Catalyst 6500 シリーズ スイッチ WebVPN 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 WebVPN サービス モジュールのコマンドをアルファベット順に表示します。

WebVPN 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 WebVPN Services Module Installation and Verification Note*』
- 『*Catalyst 6500 Series Switch WebVPN Services Module Configuration Note*』
- 『*Catalyst 6500 Series Switch WebVPN Services Module System Message Guide*』

clear webvpn nbns

WebVPN サービス モジュールの NetBIOS Name Service（NBNS）をリセットするには、**clear webvpn nbns** コマンドを使用します。

clear webvpn nbns [**context** {*name* | **all**}]

シンタックスの説明

context	（任意）特定のコンテキストの統計情報をクリアします。
name	コンテキストの名前を指定します。
all	すべてのコンテキストを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

WebVPN サービス モジュールが保持しているすべての統計情報のカウンタをリセットするには、オプションを指定せずに **clear webvpn nbns** コマンドを使用します。

例

次に、WebVPN サービス モジュール上の各システム コンポーネントが保持している統計情報のカウンタをリセットする例を示します。

```
webvpn# clear webvpn nbns context context1
```

clear webvpn platform

WebVPN サービス モジュールのプラットフォーム拡張機能をリセットするには、**clear webvpn platform** コマンドを使用します。

clear webvpn platform {**conn** | **session** | **stats** [*type*] | **tunnel stats**}

シンタックスの説明

conn	グローバル接続をクリアします。
session	セッション情報をクリアします。
stats	統計情報をクリアします。
type	（任意）使用可能なオプションについては、「使用上のガイドライン」を参照してください。
tunnel stats	トンネルのカウンタをクリアします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

stats *type* で使用できるオプションは次のとおりです。

- **crypto** — 暗号の統計情報をクリアします。
- **crypto module** *module* — 指定したモジュール タイプの暗号の統計情報をクリアします。
- **fdu** — FDU の統計情報をクリアします。
- **ipc** — IPC の統計情報をクリアします。
- **ipc module** *module* — 指定したモジュール タイプの IPC の統計情報をクリアします。
- **module** *module* — 指定したモジュール タイプの統計情報をクリアします。
  module 変数で使用できるオプションは次のとおりです。
  - **all** — すべての CPU
  - **fdu** — FDU CPU
  - **ssl1** — SSL1 CPU
  - **tcp1** — TCP1 CPU
  - **tcp2** — TCP2 CPU
- **pki** [*pki_type*] — PKI の統計情報をクリアします。
  pki_type 変数で使用できるオプションは次のとおりです。
  - **auth** — 証明書の認証および許可の統計情報
  - **cache** — ピア証明書キャッシュの統計情報
  - **cert-header** — 証明書ヘッダー挿入の統計情報
  - **expiring** — 証明書期限切れ警告の統計情報
  - **ipc** — Interprocessor Communication（IPC; プロセッサ間通信）の統計情報
  - **memory** — メモリ使用状況の統計情報

- **pki module** *module* **—** 指定したモジュール タイプの PKI の統計情報をクリアします。
- **ssl —** SSL の統計情報をクリアします。
- **tcp —** TCP の統計情報をクリアします。

例

次に、WebVPN サービス モジュール上の各システム コンポーネントが保持しているプラットフォームのカウンタをリセットする例を示します。

```
webvpn# clear webvpn platform
```

clear webvpn session

WebVPN セッションをクリアするには、**clear webvpn session** コマンドを使用します。

clear webvpn session {**context** {*name* | **all**} | **user** *name* {**context** {*name* | **all**}}}

シンタックスの説明

context	特定のコンテキストの統計情報をクリアします。
name	コンテキストの名前を指定します。
all	すべてのコンテキストを指定します。
user *name*	ユーザ名を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

WebVPN サービス モジュールが保持しているすべての統計情報のカウンタをリセットするには、オプションを指定せずに **clear webvpn nbns** コマンドを使用します。

例

次に、WebVPN サービス モジュール上の各システム コンポーネントが保持しているセッションのカウンタをリセットする例を示します。

```
webvpn# clear webvpn session
```

clear webvpn stats

WebVPN サービス モジュール上の各システム コンポーネントが保持している統計情報のカウンタをリセットするには、**clear webvpn stats** コマンドを使用します。

clear webvpn stats [**cifs** [**context** {*name* | **all**}] | **context** {*name* | **all**} | **mangle** [**context** {*name* | **all**}] | **port-forward** [**context** {*name* | **all**}] | **tunnel** [**context** {*name* | **all**}]]

シンタックスの説明

cifs	（任意）WebVPN CIFS の統計情報
context	（任意）特定のコンテキストの統計情報をクリアします。
name	（任意）コンテキストの名前を指定します。
all	（任意）すべてのコンテキストを指定します。
mangle	（任意）WebVPN マングリングの統計情報をクリアします。
port-forward	（任意）WebVPN ポートフォワーディングの統計情報をクリアします。
tunnel	（任意）WebVPN トンネル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がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

