限を 0 回に設定する方法を示します。

```
ssl-proxy (config)# ssl-proxy device-check interval 20 reset-limit 0
```

ssl-proxy mac address

MAC アドレスを設定するには、**ssl-proxy mac address** コマンドを使用します。

ssl-proxy mac address *mac-addr*

構文の説明

mac-addr	MAC アドレスの詳細については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

MAC アドレスを H.H.H の形式で入力します。

例

次に、MAC アドレスを設定する例を示します。

```
ssl-proxy (config)# ssl-proxy mac address 00e0.b0ff.f232
ssl-proxy (config)#
```

関連コマンド

show ssl-proxy mac address

ssl-proxy natpool

SSL サービス モジュールでクライアント NAT の実装に使用する IP アドレスのプールを定義するには、**ssl-proxy natpool** コマンドを使用します。

ssl-proxy natpool *nat-pool-name start-ip-addr* {**netmask** *netmask*}

構文の説明

nat-pool-name	NAT プール名。
start-ip-addr	プールの最初の IP アドレスを指定します。
netmask *netmask*	ネットマスクの詳細については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、IP アドレスのプールを定義する方法を示します。

```
ssl-proxy (config)# ssl-proxy natpool NP2 207.59.10.01 207.59.10.08 netmask 255.0.0.0
ssl-proxy (config)#
```

関連コマンド

show ssl-proxy natpool

ssl-proxy pki

SSL サービス モジュールで PKI 実装を設定および定義するには、**ssl-proxy pki** コマンドを使用します。ロギングをディセーブルにしてメモリをクリアするには、このコマンドの **no** 形式を使用します。

ssl-proxy pki {{**authenticate** {**timeout** *seconds*}} | {**cache** {{**size** *entries*} | {**timeout** *minutes*}}} | {**certificate** {**check-expiring** {**interval** *hours*}}} | **history**}

no ssl-proxy pki {**authenticate** | **cache** | **certificate** | **history**}

構文の説明

authenticate	証明書の認証および許可を設定します。
timeout *seconds*	各要求のタイムアウトを秒単位で指定します。有効な値は 1 ～ 600 秒です。
cache	ピア証明書キャッシュを設定します。
size *entries*	キャッシュ エントリの最大数を指定します。有効な値は 0 ～ 5000 エントリです。
timeout *minutes*	エントリのエージング タイムアウト値を指定します。有効な値は 1 ～ 600 秒です。
certificate	チェックの期限切れ間隔を設定します。
check-expiring interval *hours*	チェックの期限切れ間隔を指定します。有効な値は 0 ～ 720 時間です。
history	キーと証明書の履歴。

デフォルト

デフォルト設定は次のとおりです。

- **timeout** *seconds*：**180** 秒
- **size** *entries*：**0** エントリ
- **timeout** *minutes*：**15** 分
- **interval** *hours*：**0** 時間。チェックしない

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 2.1(1)	このコマンドは、次のキーワードを追加するように変更されました。 • **authenticate** • **cache** • **certificate**

使用上のガイドライン

ssl-proxy pki history コマンドでは、プロキシ サービスごとに証明書の履歴レコードのメモリへのロギングをイネーブルにして、レコードごとに Syslog メッセージを生成します。各レコードは、キー ペアまたは証明書のプロキシ サービス キーおよび証明書テーブルへの追加または削除を追跡します。

テーブルのインデックスが変更されると、このコマンドによって次の情報が記録されます。

- キー ペア名
- トラストポイント ラベル
- サービス名
- 件名
- 証明書のシリアル番号

一度に最大 512 個のレコードをメモリに保存できます。

例

次の例では、各要求のタイムアウトを秒単位で指定する方法を示します。

```
ssl-proxy (config)# ssl-proxy pki authenticate timeout 200
ssl-proxy (config)#
```

次の例では、キャッシュ サイズを指定する方法を示します。

```
ssl-proxy (config)# ssl-proxy pki cache size 50
ssl-proxy (config)#
```

次の例では、エントリのエージング タイムアウト値を指定する方法を示します。

```
ssl-proxy (config)# ssl-proxy pki cache timeout 20
ssl-proxy (config)#
```

次の例では、チェックの期限切れ間隔を指定する方法を示します。

```
ssl-proxy (config)# ssl-proxy pki certificate check-expiring interval 100
ssl-proxy (config)#
```

次の例では、PKI イベントの履歴をイネーブルにする方法を示します。

```
ssl-proxy (config)# ssl-proxy pki history
ssl-proxy (config)#
```

関連コマンド

show ssl-proxy stats

ssl-proxy policy http-header

HTTP ヘッダー挿入コンフィギュレーション サブモードを開始するには、**ssl-proxy policy http-header** コマンドを使用します。

ssl-proxy policy http-header *http-header-policy-name*

構文の説明

http-header-policy-name	HTTP ヘッダー ポリシー名。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

HTTP ヘッダー挿入コンフィギュレーション サブモードでは、ペイロードに適用できる HTTP ヘッダー挿入コンテンツ ポリシーを定義できます。

HTTP ヘッダー挿入では、追加 HTTP ヘッダーを挿入して、実際のサーバに対して接続が実際に SSL 接続であることを示すことができます。このようなヘッダーでは、サーバ アプリケーションで各 SSL セッション / クライアントの正しい情報を収集できます。

次のヘッダー タイプを挿入できます。

- クライアント証明書：クライアント証明書ヘッダー挿入では、バックエンド サーバで、SSL モジュールが認証および承認したクライアント証明書の属性を表示できます。**client-cert** を指定すると、SSL モジュールが次のヘッダーをバックエンド サーバに渡します。
  - クライアント IP およびポート アドレス：Network Address Translation（NAT; ネットワーク アドレス変換）では、クライアント IP アドレスおよびポートの情報が削除されます。**client-ip-port** を指定すると、SSL モジュールにクライアント IP アドレスおよびクライアント ポートについての情報が HTTP ヘッダーに挿入され、サーバでクライアント IP アドレスおよびポートが表示されます。
  - カスタム：**custom** *custom-string* を指定すると、SSL モジュールでユーザ定義のヘッダーが HTTP ヘッダーに挿入されます。
  - プレフィクス：**prefix** *prefix-string* を指定すると、SSL モジュールで指定されたプレフィクスが HTTP ヘッダーに追加され、接続が他のアプライアンスではなく、SSL モジュールから確立されたことをサーバで識別できます。
- SSL セッション：セッション ID を含むセッション ヘッダーが、セッション ID に基づいてクライアント証明書をキャッシュするために使用されます。また、サーバで特定の暗号スイートに基づく接続を追跡する場合、セッション ヘッダーもセッションごとにキャッシュされます。**session** を指定すると、SSL モジュールは SSL 接続に固有の情報をセッション ヘッダーとしてバックエンド サーバに渡します。

表 2-2 に、HTTP ヘッダー挿入コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-2　HTTP ヘッダー挿入コンフィギュレーション サブモード コマンドの説明

client-cert	バックエンド サーバで、SSL モジュールが認証および承認したクライアント証明書の属性を表示できます。
client-ip-port	クライアント IP アドレスおよびクライアント ポートについての情報が HTTP ヘッダーに挿入され、サーバでクライアント IP アドレスおよびポートが表示されます。
custom *custom-string*	*custom-string* ヘッダーを HTTP ヘッダーに挿入します。*custom-string* の最大長は 239 文字です。この長さを超えると、「Incomplete command」エラーが表示されます。文字列にスペースが含まれる場合、引用符（""）で囲む必要があります。
prefix	*prefix-string* を HTTP ヘッダーに追加すると、サーバで他のアプライアンスではなく、SSL モジュールから確立された接続を識別できます。
session	SSL 接続に固有の情報をヘッダーとしてバックエンド サーバに渡します。

例

次の例では、すべての HTTP ヘッダー挿入コンフィギュレーション サブモードを開始する方法を示します。

```
ssl-proxy (config)# ssl-proxy policy http-header test1
ssl-proxy (config-http-header-policy)#
```

次の例では、バックエンド サーバで、SSL モジュールが認証および承認したクライアント証明書の属性を表示できるようにする方法を示します。

```
ssl-proxy (config-http-header-policy)# client-cert
ssl-proxy (config-http-header-policy)#
```

次の例では、クライアント IP アドレスおよびクライアント ポートについての情報を HTTP ヘッダーに挿入され、サーバでクライアント IP アドレスおよびポートを表示する方法を示します。

```
ssl-proxy (config-http-header-policy)# client-ip-cert
ssl-proxy (config-http-header-policy)#
```

次の例では、custom-string ヘッダーを HTTP ヘッダーに挿入する方法を示します。

```
ssl-proxy (config-http-header-policy)# custom SSL-Frontend:Enable
ssl-proxy (config-http-header-policy)#
```

次の例では、prefix-string を HTTP ヘッダーに追加する方法を示します。

```
ssl-proxy (config-http-header-policy)# prefix
ssl-proxy (config-http-header-policy)#
```

次の例では、SSL 接続に固有の情報をヘッダーとしてバックエンド サーバに渡す方法を示します。

```
ssl-proxy (config-http-header-policy)# session
ssl-proxy (config-http-header-policy)#
```