WebVPN サービス モジュールが保持しているすべての統計情報のカウンタをリセットするには、オプションを指定せずに **clear ssl-proxy stats** コマンドを使用します。

例

次に、WebVPN サービス モジュール上の各システム コンポーネントが保持している統計情報のカウンタをリセットする例を示します。

```
webvpn# clear webvpn stats cifs
webvpn# clear webvpn stats context context1
webvpn# clear webvpn stats mangle context all
webvpn# clear webvpn stats tunnel
```

次に、WebVPN サービス モジュールが保持しているすべての統計情報のカウンタをクリアする例を示します。

```
webvpn# clear webvpn stats
webvpn#
```

crypto key export rsa pem

PEM 形式の RSA 鍵を WebVPN 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**} *pass_phrase*}

シンタックスの説明

keylabel	鍵の名前
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを指定します。*url* の有効値は次のとおりです。 • **archive: —** archive: ファイル システムにエクスポートします。 • **flash: —** flash: ファイル システムにエクスポートします。 • **ftp: —** ftp: ファイル システムにエクスポートします。 • **http: —** http: ファイル システムにエクスポートします。 • **https: —** https: ファイル システムにエクスポートします。 • **null: —** null: ファイル システムにエクスポートします。 • **nvram: —** nvram: ファイル システムにエクスポートします。 • **rcp: —** rcp: ファイル システムにエクスポートします。 • **scp: —** scp: ファイル システムにエクスポートします。 • **system: —** system: ファイル システムにエクスポートします。 • **tftp: —** tftp: ファイル システムにエクスポートします。
3des	168 ビット DES（3DES）暗号化アルゴリズムを指定します。
des	56 ビット DES-CBC 暗号化アルゴリズムを指定します。
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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

パス フレーズには空白および句読点を含む任意の句が使用できますが、疑問符（**?**）は使用できません。疑問符は、Cisco IOS のパーサーにとって特別な意味を持ちます。

パス フレーズ保護により、パス フレーズと鍵が関連付けられます。鍵は、エクスポート時にパス フレーズを使用して暗号化されます。インポート時には、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

次に、WebVPN サービス モジュールから鍵をエクスポートする例を示します。

```
wwbvpn(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:
wwbvpn(config)#
```

crypto key generate

RSA 鍵ペアを生成するには、**crypto key generate** コマンドを使用します。

crypto key generate rsa {**usage-keys**|**general-keys**} {**label** *key-label*} [**exportable**] [**modulus** *size*]

シンタックスの説明

general-keys	署名および暗号化用に汎用の RSA 鍵ペアを生成します。
usage-keys	署名および暗号化用に別個の RSA 鍵ペアを生成します。
label *key-label*	鍵を指定します。
exportable	（任意）鍵のエクスポートが可能であることを指定します。
modulus *size*	（任意）係数長をビットで指定します。有効値は 512、768、1024、1536、および 2048 ビットです。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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

WebVPN サービス モジュールは、最大 8 レベルの Certificate Authority（CA; 認証局）をサポートします（1 つのルート CA と最大 7 つの下位 CA）。

鍵の生成時に、鍵のエクスポートが可能であることを指定できます。エクスポート可能またはエクスポート不可として生成された鍵は、期限が切れるまで変更できません。

（注）　WebVPN サービス モジュールは、512、768、1024、1536、および 2048 ビットの係数長をサポートしています。512 または 768 も指定できますが、最小係数長として 1024 を推奨します。係数が長くなるほど生成にも使用にも時間がかかりますが、それだけセキュリティが強化されます。

鍵ペアを生成したら、自己署名証明書を生成して SSL サービスをテストできます。

例

次に、特殊な用途の RSA 鍵を生成する例を示します。

```
crypto key generate rsa usage-keys

The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature
Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>

Generating RSA keys.... [OK].

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption
Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>

Generating RSA keys.... [OK].
```

次に、汎用の RSA 鍵を生成する例を示します。

（注） 特殊な用途の鍵と汎用の鍵を両方とも生成することはできません。どちらか一方だけです。

```
webvpn(config)# crypto key generate rsa general-keys label kp1 exportable

The name for the keys will be: kp1

Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
Generating RSA keys.... [OK].
```

crypto key import rsa pem

PEM 形式の RSA 鍵を外部システムから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*}

シンタックスの説明

keylabel	鍵の名前
usage-keys	（任意）汎用の鍵ペアを 1 組生成するのではなく、特殊な用途の鍵ペアを 2 組生成するように指定します。
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを指定します。有効値は次のとおりです。 • **archive: —** archive: ファイル システムからインポートします。 • **cns: —** cns: ファイル システムからインポートします。 • **flash: —** flash: ファイル システムからインポートします。 • **ftp: —** ftp: ファイル システムからインポートします。 • **http: —** http: ファイル システムからインポートします。 • **https: —** https: ファイル システムからインポートします。 • **null: —** null: ファイル システムからインポートします。 • **nvram: —** nvram: ファイル システムからインポートします。 • **rcp: —** rcp: ファイル システムからインポートします。 • **scp: —** scp: ファイル システムからインポートします。 • **system: —** system: ファイル システムからインポートします。 • **tftp: —** tftp: ファイル システムからインポートします。
exportable	（任意）鍵のエクスポートが可能であることを指定します。
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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

パス フレーズには空白および句読点を含む任意の句が使用できますが、疑問符（**?**）は使用できません。疑問符は、Cisco IOS のパーサーにとって特別な意味を持ちます。

パス フレーズ保護により、パス フレーズと鍵が関連付けられます。鍵は、エクスポート時にパス フレーズを使用して暗号化されます。インポート時には、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

次に、PEM 形式の RSA 鍵を外部システムからインポートする例と、PEM 形式の RSA 鍵を WebVPN サービス モジュールにエクスポートする例を示します。

```
wwbvpn(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.

wwbvpn(config)#
```

crypto pki authenticate

Certificate Authority（CA; 認証局）の公開鍵が格納された証明書を取得するには、**crypto pki authenticate** コマンドを使用します。

crypto pki authenticate *trustpoint-label*

シンタックスの説明

trustpoint-label	トラストポイント ラベルの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

trustpoint-label 引数では、大文字と小文字が区別されます。

トラストポイントごとに、CA の公開鍵が格納された証明書を取得する必要があります。複数のトラストポイントで同じ CA を使用できます。

（注） CA に問い合わせて、証明書の正しいフィンガープリントを取得し、コンソールに表示されるフィンガープリントを検証します。

例

次に、CA の証明書を取得する例を示します。

```
webvpn(config)# crypto pki authenticate PROXY1
Certificate has the following attributes:
Fingerprint: A8D09689 74FB6587 02BFE0DC 2200B38A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
webvpn(config)# end
webvpn#
```

crypto pki certificate

WebVPN サービス モジュールで PKI 実装を設定して定義するには、**crypto pki certificate** コマンドを使用します。

crypto pki certificate {chain *name* **| map** *map_name* **| query | validate** *trustpoint-label***}**

シンタックスの説明

chain	証明書を指定します。
name	Certificate Authority（CA; 認証局）サーバ名
map	証明書の属性マップを定義します。
map_name	CA マップ タグ名
query	リブートのあとに CA から証明書を取得します。
validate	証明書チェーンを検証します。
trustpoint-label	トラストポイント ラベル名

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

crypto pki certificate chain コマンドは、証明書チェーン コンフィギュレーション モードを開始します。証明書チェーン コンフィギュレーション モードでは、証明書のコマンドを使用して証明書を削除できます。証明書を削除するには、証明書チェーン コンフィギュレーション モードを開始している必要があります。

crypto pki certificate validate コマンドは、任意のトラストポイントに対するルータ独自の証明書を検証します。このコマンドを登録後の健全性チェックとして使用して、トラストポイントが正常に認証されていること、トラストポイントの証明書が要求され、認可されていること、証明書が現在有効であることを検証します。証明書が有効である場合とは、証明書がトラストポイントの CA によって署名されている場合、期限が切れていない場合などが含まれます。

crypto pki crl request

WebVPN サービス モジュールで PKI 実装を設定して定義するには、**crypto pki crl request** コマンドを使用します。

crypto pki crl request *name*

シンタックスの説明

name	Certificate Authority（CA; 認証局）の名前を指定します。この名前は、**crypto pki trustpoint** コマンドで CA を宣言したときに使用した名前と同じものです。

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CRL には、無効になっているネットワーク デバイスの証明書がすべて表示されています。モジュールは無効になっている証明書を引き受けないので、無効になっている証明書を持つ IP Security（IPSec）デバイスはモジュールと IPSec トラフィックを交換できません。

モジュールは、ピアから証明書を受信する初回時に、CA から CRL をダウンロードします。モジュールは、ピアの証明書が無効になっていないことを確認するために、CRL をチェックします（CRL にピアの証明書が登録されていた場合、モジュールは証明書を受け入れないため、ピアは認証されません）。

CRL は、期限満了までその後の認証にも使用されます。当該の CRL の期限が満了したあとにモジュールがピアの証明書を受信した場合、モジュールは新しい CRL をダウンロードします。

モジュールの CRL の期限が満了していない場合でも、その CRL の内容が古い可能性がある場合は、**crypto pki crl request** コマンドを使用して、ただちに最新の CRL をダウンロードし、古い CRL と置き換えてください。