関連コマンド

show ssl-proxy policy

ssl-proxy policy ssl

SSL ポリシー コンフィギュレーション サブモードを開始するには、**ssl-proxy policy ssl** コマンドを使用します。SSL ポリシー コンフィギュレーション サブモードでは、1 つまたは複数の SSL ポリシー サービスの SSL ポリシーを定義できます。

ssl-proxy policy ssl *ssl-policy-name*

構文の説明

ssl-policy-name	SSL ポリシー名。

デフォルト

デフォルトの設定は次のとおりです。

- **cipher** はすべてです。
- **close-protocol** はイネーブルになっています。
- **session-caching** はイネーブルになっています。
- **version** はすべてです。
- **session-cache size** *size* は 262143 エントリです。
- **timeout session** *timeout* は 0 秒です。
- **timeout handshake** *timeout* は 0 秒です。
- **cert-req empty** はディセーブルになっています。
- **tls-rollback** はディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 1.2(1)	このコマンドは、次のサブコマンドを追加するように変更されました。 • **session-cache size** *size* • **timeout session** *timeout* [**absolute**]
SSL Services Module Release 2.1(5)	このコマンドは、次のサブコマンドを追加するように変更されました。 • **cert-req empty** • **tls-rollback** [**current** | **any**]

使用上のガイドライン

各 SSL ポリシー コンフィギュレーション サブモード コマンドがそれぞれの行で入力されます。

表 2-3 に、SSL ポリシー コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-3　SSL ポリシー コンフィギュレーション サブモード コマンドの説明

cert-req empty	SSL サービス モジュール バックエンド サービスで常にトラストポイントに関連する証明書を返し、一致する CA 名を検索しないように指定できます。
cipher-suite {**RSA_WITH_3DES_EDE_CBC_SHA** | **RSA_WITH_DES_CBC_SHA** | **RSA_WITH_RC4_128_MD5** | **RSA_WITH_RC4_128_SHA** | **all**}	プロキシ サーバで許容される暗号スイートのリストを設定できます。暗号スイートの詳細については、「使用上のガイドライン」を参照してください。
[**no**] **close-protocol enable**	SSL クローズプロトコルの動作を設定できます。クローズ プロトコルをディセーブルにするには、このコマンドの **no** 形式を使用します。
default {**cipher** | **close-protocol** | **session-cache** | **version**}	コマンドをデフォルトに設定します。
exit	SSL ポリシー コンフィギュレーション サブモードを終了します。
help	対話型ヘルプ システムの説明を表示します。
[**no**] **session-cache enable**	セッション キャッシュ機能をイネーブルにできます。セッション キャッシュをディセーブルにするには、このコマンドの **no** 形式を使用します。
session-cache size *size*	任意のサービスに割り当てられるセッション エントリの最大数を指定します。有効な値は 1 ～ 262143 エントリです。
timeout handshake *timeout*	モジュールのハンドシェイク段階で接続を維持する長さを設定できます。有効な値は 0 ～ 65535 秒です。
timeout session *timeout* [**absolute**]	セッション タイムアウトを設定できます。次に、構文を説明します。 • *timeout*：セッションのタイムアウト。有効な値は 0 ～ 72000 秒です。 • **absolute :**（任意）設定されたタイムアウトに達するまで、セッション エントリが削除されません。
tls-rollback [**current** | **any**]	TLS/SSL パラメータの秘密メッセージ内の SSL プロトコル バージョン番号を最上位バージョンにするかネゴシエートされたバージョン（**current**）にするか、またはバージョンのチェックなしにするか（**any**）を指定できます。
version {**all** | **ssl3** | **tls1**}	SSL のバージョンを次のいずれかに設定できます。 • **all**：SSL3 と TLS1 の両方のバージョンが使用されます。 • **ssl3**：SSL バージョン 3 が使用されます。 • **tls1**：TLS バージョン 1 が使用されます。

ssl-proxy policy ssl *ssl-policy-name* コマンドを使用して SSL ポリシー テンプレートを定義し、プロキシ サーバ コンフィギュレーション CLI を使用して SSL ポリシーを特定のプロキシ サーバに関連付けることができます。SSL ポリシー テンプレートでは、SSL ハンドシェイク スタックに関連付けられるさまざまなパラメータを定義できます。

close-notify をイネーブルにすると、終了通知アラート メッセージがクライアントに送信され、クライアントからの終了通知アラート メッセージも予測されます。ディセーブルになっている場合、サーバは終了通知アラート メッセージをクライアントに送信します。ただし、サーバはセッションをティアダウンするまで、クライアントからの終了通知メッセージを予測したり待機したりしません。

暗号スイート名は既存の SSL スタックと同じ規則に従います。

プロキシ サーバで許容される暗号スイートは次のとおりです。

- RSA_WITH_3DES_EDE_CBC_SHA：3des-sha 付きの RSA
- RSA_WITH_DES_CBC_SHA：des-sha 付きの RSA
- RSA_WITH_RC4_128_MD5：rc4-md5 付きの RSA
- RSA_WITH_RC4_128_SHA：rc4-sha 付きの RSA
- all：すべての暗号がサポートされます

timeout session *timeout* **absolute** コマンドを入力すると、セッション エントリはクリーンアップされるまで、設定されたタイムアウトのセッション キャッシュで保存されます。セッション キャッシュがいっぱいの場合、すべてのエントリに対してタイマーがアクティブになり、**absolute** キーワードが設定され、それ以降のすべての新しいセッションが拒否されます。

timeout session *timeout* コマンドを **absolute** キーワードなしで入力した場合、指定されたタイムアウトが最大タイムアウトとして扱われ、可能な限りセッション エントリがセッション キャッシュで保存されます。セッション キャッシュでセッション エントリの空きがなくなった場合、現在使用されているセッション エントリが新しい接続から削除されます。

cert-req empty コマンドを入力すると、SSL サービス モジュール バックエンド サービスが常にトラストポイントに関連付けられた証明書を返し、一致する CA 名を検索しません。デフォルトでは、SSL サービス モジュール は証明書を返すまで、一致する CA 名を検索します。SSL サーバがクライアント認証中に証明書要求に CA 名リストを含めない場合、証明書要求が失敗します。

デフォルトでは、SSL サービス モジュール ClientHello メッセージでサポートされる最大の SSL プロトコル バージョン（SSL2.0、SSL3.0、TLS1.0）を使用します。SSL クライアントが（ClientHello メッセージで指定されている）サポートされている最上位バージョンの代わりに、ネゴシエートされたバージョンを使用する場合、**tls-rollback** [**current** | **any**] コマンドを入力します。

tls-rollback current コマンドを入力すると、SSL プロトコル バージョンはサポートされている最上位バージョンまたはネゴシエートされたバージョンにすることができます。

tls-rollback any コマンドを入力した場合、SSL プロトコル バージョンはチェックされません。

例

次に、SSL ポリシー コンフィギュレーション サブモードを開始する例を示します。

```
ssl-proxy (config)# ssl-proxy policy ssl sslpl1
ssl-proxy (config-ssl-policy)#
```

次の例では、SSL ポリシー でサポートされる暗号スイートを定義する方法を示します。

```
ssl-proxy (config-ssl-policy)# cipher RSA_WITH_3DES_EDE_CBC_SHA
ssl-proxy (config-ssl-policy)#
```

次の例では、SSL セッション終了プロトコルをイネーブルにする方法を示します。

```
ssl-proxy (config-ssl-policy)# close-protocol enable
ssl-proxy (config-ssl-policy)#
```

次の例では、SSL セッション終了プロトコルをディセーブルにする方法を示します。

```
ssl-proxy (config-ssl-policy)# no close-protocol enable
ssl-proxy (config-ssl-policy)#
```

次の例では、特定のコマンドをデフォルトに設定する方法を示します。

```
ssl-proxy (config-ssl-policy)# default cipher
ssl-proxy (config-ssl-policy)# default close-protocol
ssl-proxy (config-ssl-policy)# default session-cache
ssl-proxy (config-ssl-policy)# default version
ssl-proxy (config-ssl-policy)#
```

次の例では、セッション キャッシュをイネーブルにする方法を示します。

```
ssl-proxy (config-ssl-policy)# session-cache enable
ssl-proxy (config-ssl-policy)#
```

次の例では、セッション キャッシュをディセーブルにする方法を示します。

```
ssl-proxy (config-ssl-policy)# no session-cache enable
ssl-proxy (config-ssl-policy)#
```

次の例では、指定されたサービスに割り当てられるセッション エントリの最大数を設定する方法を示します。

```
ssl-proxy (config-ssl-policy)# session-cache size 22000
ssl-proxy (config-ssl-policy)#
```

次の例では、セッション タイムアウトを絶対値に設定する方法を示します。

```
ssl-proxy (config-ssl-policy)# timeout session 30000 absolute
ssl-proxy (config-ssl-policy)#
```

次の例では、複数の SSL バージョンのサポートをイネーブルにする方法を示します。

```
ssl-proxy (config-ssl-policy)# version all
ssl-proxy (config-ssl-policy)# version ssl3
ssl-proxy (config-ssl-policy)# version tls1
ssl-proxy (config-ssl-policy)#
```

次の例では、ヘルプ ページを出力する方法を示します。

```
ssl-proxy (config-ssl-policy)# help
ssl-proxy (config-ssl-policy)#
```

関連コマンド

show ssl-proxy stats
show ssl-proxy stats ssl

ssl-proxy policy tcp

プロキシ ポリシー TCP コンフィギュレーション サブモードを開始するには、ssl-proxy policy tcp コマンドを使用します。プロキシ ポリシー TCP コンフィギュレーション サブモードでは、TCP ポリシー テンプレートを定義できます。

ssl-proxy policy tcp *tcp-policy-name*

構文の説明

tcp-policy-name	TCP ポリシー名。

デフォルト

デフォルトの設定は次のとおりです。

- **timeout inactivity** は 600 秒です。
- **timeout fin-wait** は 600 秒です。
- **buffer-share rx** は 32768 バイトです。
- **buffer-share tx** は 32768 バイトです。
- **mss** は 1500 バイトです。
- **timeout syn** は 75 秒です。
- **timeout reassembly** は 60 秒です。
- **tos carryover** はディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 1.2(1)	このコマンドは、**timeout reassembly** *time* サブコマンドを追加するために変更されました。
SSL Services Module Release 2.1(4)	このコマンドは、**tos carryover** サブコマンドを追加するために変更されました。