このコマンドは、コンフィギュレーションには保存されません。

例

次に、各要求に対してタイムアウトを秒単位で指定する例を示します。

```
wwbvpn(config)# crypto pki crl request
```

crypto pki enroll

トラストポイントの証明書を要求するには、**crypto pki enroll** コマンドを使用します。

crypto pki enroll *trustpoint-label*

シンタックスの説明

trustpoint-label	トラストポイント ラベルの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

trustpoint-label 引数では、大文字と小文字が区別されます。

各トラストポイントに対して、Certificate Authority（CA; 認証局）からの署名付き証明書を取得する必要があります。

コンフィギュレーションに保存されないチャレンジ パスワードを作成するオプションが用意されています。証明書を無効にする必要がある場合にこのパスワードが必要なので、このパスワードは忘れないようにしてください。

（注） **crypto pki enroll** コマンドを入力したあと、証明書を受信する前にモジュールまたはスイッチがリブートした場合は、コマンドを再入力して、CA 管理者に通知する必要があります。

例

次に、証明書を要求する例を示します。

```
webvpn(config)# crypto pki enroll PROXY1
%
% Start certificate enrollment..

% The subject name in the certificate will be: C=US; ST=California; L=San Jose;
O=Cisco; OU=Lab; CN=host1.cisco.com
% The subject name in the certificate will be: host.cisco.com
% The serial number in the certificate will be: 00000000
% The IP address in the certificate is 10.0.0.1

% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
Fingerprint:  470DE382 65D8156B 0F84C2AF 4538B913

webvpn(config)# end
```

crypto pki export pem

WebVPN 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 pki export pem** コマンドを使用します。

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

シンタックスの説明

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 DES-CBC 暗号化アルゴリズムを指定します。
3des	168 ビット DES（3DES）暗号化アルゴリズムを指定します。
url *url*	URL ロケーションを指定します。*url* の有効値は次のとおりです。 • **archive: —** archive: ファイル システムにエクスポートします。 • **flash: —** flash: ファイル システムにエクスポートします。 • **ftp: —** ftp: ファイル システムにエクスポートします。 • **http: —** http: ファイル システムにエクスポートします。 • **https: —** https: ファイル システムにエクスポートします。 • **null: —** null: ファイル システムにエクスポートします。 • **nvram: —** nvram: ファイル システムにエクスポートします。 • **rcp: —** rcp: ファイル システムにエクスポートします。 • **scp: —** scp: ファイル システムにエクスポートします。 • **system: —** system: ファイル システムにエクスポートします。 • **tftp: —** tftp: ファイル システムにエクスポートします。
pass-phrase	秘密鍵を保護するために使用するパス フレーズ

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

pass_phrase には空白および句読点を含む任意の句が使用できますが、疑問符（**?**）は使用できません。疑問符は、Cisco IOS のパーサーにとって特別な意味を持ちます。

パス フレーズ保護により、パス フレーズと鍵が関連付けられます。鍵は、エクスポート時にパス フレーズを使用して暗号化されます。インポート時には、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。

エクスポート不可の表示がある鍵はエクスポートできません。

デフォルトのファイル拡張子はプロンプトで変更できます。デフォルトのファイル拡張子は次のとおりです。

- 公開鍵（.pub）
- 秘密鍵（.prv）

- 証明書（.crt）
- CA 証明書（.ca）
- シグニチャ鍵（-sign）
- 暗号化鍵（-encr）

例

次に、WebVPN サービス モジュール上の PEM 形式のファイルをエクスポートする例を示します。

```
wwbvpn(config)# crypto pki export TP5 pem url tftp://10.1.1.1/TP5 password
```

関連コマンド

crypto pki import pem

crypto pki export pkcs12

WebVPN 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 pki export pkcs12** コマンドを使用します。

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

シンタックスの説明

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。*file_system* の有効値は次のとおりです。 **archive: —** archive: ファイル システムにエクスポートします。 **cns: —** cns: ファイル システムにエクスポートします。 **flash: —** flash: ファイル システムにエクスポートします。 **ftp: —** ftp: ファイル システムにエクスポートします。 **http: —** http: ファイル システムにエクスポートします。 **https: —** https: ファイル システムにエクスポートします。 **null: —** null: ファイル システムにエクスポートします。 **nvram: —** nvram: ファイル システムにエクスポートします。 **rcp: —** rcp: ファイル システムにエクスポートします。 **scp: —** scp: ファイル システムにエクスポートします。 **system: —** system: ファイル システムにエクスポートします。 **terminal —** PKCS12 ファイルを端末に出力します。 **tftp: —** tftp: ファイル システムにエクスポートします。
pkcs12_filename	（任意）インポートする PKCS12 ファイルの名前を指定します。
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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

インポートした鍵ペアはエクスポートできません。

SSH を使用している場合、PKCS12 ファイルをエクスポートする際には Secure File Transfer（SCP）の使用を推奨します。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 値を指定しない場合は、デフォルトのファイル名（*trustpoint_label* 値）を受け入れるか、ファイル名を入力するかを確認するプロンプトが表示されます。**ftp:** または **tftp:** 値には、*pkcs12_filename* 値の完全なパスを含めます。

間違ったパス フレーズを入力すると、エラーを受信します。

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

例

次に、SCP を使用して PKCS12 ファイルをエクスポートする例を示します。

```
wwbvpn(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.
wwbvpn(config)#
```

crypto pki import pem

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

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

シンタックスの説明

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鍵を指定します。
terminal	端末上に要求を表示します。
url *url*	URL ロケーションを指定します。*url* の有効値は次のとおりです。 • **archive: —** archive: ファイル システムからインポートします。 • **flash: —** flash: ファイル システムからインポートします。 • **ftp: —** ftp: ファイル システムからインポートします。 • **http: —** http: ファイル システムからインポートします。 • **https: —** https: ファイル システムからインポートします。 • **null: —** null: ファイル システムからインポートします。 • **nvram: —** nvram: ファイル システムからインポートします。 • **rcp: —** rcp: ファイル システムからインポートします。 • **scp: —** scp: ファイル システムからインポートします。 • **system: —** system: ファイル システムからインポートします。 • **tftp: —** tftp: ファイル システムからインポートします。
usage-keys	汎用の鍵ペアを 1 組生成するのではなく、特殊な用途の鍵ペアを 2 組生成するように指定します。
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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

間違ったパス フレーズを入力すると、エラーを受信します。パス フレーズには空白および句読点を含む任意の句が使用できますが、疑問符（**?**）は使用できません。疑問符は、Cisco IOS のパーサーにとって特別な意味を持ちます。

パス フレーズ保護により、パス フレーズと鍵が関連付けられます。鍵は、エクスポート時にパス フレーズを使用して暗号化されます。インポート時には、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 鍵をインポートする場合は、公開鍵または対応する証明書が使用できます。

crypto ca import pem コマンドでインポートできるのは、秘密鍵（.prv）、サーバ証明書（.crt）、発行者 Certificate Authority（CA; 認証局）証明書（.ca）だけです。証明書チェーンに複数レベルの CA がある場合は、このコマンドが認証で使用される前に、ルートおよび下位 CA 証明書をインポートする必要があります。カット & ペースト機能または TFTP を使用して、ルートおよび下位 CA 証明書をインポートしてください。

例

次に、WebVPN 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例を示します。

```
wwbvpn(config)# crypto pki 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.
wwbvpn(config)# end
webvpn#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

関連コマンド

crypto pki export pem

crypto pki import pkcs12

WebVPN サービス モジュールに PKCS12 ファイルをインポートするには、**crypto ca import pkcs12** コマンドを使用します。

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

シンタックスの説明

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。*file_system* の有効値は次のとおりです。 **archive: —** archive: ファイル システムにエクスポートします。 **cns: —** cns: ファイル システムにエクスポートします。 **flash: —** flash: ファイル システムにエクスポートします。 **ftp: —** ftp: ファイル システムにエクスポートします。 **http: —** http: ファイル システムにエクスポートします。 **https: —** https: ファイル システムにエクスポートします。 **null: —** null: ファイル システムにエクスポートします。 **nvram: —** nvram: ファイル システムにエクスポートします。 **rcp: —** rcp: ファイル システムにエクスポートします。 **scp: —** scp: ファイル システムにエクスポートします。 **system: —** system: ファイル システムにエクスポートします。 **terminal —** PKCS12 ファイルを端末に出力します。 **tftp: —** tftp: ファイル システムにエクスポートします。
pkcs12_filename	（任意）インポートする PKCS12 ファイルの名前を指定します。
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がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

SSH を使用している場合、PKCS12 ファイルをインポートする際には Secure File Transfer（SCP）の使用を推奨します。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 値を指定しない場合は、デフォルトのファイル名（*trustpoint_label* 値）を受け入れるか、ファイル名を入力するかを確認するプロンプトが表示されます。**ftp:** または **tftp:** 値には、*pkcs12_filename* 値の完全なパスを含めます。

間違ったパス フレーズを入力すると、エラーを受信します。

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

例

次に、SCP を使用して PKCS12 ファイルをインポートする例を示します。