使用上のガイドライン

TCP ポリシーを定義すると、プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドを使用して、TCP ポリシーをサーバに関連付けることができます。

プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドがそれぞれの行で入力されます。

表 2-4 に、プロキシ ポリシー TCP コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-4　プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドの説明

default	コマンドをデフォルトに設定します。
exit	プロキシ サービス コンフィギュレーション サブモードを終了します。
[**no**] **timeout fin-wait** *timeout-in-seconds*	FIN の待機タイムアウトを設定できます。有効な値は 75 ～ 600 秒です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
help	対話型ヘルプ システムの説明を表示します。
[**no**] **timeout inactivity** *timeout-in-seconds*	非アクティブ タイムアウトを設定できます。有効な値は 0 ～ 960 秒です。このコマンドでは、アイドル状態の接続のエージング タイムアウトを設定でき、接続リソースの保護に役立ちます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
[**no**] **buffer-share rx** *buffer-limit-in-bytes*	接続ごとの受信バッファ共有の最大サイズを設定できます。有効な値は 8192 ～ 262144 です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。 **（注）** サイズの大きい暗号化されたファイルがモジュールによって転送される場合、受信バッファ サイズは、SSL レコードの再アセンブリのために、最大 SSL レコード サイズの 16384 バイト以上にする必要があります。最適なパフォーマンスのために、受信バッファ サイズを 20000 バイト以上にすることを推奨します。
[**no**] **buffer-share tx** *buffer-limit-in-bytes*	接続ごとの伝送バッファ共有の最大サイズを設定できます。有効な値は 8192 ～ 262144 です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。 **（注）** サイズの大きい暗号化されたファイルがモジュールによって転送される場合、伝送バッファ サイズは、SSL レコードの再アセンブリのために、最大 SSL レコード サイズの 16384 バイト以上にする必要があります。最適なパフォーマンスのために、伝送バッファ サイズを 20000 バイト以上にすることを推奨します。
[**no**] **mss** *max-segment-size-in-bytes*	接続で識別する生成された SYN パケットの最大セグメント サイズを設定できます。有効な値は 64 ～ 1460 です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
[**no**] **timeout syn** *timeout-in-seconds*	接続の確立タイムアウトを設定できます。有効な値は 5 ～ 75 秒です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

表 2-4　プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドの説明 （続き）

[**no**] **timeout reassembly** *time*	リアセンブリ キューがクリアされるまでの時間を秒単位で設定できます。有効な値は 0 ～ 960 秒です（0 の場合、ディセーブル）。トランザクションが指定された時間内に完了しなかった場合、リアセンブリ キューがクリアされ、接続がドロップされます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
[**no**] **tos carryover**	タイプ オブ サービス（ToS）値をフロー内のすべてのパケットに転送します。 **（注）** ポリシーがサーバ TCP ポリシーとして設定される場合、ToS 値がサーバからクライアントへ送信されます。ポリシーが仮想ポリシーとして設定される場合、ToS 値がクライアントからサーバへ送信されます。 **（注）** ToS 値を伝播できるようにするには、その値を学習する必要があります。たとえば、ToS 値がサーバからクライアントへの接続で伝播するように設定されている場合、その値を学習して伝播する前にサーバ接続を確立する必要があります。したがって、一部の初期パケットは ToS 値を伝送しません。

使用上のガイドライン

SSL サービス モジュールで入力した TCP コマンドは、グローバルに、または特定のプロキシ サーバに適用できます。

プロキシ サーバのクライアント側とサーバ側の最大セグメント サイズには、異なるサイズを設定できます。

TCP ポリシー テンプレートでは、TCP スタックに関連付けられるパラメータを定義できます。

コマンドの **no** 形式を入力するか、または **default** キーワードを使用してデフォルト設定に戻します。

例

次に、プロキシ ポリシー TCP コンフィギュレーション サブモードを開始する例を示します。

```
ssl-proxy (config)# ssl-proxy policy tcp tcppl1
ssl-proxy (config-tcp-policy)#
```

次の例では、特定のコマンドをデフォルト値に設定する方法を示します。

```
ssl-proxy (config-tcp-policy)# default timeout fin-wait
ssl-proxy (config-tcp-policy)# default inactivity-timeout
ssl-proxy (config-tcp-policy)# default buffer-share rx
ssl-proxy (config-tcp-policy)# default buffer-share tx
ssl-proxy (config-tcp-policy)# default mss
ssl-proxy (config-tcp-policy)# default timeout syn
ssl-proxy (config-tcp-policy)#
```

次の例では、FIN 待機タイムアウトを秒単位で定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# timeout fin-wait 200
ssl-proxy (config-tcp-policy)#
```

次の例では、非アクティブ タイムアウトを秒単位で定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# timeout inactivity 300
ssl-proxy (config-tcp-policy)#
```

次の例では、受信バッファ設定の最大サイズを定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# buffer-share rx 16384
ssl-proxy (config-tcp-policy)#
```

次の例では、伝送バッファ設定の最大サイズを定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# buffer-share tx 13444
ssl-proxy (config-tcp-policy)#
```

次の例では、TCP セグメントの最大サイズを定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# mss 1460
ssl-proxy (config-tcp-policy)#
```

次の例では、初期接続（SYN）タイムアウト値を定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# timeout syn 5
ssl-proxy (config-tcp-policy)#
```

次の例では、リアセンブリ タイムアウト値を定義する方法を示します。

```
ssl-proxy (config-tcp-policy)# timeout reassembly 120
ssl-proxy (config-tcp-policy)#
```

次の例では、ToS 値をフロー内のすべてのパケットへの伝送をイネーブルにします。

```
ssl-proxy (config-tcp-policy)# tos carryover
ssl-proxy (config-tcp-policy)#
```

関連コマンド

show ssl-proxy policy

ssl-proxy policy url-rewrite

URL 書き換えコンフィギュレーション サブモードを開始するには、**ssl-proxy policy url-rewrite** コマンドを使用します。URL 書き換えコンフィギュレーション サブモードでは、ペイロードに適用される URL 書き換えコンテンツ ポリシーを定義できます。

ssl-proxy policy url-rewrite *url-rewrite-policy-name*

構文の説明

url-rewrite-policy-name	URL 書き換えポリシー名。

デフォルト

このコマンドには、引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

URL 書き換えでは、リダイレクト リンクのみを書き換えできます。

URL 書き換えポリシーは、SSL ポリシー サービスごとに最大 32 個の書き換えルールで構成されます。

表 2-5 に、プロキシ ポリシー コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-5　プロキシ ポリシー コンフィギュレーション サブモード コマンドの説明

default	コマンドをデフォルトに設定します。
exit	プロキシ ポリシー コンフィギュレーション サブモードを終了します。
help	対話型ヘルプ システムの説明を表示します。
[**no**] **url** *url-string*[**clearport** *port-number* | **sslport** *port-number*]	書き換える URL ストリングを設定できます。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

url-string：書き換える URL リンクの host 部分を指定します。最大 251 文字まで指定できます。ワイルドカード「*」は、書き換えルールの *hostname* のプレフィクスまたはサフィクスとしてのみ使用できます。たとえば、次のいずれかの方法で *hostname* を使用できます。

- www.cisco.com
- *.cisco.com
- wwwin.cisco.*

clearport *port-number*：（任意）書き換える URL リンクの port 部分を指定します。有効な値は 1 ～ 65535 です。

sslport *port-number*：（任意）書き込む URL リンクの *port* 部分を指定します。有効な値は 1 ～ 65535 です。

このコマンドの **no** 形式を入力して、ポリシーを削除します。

（注） サーバに URL リダイレクトのデフォルト HTTP ポート番号 80 が含まれる場合（たとえば、www.example.com:80）、同様に **url** コマンドを設定する必要があります（たとえば、**url www.example.com:80**）。標準以外のポート番号を URL の一部として設定する必要はありませんが、代わりに **clearport** キーワードを使用して設定することはできます。

例

次の例では、test1 ポリシーの URL 書き換えコンフィギュレーション サブモードを開始する方法を示します。

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy#
```

次の例では、test1 ポリシーの URL 書き換えポリシーを定義する方法を示します。

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# url www.cisco.com clearport 80 sslport 443
ssl-proxy(config-url-rewrite-policy#
```

次の例では、test1 ポリシーの URL 書き換えポリシーを削除する方法を示します。

```
ssl-proxy (config)# ssl-proxy policy url-rewrite test1
ssl-proxy(config-url-rewrite-policy# no url www.cisco.com clearport 80 sslport 443
ssl-proxy(config-url-rewrite-policy#
```