```
wwbvpn(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
!
wwbvpn(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
wwbvpn(config)#
```

crypto pki profile enrollment

登録プロファイルを定義するには、グローバル コンフィギュレーション モードで **crypto pki profile enrollment** コマンドを使用します。この登録プロファイルに関連付けられたすべての情報を削除するには、このコマンドの **no** 形式を使用します。

crypto pki profile enrollment *label*

シンタックスの説明

label	証明書の登録プロファイル タグ

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

crypto pki profile enrollment コマンドを入力したあと、次のいずれかのコマンドを使用してプロファイル パラメータを定義できます。

- **authentication command —** 認証用に Certificate Authority（CA; 認証局）に送信される HTTP コマンドを指定します。
- **authentication terminal —** カット & ペーストによる手動での証明書認証要求を指定します。
- **authentication url —** 認証要求を送信する CA サーバの URL を指定します。
- **enrollment command —** 登録用に CA に送信される HTTP コマンドを指定します。
- **enrollment terminal —** カット & ペーストによる手動での証明書登録を指定します。
- **enrollment url —** 登録要求を送信する CA サーバの URL を指定します。
- **parameter —** 登録プロファイルのパラメータを指定します。このコマンドは、authentication command または enrollment command が使用されている場合にのみ使用できます。

（注）　authentication url、enrollment url、authentication terminal、および enrollment terminal のコマンドを使用すると、証明書の認証および登録に対してさまざまな方法（TFTP 認証や手動による登録など）を指定できます。

例

次に、各要求に対してタイムアウトを秒単位で指定する例を示します。

```
webvpn(config)# crypto pki profile enrollment test
webvpn(ca-profile-enroll)#
```

crypto pki trustpoint

Certificate Authority（CA; 認証局）トラストポイントのコンフィギュレーション サブモードを開始して、CA トラストポイントを定義するには、**crypto pki trustpoint** コマンドを使用します。WebVPN サブコマンド モードで入力したコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

crypto pki trustpoint *trustpoint-label*

no crypto pki trustpoint *trustpoint-label*

シンタックスの説明

trustpoint-label	（任意）トラストポイント ラベルの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

trustpoint-label 引数では、大文字と小文字が区別されます。

crypto pki trustpoint コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(ca-trustpoint)#
```

ca-trustpoint サブモードを開始した場合、次のコマンドを使用して CA トラストポイントを設定できます。表 2-1 に、ca-trustpoint サブモード コマンドを示します。

表 2-1　CA トラストポイント サブモード コマンド

コマンド	目的および注意事項	デフォルト
authorization {**list** *listname* | **username** **{subjectname** *subjectname*}}	許可パラメータは次のとおりです。 **list** *listname* **—** AAA 許可リストを指定します。 **username subjectname** *subjectname* **—** AAA ユーザ名の作成に使用する各証明書フィールドのパラメータを設定します。 AAA ユーザ名として使用可能なオプションは次のとおりです。 • **commonname —** 証明書の通常名 • **country —** 証明書の国 • **email —** 証明書の E メール • **ipaddress —** 証明書の IP アドレス • **locality —** 証明書の地域 • **organization —** 証明書の組織 • **organizationalunit —** 証明書の組織ユニット • **postalcode —** 証明書の郵便番号 • **serialnumber —** 証明書のシリアル番号 • **state —** 証明書の州 • **streetaddress —** 証明書の所在地 • **title —** 証明書のタイトル • **unstructuredname —** 証明書の非公式名	
auto-enroll [[*value*] **regenerate**]]	このルータの ID を自動登録します。 **regenerate —** （任意）名前付きの鍵がすでに存在している場合でも、証明書の新しい鍵が生成されます。 *value* の有効値は 1 ～ 100 です。	
crl query *url*		
default	コマンドをデフォルトに設定します。	

表 2-1　CA トラストポイント サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
enrollment [**http-proxy**][**mode ra**] [**retry** {**period** *minutes* | **count** *count*}] **url** *url*	CA の登録パラメータを次のように指定します。 • **http-proxy —** 登録用の HTTP プロキシ サーバ • **mode ra —** Registration Authority（RA; 登録局）モード • **retry count** *count* **—** CA に、証明書に関してポーリングを実行する回数。*count* の有効値は 1 ～ 100 です。 • **retry period** *minutes* **—** CA に対する証明書の要求間隔。*minutes* の有効値は 1 ～ 60 です。 • **url** *url* **—** URL または次のいずれかを指定します。 － **archive: —** archive: ファイル システムを使用して登録します。 － **flash: —** flash: ファイル システムを使用して登録します。 － **ftp: —** ftp: ファイル システムを使用して登録します。 － **http: —** http: ファイル システムを使用して登録します。 － **https: —** https: ファイル システムを使用して登録します。 － **null: —** null: ファイル システムを使用して登録します。 － **nvram: —** nvram: ファイル システムを使用して登録します。 － **rcp: —** rcp: ファイル システムを使用して登録します。 － **scp: —** scp: ファイル システムを使用して登録します。 － **system: —** system: ファイル システムを使用して登録します。 － **tftp: —** tftp: ファイル システムを使用して登録します。	**period** *minutes* **—** 1 **count** *count* **—** 10
exit	ca-trustpoint コンフィギュレーション モードを終了します。	
fqdn {*fqdn* | **none**}	Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用します。 *fqdn* **—** FQDN を入力します。 **none —** FQDN を使用しません。	
ip-address *server-ip-addr*	（任意）この証明書を使用する WebVPN ゲートウェイの IP アドレスを指定します。	