関連コマンド

show ssl-proxy policy

ssl-proxy pool ca

認証局プール コンフィギュレーション サブモードを開始するには、**ssl-proxy pool ca** コマンドを使用します。認証局プール コンフィギュレーション サブモードでは、モジュールが信頼できる CA を表示する認証局プールを設定できます。

ssl-proxy pool *ca-pool-name*

構文の説明

ca-pool-name	認証局プール名。

デフォルト

このコマンドには、引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

各認証局プール コンフィギュレーション サブモード コマンドをそれぞれの行で入力します。

表 2-6 に、認証局プール TCP コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-6　プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドの説明

ca	認証局を設定します。使用できるサブコマンドは次のとおりです。 **trustpoint** *ca-trustpoint-name*：認証局トラストポイントを設定します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
default	コマンドをデフォルトに設定します。
exit	プロキシ サービス コンフィギュレーション サブモードを終了します。
help	接続の確立タイムアウトを設定できます。有効な値は 5 ～ 75 秒です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

例

次の例では、認証局トラストポイントをプールに追加する方法を示します。

```
ssl-proxy (config)# ssl-proxy pool test1
ssl-proxy(config-ca-pool)# ca trustpoint test20
ssl-proxy(config-ca-pool)#
```

ssl-proxy service

プロキシ サービス コンフィギュレーション サブモードを開始するには、**ssl-proxy-service** コマンドを使用します。

ssl-proxy service *ssl-proxy-name* [**client**]

構文の説明

ssl-proxy-name	SSL プロキシ名。
client	（任意）SSL クライアント プロキシ サービスを設定できます。**ssl-proxy service client** コマンドを参照してください。

デフォルト

サーバ NAT がイネーブルになっていて、クライアント NAT がディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 2.1(1)	このコマンドは、次のキーワードを含めるように変更されました。 • **authenticate**：証明書の確認方法を設定します。 • **client**：SSL クライアント プロキシ サービスを設定します。 • **policy urlrewrite**：URL 書き換えポリシーをプロキシ サーバに適用します。 • **sslv2**：SSL バージョン 2 をイネーブルにします。**server ipaddr** *ip-addr* **protocol** *protocol* **port** *portno* サブコマンドを参照してください。 • **trusted-ca** *ca-pool-name*：信頼できる認証局の設定をプロキシ サーバに適用します。

使用上のガイドライン

プロキシ サービス コンフィギュレーション サブモードでは、プロキシ サービスに関連付けられた仮想 IP アドレスとポート、および関連付けられたターゲット IP アドレスとポートを設定できます。また、プロキシのクライアント側（**virtual** キーワードで始まる）とサーバ側（**server** キーワードで始まる）の両方の TCP ポリシーと SSL ポリシーを定義することもできます。

クライアントのプロキシ サービス コンフィギュレーション サブモードで、クリア テキストのトラフィックを受け入れ、SSL トラフィックに暗号化し、バックエンド SSL サーバに転送するプロキシ サービスを指定します。

ほとんどの場合、実行されるほぼすべての SSL サーバ プロキシ設定が SSL クライアント プロキシ設定に対して有効です。ただし、次は例外です。

- SSL サーバ プロキシのための証明書を設定する必要がありますが、SSL クライアント プロキシのための証明書を設定する必要はありません。SSL クライアント プロキシのための証明書を設定する場合、ハンドシェイク プロトコルのクライアント認証段階でサーバからの証明書要求メッセージに応じてその証明書が送信されます。
- SSL ポリシーはサーバの SSL クライアント プロキシ サブコマンドに添付されるため、ssl サーバ プロキシの仮想サブコマンドに添付されます。

各プロキシ サービス コンフィギュレーション サブモード コマンドまたはプロキシ クライアント コンフィギュレーション サブモード コマンドをそれぞれの行で入力します。

表 2-7 に、プロキシ サービス コンフィギュレーション サブモードまたはプロキシ クライアント コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-7　プロキシ サービス コンフィギュレーション サブモード コマンドの説明

構文	説明
authenticate verify {**all** | **signature-only**}	証明書の確認方法を設定します。次のことを指定できます。 • **all**：CRL と署名機関を確認します。 • **signature-only**：署名のみを確認します。
certificate rsa general-purpose trustpoint *trustpoint-name*	証明書を RSA 汎用キーとともに設定し、トラストポイントを証明書に関連付けます。
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	コマンドをデフォルトに設定します。
exit	プロキシ サービス コンフィギュレーション サブモードまたはプロキシ クライアント コンフィギュレーション サブモードを終了します。
help	対話型ヘルプ システムの説明を表示します。
inservice	プロキシ サーバまたはクライアントが管理用にアップしていると宣言します。
nat {**server** | **client** *natpool-name*}	• **server :** クライアント側のトラフィックがサーバに転送される場合、宛先 IP アドレスの Network Address Translation（NAT; ネットワーク アドレス変換）をイネーブルにします。これがイネーブルの場合、宛先 IP アドレスがサービスのサーバ IP アドレスに置換されます。デフォルトでは、**nat server** はイネーブルです。 • **client** *natpool-name*：クライアント側のトラフィックがサーバに転送される場合、送信元 IP アドレスの Network Address Translation（NAT; ネットワーク アドレス変換）をイネーブルにします。アドレスのプールは、nat pool コマンドの対応するインスタンスで定義されます。 **（注）**　少なくとも 8 つの IP アドレスのプールを設定する必要があります。デフォルトでは、**nat client** はディセーブルです。
policy urlrewrite *policy-name*	URL 書き換えポリシーをプロキシ サーバに適用します。
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	プロキシ サーバにターゲット サーバの IP アドレスを定義します。また、ポート番号と転送プロトコルも指定できます。宛先 IP アドレスは SLB デバイスの仮想 IP アドレスまたは Web サーバの実際の IP アドレスにすることができます。**sslv2** キーワードは、SSL バージョン 2 のトラフィックの処理に使用されるサーバを指定します。
server policy tcp *server-side-tcp-policy-name*	TCP ポリシーをプロキシ サーバのサーバ側に適用します。ポート番号と転送プロトコルを指定できます。

表 2-7　プロキシ サービス コンフィギュレーション サブモード コマンドの説明 （続き）

構文	説明
trusted-ca *ca-pool-name*	信頼できる証明書の認証設定をプロキシ サーバに適用します。
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	STE がプロキシ処理を行う仮想サーバの仮想 IP アドレスを定義します。また、ポート番号と転送プロトコルも指定できます。*protocol* の有効な値は **tcp** です。*portno* の有効な値は 1 ～ 65535 です。**secondary** キーワード（任意）は、仮想 IP アドレスへの ARP 要求に STE が応答するのを回避します。
virtual {**policy ssl** *ssl-policy-name*}	SSL ポリシーをプロキシ サーバのクライアント側に適用します。
virtual {**policy tcp** *client-side-tcp-policy-name*}	TCP ポリシーをプロキシ サーバのクライアント側に適用します。

Content Switching Module（CSM; コンテンツ スイッチング モジュール）と SSL サービス モジュールの間のセキュア モードとブリッジ モードの両方がサポートされます。

ブリッジ モード トポロジに **secondary** キーワード（任意）を使用します。

例

次に、プロキシ サービス コンフィギュレーション サブモードを開始する例を示します。

```
ssl-proxy (config)# ssl-proxy service S6
ssl-proxy (config-ssl-proxy)#
```

次に、証明書の確認方法を設定する例を示します。

```
ssl-proxy (config-ssl-proxy)# authenticate verify all
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された SSL プロキシ サービスの証明書を設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定されたコマンドをデフォルト値に設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

次の例では、信頼できる証明書の認証設定をプロキシ サーバに適用する方法を示します。

```
ssl-proxy (config-ssl-proxy)# trusted-ca test1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの仮想 IP アドレスを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの SSL ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの TCP ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、暗号化されたトラフィックを転送する SSL サービス モジュールのクリア テキストの Web サーバを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

次の例では、特定のクリア テキストの Web サーバの TCP ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定されたサービス SSL オフロードのサーバ接続で使用されるクライアント アドレスの NAT プールを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

次の例では、クライアント側のトラフィックがサーバに転送される場合に宛先 IP アドレスの NAT をイネーブルにする方法と、クライアント側のトラフィックがサーバに転送される場合に送信元 IP アドレスの NAT をイネーブルにする方法を示します。

```
ssl-proxy (config-ssl-proxy)# nat server
  client  Enable client nat
  server  Enable server nat

Ssl-proxy(config-ssl-proxy)#nat server

Ssl-proxy(config-ssl-proxy)#nat client
Ssl-proxy(config-ssl-proxy)#exit
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8
  netmask  netmask
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8 netmask 255.255.255.0
Ssl-proxy(config-context)#natpool Test_nat 192.168.10.1 192.168.10.8 netmask 255.255.255.0
```

関連コマンド

show ssl-proxy service

ssl-proxy service client

クライアントのプロキシ サービス コンフィギュレーション サブモードを開始するには、**ssl-proxy service client** コマンドを使用します。

ssl-proxy service *ssl-proxy-name* **client**

構文の説明

ssl-proxy-name	SSL プロキシ サービス名。

デフォルト

クライアント NAT はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

クライアントのプロキシ サービス コンフィギュレーション サブモードで、クリア テキストのトラフィックを受け入れ、SSL トラフィックに暗号化し、バックエンド SSL サーバに転送するプロキシ サービスを指定します。

ほとんどの場合、実行されるほぼすべての SSL サーバ プロキシ設定が SSL クライアント プロキシ設定に対して有効です。ただし、次は例外です。

- SSL サーバ プロキシのための証明書を設定する必要がありますが、SSL クライアント プロキシのための証明書を設定する必要はありません。SSL クライアント プロキシのための証明書を設定する場合、ハンドシェイク プロトコルのクライアント認証段階でサーバからの証明書要求メッセージに応じてその証明書が送信されます。
- SSL ポリシーはサーバの SSL クライアント プロキシ サブコマンドに添付されるため、ssl サーバ プロキシの仮想サブコマンドに添付されます。

各プロキシ サービス コンフィギュレーション サブモード コマンドまたはプロキシ クライアント コンフィギュレーション サブモード コマンドをそれぞれの行で入力します。

表 2-8 に、プロキシ クライアント コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-8　プロキシ クライアント コンフィギュレーション サブモード コマンドの説明

構文	説明
certificate rsa general-purpose trustpoint *trustpoint-name*	証明書を RSA 汎用キーとともに設定し、トラストポイントを証明書に関連付けます。
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	コマンドをデフォルトに設定します。
exit	プロキシ クライアント コンフィギュレーション サブモードを終了します。
help	対話型ヘルプ システムの説明を表示します。

表 2-8　プロキシ クライアント コンフィギュレーション サブモード コマンドの説明 （続き）

構文	説明
inservice	プロキシ クライアントが管理用にアップしていると宣言します。
nat {**server** | **client** *natpool-name*}	SSL サービス モジュールによって開かれるサーバ側の接続のサーバ NAT またはクライアント NAT の使用状況を指定します。
policy urlrewrite *policy-name*	URL 書き換えポリシーをプロキシ サーバに適用します。
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno* [**sslv2**]	プロキシ サーバにターゲット サーバの IP アドレスを定義します。また、ポート番号と転送プロトコルも指定できます。宛先 IP アドレスは SLB デバイスの仮想 IP アドレスまたは Web サーバの実際の IP アドレスにすることができます。**sslv2** キーワードは SSL バージョン 2 をイネーブルにします。
server policy tcp *server-side-tcp-policy-name*	TCP ポリシーをプロキシ サーバのサーバ側に適用します。ポート番号と転送プロトコルを指定できます。
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	プロキシ サーバにターゲット サーバの IP アドレスを定義します。また、ポート番号と転送プロトコルも指定できます。宛先 IP アドレスは SLB デバイスの仮想 IP アドレスまたは Web サーバの実際の IP アドレスにすることができます。**sslv2** キーワードは、SSL バージョン 2 のトラフィックの処理に使用されるサーバを指定します。
virtual {**policy ssl** *ssl-policy-name*}	SSL ポリシーをプロキシ サーバのクライアント側に適用します。
virtual {**policy tcp** *client-side-tcp-policy-name*}	TCP ポリシーをプロキシ サーバのクライアント側に適用します。

Content Switching Module（CSM; コンテンツ スイッチング モジュール）と SSL サービス モジュールの間のセキュア モードとブリッジ モードの両方がサポートされます。

ブリッジ モード トポロジに **secondary** キーワード（任意）を使用します。

例

次に、クライアントのプロキシ サービス コンフィギュレーション サブモードを開始する例を示します。

```
ssl-proxy (config)# ssl-proxy service S7 client
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された SSL プロキシ サービスの証明書を設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定されたコマンドをデフォルト値に設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの仮想 IP アドレスを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの SSL ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定された仮想サーバの TCP ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、暗号化されたトラフィックを転送する SSL サービス モジュールのクリア テキストの Web サーバを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

次の例では、特定のクリア テキストの Web サーバの TCP ポリシーを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定されたサービス SSL オフロードのサーバ接続で使用されるクライアント アドレスの NAT プールを設定する方法を示します。

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

次の例では、指定されたサービス SSL オフロードのサーバ接続に対して NAT サーバ アドレスをイネーブルにする方法を示します。

```
ssl-proxy (config-ssl-proxy)# nat server
ssl-proxy (config-ssl-proxy)#
```

関連コマンド

show ssl-proxy service

ssl-proxy ssl ratelimit

過負荷の状況で新しい接続を禁止するには、**ssl-proxyy ssl ratelimit** コマンドを使用します。このコマンドの **no** 形式を使用すると、メモリを使用できる場合に新しい接続が可能になります。

ssl-proxyy ssl ratelimit

no ssl-proxyy ssl ratelimit

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次の例では、過負荷の状況で新しい接続を禁止する方法を示します。

```
ssl-proxy (config)# ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

次の例では、過負荷の状況でメモリを使用できる場合に新しい接続を許可する方法を示します。

```
ssl-proxy (config)# no ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

ssl-proxy vlan

プロキシ VLAN コンフィギュレーション サブモードを開始するには、**ssl-proxy vlan** コマンドを使用します。プロキシ VLAN コンフィギュレーション サブモードでは、SSL サービス モジュールの VLAN を設定できます。

ssl-proxy vlan *vlan*

構文の説明

vlan	VLAN ID。有効な値は 1 ～ 1005 です。

デフォルト

デフォルトの設定は次のとおりです。

- *hellotime* は 3 秒です。
- *holdtime* は 10 秒です。
- *priority* は 100 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 12.1(13)E および SSL Services Module Release 1.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。
SSL Services Module Release 2.1(1)	このコマンドは、HSRP を設定する **standby** キーワードと引数を含めるように変更されました。

使用上のガイドライン

CSM では VLAN 1 がサポートされません。

SSL サービス モジュールでは、拡張範囲 VLAN がサポートされません。

各 プロキシ VLAN コンフィギュレーション サブモード コマンドをそれぞれの行で入力します。

表 2-9 に、プロキシ VLAN コンフィギュレーション サブモードで使用できるコマンドを示します。

表 2-9　プロキシ VLAN コンフィギュレーション サブモード コマンドの説明

構文	説明
admin	VLAN を管理 VLAN として設定します。
exit	プロキシ VLAN コンフィギュレーション サブモードを終了します。
gateway *prefix* [**drop** | **forward**]	VLAN をインターネットへのゲートウェイとともに設定します。
help	対話型ヘルプ システムの説明を表示します。
ipaddr *prefix mask*	VLAN を IP アドレスおよびサブネット マスクとともに設定します。
no	コマンドを無効にするか、デフォルト値を設定します。

表 2-9　プロキシ VLAN コンフィギュレーション サブモード コマンドの説明 （続き）

構文	説明
route {*prefix mask*} {**gateway** *prefix*}	SSL サービス モジュールが直接接続されていないサブネットワークに到達できるようにゲートウェイを設定します。
standby [*group-number*] {**authentication text** *string*} | {**delay minimum** [*min-delay*] **reload** [*reload-delay*]} | {**ip** [*ip-address* [**secondary**]]} | {**mac-address** *mac-address*} | {**mac-refresh** *seconds*} | {**name** *group-name*} | {**preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]} | {**priority** *priority*} | {**redirects** [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]} | {**timers** [**msec**] *hellotime* [**msec**] *holdtime*} | {**track** *object-number* [**decrement** *priority*]}	VLAN で冗長性を設定します。有効な値については、次のコマンドを参照してください。 • **standby authentication** • **standby delay minimum reload** • **standby ip** • **standby mac-address** • **standby mac-refresh** • **standby name** • **standby preempt** • **standby priority** • **standby redirects** • **standby timers** • **standby track** • **standby use-bia**

異なる管理 VLAN を設定できるようにするには、現在の管理 VLAN の管理 VLAN ステータスを削除する必要があります。

管理 VLAN は、証明書エージェント（PKI）と管理ステーション（SNMP）との通信に使用されます。

ゲートウェイを設定する場合、**drop** キーワードを使用すると、パケットに関連付けられた仮想サービスが見つからない場合、SSL サービス モジュールでパケットをドロップできます。

ゲートウェイを設定する場合、**forward** キーワードを使用すると、パケットに関連付けられた仮想サービスが見つからない場合、SSL サービス モジュールで、指定された VLAN のゲートウェイにパケットを転送できます。

HSRP の設定に有効な値は次のとおりです。

- *group-number*：（任意）HSRP がアクティブになっているインターフェイス上のグループ番号。有効な値は 0 ～ 255 です。*group-number* を指定しなかった場合は、グループ **0** が使用されます。
- **ip** *ip-addr* : HSRP インターフェイスの IP アドレスを指定します。
- **priority** *priority* : HSRP インターフェイスのプライオリティを指定します。HSRP グループ内の 1 つ以上のインターフェイスのプライオリティを上げます。プライオリティが最高のインターフェイスが HSRP グループに対してアクティブになります。
- **prempt** ：プリエンプションをイネーブルにします。プリエンプションをイネーブルにすると、ローカル ルータのホット スタンバイのプライオリティが現在アクティブなルータよりも高い場合、ローカル ルータがアクティブ ルータとして制御を引き継ごうとします。プリエンプションを設定しない場合、ローカル ルータはアクティブ状態のルータがないことを示す情報を受け取った場合のみ、アクティブ ルータとして制御を引き継ぎます（指定ルータとして動作する）。

- **delay**：（任意）プリエンプションの遅延を指定します。ルータが最初に起動するときは、完全なルーティング テーブルがありません。プリエンプション処理するように設定されている場合、アクティブ ルータになりますが、適切なルーティング サービスを提供できません。プリエンプション処理を行うルータが実際にアクティブ ルータのプリエンプション処理する前の遅延を設定できます。
- *type time*：プリエンプションのタイプと遅延を指定します。有効な値は次のとおりです。
  - **minimum** *time*：遅延の最小期間を秒単位で指定します。有効な値は 0 ～ 3600 秒（1 時間）です。
  - **reload** *time*：リロードした後のみのプリエンプション遅延を指定します。
  - **sync** *time*：遅延の最大同期期間を秒単位で指定します。
- **timers** [**msec**] *hellotime holdtime*：hello パケットの間隔と、他のルータがアクティブ ホット スタンバイ ルータまたはスタンバイ ルータのダウンを宣言するまでの時間を設定します。有効な値は次のとおりです。
  - **msec**：（任意）間隔（ミリ秒単位）。ミリ秒のタイマーにより、フェールオーバーを迅速に実行できます。
  - *hellotime*：hello の間隔（秒単位）。有効な値は 1 ～ 254 秒です。hello 間隔は **msec** キーワードでミリ秒単位で指定できます。有効な値は 15 ～ 999 ミリ秒です。デフォルト値は 3 秒です。
  - *holdtime*：アクティブ ルータまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒単位）。有効な値は x ～ 255 です。ホールドタイムは **msec** キーワードでミリ秒単位で指定できます。有効な値は y ～ 3000 ミリ秒です。デフォルト値は 10 秒です。

    ここで

    x は *hellotime* + 50 ミリ秒で、1 秒未満は切り上げます。

    y は *hellotime* の 3 倍以上であり、かつ 50 ミリ秒以上です。

例

次に、プロキシ VLAN コンフィギュレーション サブモードを開始する例を示します。