表 2-1　CA トラストポイント サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
match certificate *map_name* [**map** | **override** | **skip**]	**crypto pki certificate map** コマンドで定義した証明書ベース Access Control List（ACL; アクセス制御リスト）を関連付けます。 *map_name* **—** 事前に定義された **crypto pki certificate map** *map_name* コマンドに指定されている *map_name* 引数を照合します。 **allow —** 期限切れの証明書が受け入れられるようにします。 **override —** 証明書のフィールドを無効にします。 **skip —** 証明書の妥当性チェックを省略します。	
no	コマンドを無効にするか、またはデフォルトに設定します。	
ocsp url *url*	Online Certificate Status Protocol（OCSP）パラメータを入力します。 *url* **—** 指定された HTTP URL の OCSP サーバで、設定されたトラストポイントに関連付けられたすべての証明書を確認します。	
password *password*	（任意）チャレンジ パスワードを設定します。	
primary	トラストポイントをプライマリに指定します。	
query certificate	指定したトラストポイントのクエリー モードをオンにして、証明書がローカルに保存されず、リモート サーバから取得されるようにします。	
rsakeypair *key-label*	証明書に関連付ける鍵ペアを指定します。	
regenerate	再登録時に鍵を再生成します。	
revocation-check {**crl** | **none** | **ocsp**}	（任意）このトラストポイントに関連付けられた証明書を検証するときに、トラストポイントが Certificate Revocation List（CRL; 証明書失効リスト）を調べる方法を指定します。 **crl —** CRL による失効チェック **none —** 失効チェックを無視 **ocsp —** OCSP による失効チェック	
root tftp *hostname filename*	TFTP プロトコルを定義して、所定の CA のルート証明書を取得します。このコマンドを使用すると、認証されたルート証明書を TFTP サーバにファイルとして保存できます。	
serial-number [**none**]	シリアル番号を使用するかどうかを指定します。	使用しない
show	このルータのトラストポイントを表示します。	
source interface *interface-name*	トラストポイントに対応付けられたすべての発信 TCP 接続の送信元アドレスとして使用されるインターフェイスのアドレスを指定します。 *interface-name* **—** 送信元アドレスとして使用されるインターフェイス アドレス	
subject-name *line*	（任意）WebVPN ゲートウェイのホスト名を設定します。	

表 2-1　CA トラストポイント サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
usage {**ike** | **ssl-client** | **ssl-server**}	（任意）証明書の使用目的を指定します。	
vrf *vrf*	CRL の登録および取得に使用する VPN Routing/Forwarding instance（VRF; VPN ルーティング / 転送インスタンス）名	

各証明書に対して、モジュールが使用するトラストポイントを 1 つ設定する必要があります。

trustpoint-label 値は鍵の *key-label* 値と一致させます。ただし、これは必須ではありません。

この証明書で使用される WebVPN ゲートウェイの IP アドレスを指定すると、一部の Web ブラウザでは SSL サーバ証明書内の IP アドレスと、URL に含まれる IP アドレスを比較します。これらの IP アドレスが一致しない場合、ブラウザは、この証明書を受け入れるかまたは拒否するかをクライアントに確認するダイアログボックスを表示することがあります。

subject-name *line* 値を指定する場合、次の注意事項に従ってください。

- **subject-name** コマンドは Lightweight Directory Access Protocol（LDAP）形式を使用します。
- 件名に指定された引数にカンマが含まれる場合は、引用符で囲む必要があります。たとえば、**O="Cisco, Inc."** のようになります。
- 一部のブラウザでは、SSL サーバ証明書の件名の Common Name（CN; 通常名）フィールドと、URL に含まれるホスト名を比較します。これらの名前が一致しない場合、ブラウザは、この証明書を受け入れるかまたは拒否するかをクライアントに確認するダイアログボックスを表示することがあります。また、証明書に CN フィールドが定義されていない場合、一部のブラウザは SSL セッションの確立を拒否して、セッションを閉じます。

例

次に、トラストポイント PROXY1 を設定して、接続を検証する例を示します。

```
webvpn(config)# crypto pki trustpoint PROXY1
webvpn(ca-trustpoint)# rsakeypair PROXY1
webvpn(ca-trustpoint)# enrollment url http://exampleCA.cisco.com
webvpn(ca-trustpoint)# ip-address 10.0.0.1
webvpn(ca-trustpoint)# password password
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# subject-name C=US; ST=California; L=San Jose; O=Cisco; OU=Lab;
CN=host1.cisco.com
webvpn(ca-trustpoint)# end
webvpn# ping example.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
webvpn#
```

debug webvpn

各システム コンポーネントのデバッグ フラグをオンにするには、**debug webvpn** コマンドを使用します。デバッグ フラグをオフにするには、このコマンドの **no** 形式を使用します。

debug webvpn [**aaa** | **cifs** | **citrix** | **cookie** | **csd** | **dns** | **emweb** | **http** | **package** | **platform** [*type*] | **port-forward** | **sock** | **timer** | **trie** | **tunnel** | **webservice**]