```
ssl-proxy (config)# ssl-proxy vlan 6
ssl-proxy (config-vlan)#
```

次の例では、指定されたコマンドをデフォルト値に設定する方法を示します。

```
ssl-proxy (config-vlan)# default admin
ssl-proxy (config-vlan)# default gateway
ssl-proxy (config-vlan)# default ipaddr
ssl-proxy (config-vlan)# default route
```

次の例では、指定した VLAN をゲートウェイとともに設定する方法を示します。

```
ssl-proxy (config-vlan)# gateway 209.0.207.5
ssl-proxy (config-vlan)#
```

次の例では、指定した VLAN を IP アドレスおよびサブネット マスクとともに設定する方法を示します。

```
ssl-proxy (config-vlan)# ipaddr 208.59.100.18 255.0.0.0
ssl-proxy (config-vlan)#
```

次の例では、SSL サービス モジュールから直接接続されていないサブネットワークに到達するためのゲートウェイを設定する方法を示します。

```
ssl-proxy (config-vlan)# route 210.0.207.0 255.0.0.0 gateway 209.0.207.6
ssl-proxy (config-vlan)#
```

次の例では、SSL モジュール上に HSRP を設定する方法を示します。

```
ssl-proxy(config)# ssl-proxy vlan 100
ssl-proxy(config-vlan)# ipaddr 10.1.0.20 255.255.255.0
ssl-proxy(config-vlan)# gateway 10.1.0.1
ssl-proxy(config-vlan)# admin
ssl-proxy(config-vlan)# standby 1 ip 10.1.0.21
ssl-proxy(config-vlan)# standby 1 priority 110
ssl-proxy(config-vlan)# standby 1 preempt
ssl-proxy(config-vlan)# standby 2 ip 10.1.0.22
ssl-proxy(config-vlan)# standby 2 priority 100
ssl-proxy(config-vlan)# standby 2 preempt
ssl-proxy(config-vlan)# end
ssl-proxy#
```

関連コマンド

show ssl-proxy vlan

standby authentication

HSRP の認証ストリングを設定するには、**standby authentication** コマンドを使用します。認証ストリングを削除するには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **authentication text** *string*

no standby [*group-number*] **authentication text** *string*

構文の説明

group-number	（任意）この認証ストリングを適用するインターフェイス上のグループ番号。
text *string*	認証ストリングは、最大 8 文字にすることができます。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は **0** です。
- *string* は **cisco** です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

HSRP は、認証されていない HSRP メッセージを無視します。

認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバに同じ認証ストリングを設定する必要があります。認証の不一致が発生すると、デバイスで、HSRP で設定される他のルータから、指定されたホット スタンバイ IP アドレスおよびホット スタンバイ タイマー値を学習できません。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるための認証ストリングとして、「word」を設定する例を示します。

```
ssl-proxy (config-vlan)# standby 1 authentication text word
ssl-proxy (config-vlan)#
```

standby delay minimum reload

HSRP グループが初期化されるまでの遅延を設定するには、**standby delay minimum reload** コマンドを使用します。遅延をディセーブルにするには、このコマンドの **no** 形式を使用します。

standby delay minimum [*min-delay*] **reload** [*reload-delay*]

no standby delay minimum [*min-delay*] **reload** [*reload-delay*]

構文の説明

min-delay	（任意）インターフェイスの起動後に HSRP グループの初期化を遅延する最小時間（秒単位）。有効な値は ____ ～ ____ 秒です。
reload-delay	（任意）ルータがリロードされた後の遅延時間（秒単位）。有効な値は ____ ～ ____ 秒です。

デフォルト

デフォルトの設定は次のとおりです。

- *min-delay* は **1** 秒です。
- *reload-delay* は **5** 秒です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

min-delay は、後続のすべてのインターフェイス イベントに適用されます。

reload-delay は、ルータがリロードした後の最初のインターフェイス起動イベントにのみ適用されます。

アクティブ ルータに障害が発生したか、ネットワークから削除された場合、スタンバイ ルータが自動的に新しいアクティブ ルータになります。以前のアクティブ ルータがオンラインに戻った場合、**standby preempt** コマンドを使用して、アクティブ ルータを引き継ぐかどうかを制御できます。

ただし、場合によっては、**standby preempt** コマンドを使用しなくても、以前のアクティブ ルータがリロードされ、オンラインに戻った後で、アクティブ ロールを再開します。HSRP グループの初期化の遅延を設定するには、**standby delay minimum reload** コマンドを使用します。このコマンドを使用すると、ルータがアクティブ ロールを再開する前にパケットが通過する時間を指定できます。

standby timers コマンドがミリ秒単位で設定されている場合や、HSRP がスイッチの VLAN インターフェイスで設定されている場合、**standby delay minimum reload** コマンドを使用することを推奨します。

ほとんどの設定では、デフォルト値でパケットが通過するための十分な時間が得られるため、より長い遅延値を設定する必要はありません。

HSRP パケットがインターフェイスで受信された場合、遅延がキャンセルされます。

例

次の例では、遅延の最小値を 30 秒に設定し、最初のリロード後の遅延を 120 秒に設定する方法を示します。

```
ssl-proxy (config-vlan)# standby delay minimum 30 reload 120
ssl-proxy (config-vlan)#
```

関連コマンド

show standby delay
standby preempt
standby timers

standby ip

HSRP をアクティブ化するには、**standby ip** コマンドを使用します。HSRP をディセーブルにするには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **ip** [*ip-address* [**secondary**]]

no standby [*group-number*] **ip** [*ip-address*]

構文の説明

group-number	（任意）HSRP をアクティブ化するインターフェイスのグループ番号。
ip-address	（任意）ホット スタンバイ ルータ インターフェイスの IP アドレス。
secondary	（任意）IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを示します。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は 0 です。
- HSRP はデフォルトでディセーブルです。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

standby ip コマンドを使用すると、プライマリ HSRP アドレスとセカンダリ HSRP アドレスを設定できます。

standby ip コマンドを実行すると、設定されたインターフェイスで HSRP がアクティブになります。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しない場合、指定アドレスがスタンバイ機能によって学習されます。HSRP で指定ルータを選択できるようにするには、ケーブル上の 1 つ以上のルータが指定アドレスと一緒に設定されているか、または学習している必要があります。アクティブ ルータ上の指定アドレスを設定すると、常に現在使用されている指定アドレスが上書きされます。

インターフェイス上で **standby ip** コマンドをイネーブルにした場合、プロキシ ARP 要求の処理が変更されます（プロキシ ARP がディセーブルになっていない場合）。インターフェイスのホット スタンバイの状態がアクティブの場合、ホット スタンバイ グループの MAC アドレスを使用して、プロキシ ARP 要求に応答されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

例

次に、イーサネット インターフェイス 0 のグループ 1 に対して HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

```
ssl-proxy (config-vlan)# standby 1 ip
ssl-proxy (config-vlan)#
```

次の例では、IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを示す方法を示します。

```
ssl-proxy (config-vlan)# standby ip 1.1.1.254
ssl-proxy (config-vlan)# standby ip 1.2.2.254 secondary
ssl-proxy (config-vlan)# standby ip 1.3.3.254 secondary
```

standby mac-address

HSRP の仮想 MAC アドレスを指定するには、**standby mac-address** コマンドを使用します。標準の仮想 MAC アドレス（0000.0C07.ACxy）に戻すには、このコマンドの no 形式を使用します。

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

構文の説明

group-number	（任意）HSRP をアクティブ化するインターフェイスのグループ番号。デフォルトは 0 です。
mac-address	MAC アドレス。

デフォルト

このコマンドが設定されておらず、**standby use-bia** コマンドが設定されていない場合、標準の仮想 MAC アドレスの 0000.0C07.AC*xy* が使用されます。*xy* は 16 進数のグループ番号です。このアドレスは RFC 2281、『*Cisco Hot Standby Router Protocol (HSRP)*』で指定されています。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

このコマンドは、トークン リング インターフェイスでは使用できません。

HSRP を使用すると、エンド ステーションで IP ルーティングのファーストホップ ゲートウェイを見つけるのに役立ちます。エンド ステーションは、デフォルトのゲートウェイで設定されます。ただし、HSRP はその他のプロトコルにファーストホップの冗長性を提供できます。Advanced Peer-to-Peer Networking（APPN; 拡張分散ネットワーク機能）などの一部のプロトコルでは、MAC アドレスを使用して、ルーティングのためのファーストホップを特定します。この際、多くの場合で仮想 MAC アドレスを指定できる必要があります。仮想 IP アドレスは、これらのプロトコルには重要ではありません。仮想 MAC アドレスを指定するには、**standby mac-address** コマンドを使用します。

ルータがアクティブな場合、指定された MAC アドレスが仮想 MAC アドレスとして使用されます。

このコマンドは、特定の APPN 設定を対象としています。類似用語については、表 2-10 を参照してください。

表 2-10　APPN と IP の類似用語

APPN	IP
エンド ノード	ホスト
ネットワーク ノード	ルータまたはゲートウェイ

APPN ネットワークでは、エンドノードは隣接するネットワーク ノードの MAC アドレスを使用して設定されていることがほとんどです。仮想 MAC アドレスをエンド ノートで使用される値に設定するには、ルータで **standby mac-address** コマンドを使用します。

例

次の例では、HSRP グループ 1 に仮想 MAC アドレスを設定する方法を示します。

```
ssl-proxy (config-vlan)# standby 1 mac-address 4000.1000.1060
ssl-proxy (config-vlan)#
```

関連コマンド

show standby
standby use-bia

standby mac-refresh

HSRP が FDDI で動作する場合に MAC キャッシュを更新するためのパケットが送信される間隔を変更するには、**standby mac-refresh** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

standby mac-refresh *seconds*

no standby mac-refresh

構文の説明

seconds	MAC キャッシュを更新するためにパケットが送信される間隔（秒単位）。有効な値は 1 ～ 255 秒です。

デフォルト

seconds は **10** 秒です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

このコマンドは、FDDI で動作する HSRP のみに適用されます。ラーニング ブリッジまたはスイッチ上の MAC キャッシュを更新するために、パケットが 10 秒間隔で送信されます。デフォルトでは、MAC キャッシュ エントリが 300 秒（5 分）で期限切れになります。

パケットはラーニング ブリッジまたはスイッチのみを対象としていますが、FDDI リング上の HSRP に参加しているその他のすべてのルータが更新パケットを受信します。間隔を変更するには、このコマンドを使用します。パケットの更新を回避する場合、間隔を 0 に設定します（FDDI は存在しているものの、ラーニング ブリッジまたはスイッチがない場合）

例

次の例では、MAC 更新の間隔を 100 秒に変更する方法を示します。次の例では、エントリが期限切れになる前にラーニング ブリッジで 3 つのパケットを失う必要があります。

```
ssl-proxy (config-vlan)# standby mac-refresh 100
ssl-proxy (config-vlan)#
```

standby name

スタンバイ グループ名を設定するには、**standby name** コマンドを使用します。名前をディセーブルにするには、このコマンドの **no** 形式を使用します。

standby name *group-name*

no standby name *group-name*

構文の説明

group-name	スタンバイ グループの名前を指定します。

デフォルト

HSRP はディセーブルです。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

group-name 引数は HSRP グループを指定します。

例

次の例では、スタンバイ名を SanJoseHA に指定する方法を示します。

```
ssl-proxy (config-vlan)# standby name SanJoseHA
ssl-proxy (config-vlan)#
```

関連コマンド

ip mobile home-agent redundancy（『*Cisco IOS Release 12.2 Command Reference*』を参照）

standby preempt

HSRP プリエンプションおよびプリエンプションの遅延を設定するには、**standby preempt** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

no standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

構文の説明

group-number	（任意）このコマンドの他の引数を適用するインターフェイス上のグループ番号。
delay	（任意）**minimum**、**reload**、または **sync** キーワードが指定されている場合に必要です。
minimum *delay*	（任意）*delay* に遅延の最小期間を秒単位で指定します。有効な値は 0 ～ 3600 秒（1 時間）です。
reload *delay*	（任意）リロード後のみのプリエンプションの遅延を指定します。
sync *delay*	（任意）*delay* に遅延の最大同期期間を秒単位で指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は 0 です。
- *delay* は 0 秒です。ルータはただちにプリエンプション処理を実行します。デフォルトでは、後で起動するルータがスタンバイ ルータになります。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

delay 引数を指定すると、ローカル ルータでアクティブ ロールの引き継ぎが、ルータが最後に再起動されてから *delay*（最小）秒間延期されます。

このコマンドを使用する場合、ルータはプリエンプション処理を実行するように設定されます。これはローカル ルータに現在のアクティブ ルータよりも高いホット スタンバイのプライオリティが設定されている場合、ローカル ルータがアクティブ ルータとして制御を引き継ぐ必要があることを意味します。プリエンプションを設定しない場合、ローカル ルータはアクティブ状態のルータがないことを示す情報を受け取った場合のみ、アクティブ ルータとして制御を引き継ぎます（指定ルータとして動作する）。

ルータが最初に起動するときは、完全なルーティング テーブルがありません。ルータでプリエンプション処理を実行するように設定した場合、アクティブ ルータになりますが、適切なルーティング サービスは提供できません。プリエンプション処理を行うルータが実際にアクティブ ルータのプリエンプション処理する前の遅延を設定できます。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

IP 冗長クライアントでは、プリエンプションの実行を回避できます。**standby preempt delay sync** *delay* コマンドでは、IP 冗長クライアントでプリエンプションを回避できる最大秒数を指定します。この期限が切れた場合、IP 冗長クライアントの状態に関係なく、プリエンプションが実行されます。

standby preempt delay reload *delay* コマンドでは、ルータのリロード後にのみプリエンプションが発生するように指定できます。これによって、ルータが安定して起動するようになります。この起動時の初期遅延後に、デフォルトの動作に戻ります。

no standby preempt delay コマンドでは、プリエンプション遅延がディセーブルになりますが、プリエンプションはイネーブルのままです。**no standby preempt delay minimum** *delay* コマンドでは、最小遅延がディセーブルになりますが、同期化の遅延が設定されている場合、これはそのままです。

例

次の例では、ルータがアクティブ ルータになるように試行する前に、300 秒（5 分）間待機するように設定する例を示します。

```
ssl-proxy (config-vlan)# standby preempt delay minimum 300
ssl-proxy (config-vlan)#
```

standby priority

HSRP のプライオリティを設定するには、**standby priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

構文の説明

group-number	（任意）このコマンドの他の引数を適用するインターフェイス上のグループ番号。
priority	潜在的なホット スタンバイ ルータの優先順位を指定するプライオリティ値。有効な値は 1 ～ 255 で、1 の場合は最小のプライオリティを指定し、255 の場合は最高のプライオリティを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は 0 です。
- *priority* は 100 です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

HSRP グループ内の最高のプライオリティ値が設定されたルータがアクティブ ルータになります。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

割り当てられたプライオリティは、アクティブ ルータとスタンバイ ルータを選択するために使用されます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータが指定されたアクティブ ルータになります。プライオリティが等しい場合、プライマリ IP アドレスが比較され、大きい IP アドレスが優先されます。

インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。

例

次の例では、ルータのプライオリティを確認する方法を示します。

```
ssl-proxy (config-vlan)# standby priority 120
ssl-proxy (config-vlan)#
```

例

standby track

standby redirects

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）リダイレクト メッセージの HSRP フィルタリングをイネーブルにするには、**standby redirects** コマンドを使用します。ICMP リダイレクト メッセージの HSRP フィルタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

standby redirects [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

no standby redirects [**unknown**]

構文の説明

enable	（任意）HSRP で設定されるインターフェイス上の ICMP リダイレクト メッセージのフィルタリングを実行できるようにします。ネクストホップ IP アドレスは HSRP 仮想 IP アドレスに変更できます。
disable	（任意）HSRP で設定されるインターフェイス上の ICMP リダイレクト メッセージのフィルタリングをディセーブルにします。
timers	（任意）HSRP ルータ アドバタイズメント タイマーを調整します。
advertisement	（任意）HSRP ルータ アドバタイズメント間隔（秒単位）。有効な値は 10 ～ 180 秒です。
holddown	（任意）HSRP ルータ ホールドダウン間隔（秒単位）。有効な値は 61 ～ 3600 です。
unknown	（任意）パケットに含まれるネクストホップ IP アドレスが実際の IP アドレスとアクティブな仮想 IP アドレスの HSRP テーブルで不明な場合に ICMP パケットを送信できるようにします。

デフォルト

デフォルトの設定は次のとおりです。

- インターフェイス上に HSRP を設定する場合、ICMP リダイレクト メッセージの HSRP フィルタリングはイネーブルです。
- *advertisement* は 60 秒です。
- *holddown* は 180 秒です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

standby redirects コマンドをグローバルに、またはインターフェイスごとに設定できます。インターフェイス上で最初に HSRP を設定する場合、このインターフェイスの設定ではグローバル値を継承します。インターフェイス上の ICMP リダイレクトのフィルタリングを明示的にディセーブルにする場合、グローバル コマンドでこの機能を再びイネーブルにできません。

no standby redirects コマンドは **standby redirects disable** コマンドと同じです。このコマンドの **no** 形式を NVRAM に保存することは推奨しません。デフォルトでは、このコマンドがディセーブルになっているため、**standby redirects disable** コマンドを使用して、この機能をディセーブルにすることを推奨します。

standby redirects コマンドをイネーブルにすると、ルータの実際の IP アドレスを、ネクストホップアドレスまたはリダイレクト パケットのゲートウェイ フィールドの仮想 IP アドレスに置換できます。HSRP は、実際の IP アドレスと仮想 IP アドレスのテーブルでネクストホップ IP アドレスを検索します。一致するアドレスが見つからない場合、HSRP ルータではリダイレクト パケットを変更しないまま送出できます。ホスト HSRP ルータは不明なルータ、つまり、アクティブな HSRP グループがないルータにリダイレクトされます。このリダイレクトの送信を停止するには、**no standby redirect unknown** コマンドを使用します。

例

次の例では、HSRP で ICMP リダイレクト メッセージをフィルタリングする方法を示します。

```
ssl-proxy (config-vlan)# standby redirects
ssl-proxy (config-vlan)#
```

次の例では、インターフェイス イーサネット 0 で HSRP ルータ アドバタイズメント間隔を 90 秒に、ホールドダウン タイマーを 270 秒に変更する例を示します。

```
ssl-proxy (config-vlan)# standby redirects timers 90 270
ssl-proxy (config-vlan)#
```

関連コマンド

show standby
show standby redirect

standby timers

hello パケットの間隔と他のルータがアクティブ ホット スタンバイまたはスタンバイ ルータのダウンを宣言するまでの時間を設定するには、**standby timers** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

構文の説明

group-number	（任意）タイマーが適用されるインターフェイス上のグループ番号。
msec	（任意）間隔（ミリ秒単位）。
hellotime	Hello 間隔（秒単位）。有効な値については、「使用上のガイドライン」を参照してください。
holdtime	アクティブ ルータまたはスタンバイ ルータのダウンが宣言されるまでの時間（秒単位）。有効な値については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は 0 です。
- *hellotime* は 3 秒です。
- *holdtime* は 10 秒です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

hellotime の有効な値は次のとおりです。

- **msec** キーワードを入力しない場合、有効な値は 1 ～ 254 秒です。
- **msec** キーワードを入力する場合、有効な値は 15 ～ 999 ミリ秒です。

holdtime の有効な値は次のとおりです。

- **msec** キーワードを入力しない場合、有効な値は *x* ～ 255 秒です。*x* は *hellotime* + 50 ミリ秒で、1 秒未満は切り上げます。
- **msec** キーワードを入力する場合、有効な値は *y* ～ 3000 ミリ秒です。*y* は *hellotime* の 3 倍以上かつ 50 ミリ秒以上です。

msec キーワードを指定する場合、hello 間隔はミリ秒単位です。ミリ秒のタイマーにより、フェールオーバーを迅速に実行できます。

standby timers コマンドでは、スタンバイ hello パケットの間隔と、アクティブ ルータまたはスタンバイ ルータのダウンを宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を取得できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。ホット スタンバイ グループのすべてのルータは同じタイマー値を使用する必要があります。通常の場合、holdtime は hellotime 値の 3 倍以上です。holdtime の値の範囲によって、hellotime よりも大きい holdtime が強制されます。タイマーの値がミリ秒単位で指定されている場合、holdtime は hellotime 値の 3 倍以上かつ 50 ミリ秒以上にする必要があります。

一部の HSRP 状態のフラッピングは、holdtime が 250 ミリ秒未満に設定されていて、プロセッサがビジー状態の場合に発生する可能性があります。Cisco 7200 以降のプラットフォーム、Fast-Ethernet または FDDI インターフェイス以上では、250 ミリ秒未満の holdtime 値を使用することを推奨します。**process-max-time** コマンドを適切な値に設定することは、フラッピングにも役立つ場合があります。

スタンバイ タイマーの値が 1 秒未満の場合、HSRP hello では学習されません。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

例

次の例では、イーサネット インターフェイス 0 上のグループ番号 1 で、hello パケットの間隔を 5 秒、ルータがダウンしていると見なされてからの時間を 15 秒に設定します。

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

次の例では、イーサネット インターフェイス 0 上の 172.19.10.1 に配置されるホット ルータ インターフェイスで、hello パケットの間隔を 300 ミリ秒、ルータがダウンしていると見なされてからの時間を 900 ミリ秒に設定します。

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

次の例では、イーサネット インターフェイス 0 上の 172.18.10.1 に配置されるホット ルータ インターフェイスで、hello パケットの間隔を 15 ミリ秒、ルータがダウンしていると見なされてからの時間を 50 ミリ秒に設定します。holdtime の最小値は 50 ミリ秒であるため、holdtime は hellotime の 3 倍より大きいことに注意してください。

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

standby track

HSRP でオブジェクトをトラッキングし、オブジェクトの状態に基づいてホット スタンバイのプライオリティを変更するように設定するには、**standby track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

standby [*group-number*] **track** *object-number* [**decrement** *priority*]

no standby [*group-number*] **track** *object-number* [**decrement** *priority*]

構文の説明

group-number	（任意）トラッキングが適用されるグループ番号です。
object-number	トラッキングされるオブジェクトを表すオブジェクト番号。値の範囲は 1 ～ 500 です。
decrement *priority*	（任意）トラッキング オブジェクトがダウンした（またはアップに戻った）際の、ルータのホット スタンバイ プライオリティを減少（または増加）させる量です。
group-number	（任意）トラッキングが適用されるインターフェイス上のグループ番号。

デフォルト

デフォルトの設定は次のとおりです。

- *group-number* は **0** です。
- *priority* は **10** です。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

このコマンドでは、ルータのホット スタンバイ プライオリティとトラッキングされるオブジェクトの可用性を関連付けます。インターフェイス オブジェクトまたは IP ルート オブジェクトをトラッキングするには、**track interface** または **track ip route** グローバル コンフィギュレーション コマンドを使用します。HSRP クライアントは **standby track** コマンドを使用してトラッキング プロセスにトラッキング対象を登録でき、オブジェクト変更時にアクションを実行できます。

トラッキングされるオブジェクトがダウンすると、プライオリティが 10 下がります。オブジェクトがトラッキングされない場合、状態の変更はプライオリティに影響しません。ホット スタンバイ用に設定されたオブジェクトごとに、トラッキングするオブジェクトのリストを個別に設定できます。

オプションの *priority* 引数は、トラッキングされるオブジェクトがダウンした場合にホット スタンバイ プライオリティがどれだけ下がるかを指定します。トラッキングされるオブジェクトが稼動状態に戻ると、プライオリティは同じ分だけ増加します。

複数のトラッキングされるオブジェクトがダウンしている場合、*priority* 値で設定されたかどうかに関係なく、プライオリティの低下は累積的です、

グループのすべてのトラッキング設定を削除するには、**no standby** *group-number* **track** コマンドを使用します。

グループ番号 0 を使用する場合、NVRAM にグループ番号が書き込まれず、下位互換性が提供されます。

リリース 12.2(15)T 以前の **standby track** コマンド構文は引き続きサポートされます。古い形式を使用すると、トラッキングされるオブジェクトが新しいトラッキング プロセスで作成されます。このトラッキング情報は、**show track** コマンドを使用して表示できます。

例

次の例では、シリアル インターフェイス 1/0 の IP ルーティング機能をトラッキングする方法を示します。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ステートがダウンになると、その HSRP グループのプライオリティが 10 だけ引き下げられます。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。

ただし、ルータ A のシリアル インターフェイス 1/0 の IP ルーティングに障害が発生すると、HSRP グループのプライオリティが引き下げられてルータ B がアクティブ ルータとして処理を引き継ぐため、ホストに対するデフォルトの仮想ゲートウェイ サービスはサブネット 10.1.0.0 で継続されます。

ルータ A の設定

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.21 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 105
  standby 1 track 100 decrement 10
```

ルータ B の設定

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
  ip address 10.1.0.22 255.255.0.0
  standby 1 ip 10.1.0.1
  standby 1 priority 100
  standby 1 track 100 decrement 10
```

関連コマンド

standby preempt
standby priority

standby use-bia

割り当て済みの（イーサネットおよび FDDI の）MAC アドレスまたは（トークン リング上で）機能アドレスではなく、インターフェイスの焼き付けアドレスを仮想 MAC アドレスとして HSRP で使用するように設定するには、**standby use-bia** コマンドを使用します。デフォルト仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

standby use-bia [**scope interface**]

no standby use-bia

構文の説明

scope interface	（任意）主要なインターフェイスの代わりに、このコマンドが入力されたサブインターフェイスのみに対してこのコマンドが設定されるように指定します。

デフォルト

HSRP では、イーサネットおよび FDDI またはトークン リングの機能アドレスで事前に割り当てられた MAC アドレスを使用します。

コマンド モード

プロキシ VLAN コンフィギュレーション サブモードを開始します。

コマンド履歴

リリース	変更内容
SSL Services Module Release 2.1(1)	このコマンドのサポートは、Catalyst 6500 シリーズ スイッチで導入されました。

使用上のガイドライン

standby use-bia コマンドを入力すると、インターフェイス上の複数のスタンバイ グループを設定できます。インターフェイス上のホストにデフォルト ゲートウェイを設定する必要があります。インターフェイス上で **no ip proxy-arp** コマンドを設定することを推奨します。また、機能アドレスに設定されている送信元ハードウェア アドレスでの ARP 応答を拒否するデバイスがある場合、トークン リング インターフェイスで **standby use-bia** コマンドを設定することも推奨します。

HRSP が複数リングのソースルート ブリッジング環境で実行されていて、異なるリングに HSRP ルータが存在する場合に、**standby use-bia** コマンドを設定すると、Routing Information Field（RIF; ルーティング情報フィールド）に関する混乱を防ぐことができます。

scope interface キーワードなしの **standby use-bia** コマンドは、主要なインターフェイスのすべてのサブインターフェイスに適用されます。**scope interface** キーワード付き、およびこのキーワードなしの **standby use-bia** コマンドを同時に入力できません。

例

次の例では、仮想 MAC アドレスを仮想 IP アドレスにマッピングする方法を示します。

```
ssl-proxy (config-vlan)# standby use-bia
ssl-proxy (config-vlan)#
```