シンタックスの説明

aaa	WebVPN AAA のデバッグをイネーブルにします。
cifs	WebVPN CIFS をイネーブルにします。
citrix	WebVPN Citrix のデバッグをイネーブルにします。
cookie	WebVPN クッキーのデバッグをイネーブルにします。
csd	Cisco Secure Desktop（CSD）のデバッグをイネーブルにします。
dns	DNS のデバッグをイネーブルにします。
emweb	EmWeb のデバッグをイネーブルにします。
http	HTTP のデバッグをイネーブルにします。
package	パッケージのデバッグをイネーブルにします。
platform *type*	**platform** *type* オプションについては、「使用上のガイドライン」を参照してください。
port-forward	ポートフォワーディングのデバッグをイネーブルにします。
sock	Socks のデバッグをイネーブルにします。
timer	タイマーのデバッグをイネーブルにします。
trie	トライのデバッグをイネーブルにします。
tunnel	トンネルのデバッグをイネーブルにします。
webservice	Web サービスのデバッグ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がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	Citrix および CSD のデバッグが追加されました。
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

（注）　以下に示すオプションに関し、**module** *module* の有効値は次のとおりです。

- **fdu —** FDU CPU
- **ssl1 —** SSL1 CPU
- **tcp1 —** TCP1 CPU
- **tcp2 —** TCP2 CPU

platform *type* には次のオプションがあります。

platform app には次の値を使用できます。
- **app** [**module** [*module*]] **—** アプリケーションの記録層
- **hdr** [**module** [*module*]] **—** アプリケーションへの HTTP ヘッダー挿入
- **module** [*module*] **—** デバッグ対象のモジュール
- **url** [**module** [*module*]] **—** アプリケーションの URL の書き換え

platform app-driver には次の値を使用できます。
- **dispatch —** ディスパッチ イベント
- **error —** エラー イベント
- **event** {**app** | **next-hop** | **tcp**} **—** イベント デバッギング
- **fsm —** FSM
- **mc —** マルチコア イベント

platform content には次の値を使用できます。
- **detail** [**module** [*module*]] **—** コンテントの詳細
- **error** [**module** [*module*]] **—** コンテント エラー
- **ipc** [**module** [*module*]] **—** コンテント IPC
- **module** [*module*] **—** デバッグ対象のモジュール
- **rewriting** [**module** [*module*]] **—** コンテントの書き換え
- **scanning** [**module** [*module*]] **—** コンテントのスキャン

platform fdu には次の値を使用できます。
- **cli** [**module** [*module*]] **—** FDU CLI
- **hash** [**module** [*module*]] **—** FDU ハッシュ
- **ipc** [**module** [*module*]] **—** FDU IPC
- **module** [*module*] **—** デバッグ対象のモジュール
- **trace** [**module** [*module*]] **—** FDU トレース

platform flash には次の値を使用できます。
- **module** [*module*] **—** デバッグ対象のモジュール

platform ipc には次の値を使用できます。
- **module** [*module*] **—** デバッグ対象のモジュール

platform pc には次の値を使用できます。
- **module** [*module*] **—** デバッグ対象のモジュール

platform pki には次の値を使用できます。
- **auth —** 証明書の認証および許可
- **ca-pool —** CA プール
- **cert —** 証明書管理
- **events —** イベント
- **history —** 証明書履歴
- **ipc —** IPC メッセージおよびバッファ
- **key —** 鍵管理

platform remote には次の値を使用できます。
- **loop** *count* [**module** [*module*]] **—** リモート デバッグ。count の有効値は 1 ～ 65535 です。
- **module** [*module*] **—** デバッグ対象のモジュール

platform ssl キーワードには次の値を使用できます。

- **alert** [**module** [*module*]] **—** SSL アラート イベント
- **error** [**module** [*module*]] **—** SSL エラー イベント
- **handshake** [**module** [*module*]] **—** SSL ハンドシェイク イベント
- **module** [*module*] **—** デバッグ対象のモジュール
- **pkt** [**module** [*module*]] **—** 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、負荷がほとんどまたはまったくない状態（仮想サーバまたは実サーバとの接続がまったく確立されていない場合など）に、基本的な接続の問題のトラブルシューティングを行う場合のみ使用してください。

TCP デバッグ コマンドを使用すると、TCP モジュールはコンソールにデバッグ情報を大量に表示するため、モジュールのパフォーマンスが大幅に低下することがあります。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、およびステート移行の処理に遅延が生じます。

platform tcp キーワードには次の値を使用できます。

- **events** [**module** [*module*]] **—** TCP イベントをデバッグします。
- **module** [*module*] **—** デバッグ対象のモジュール
- **pkt** [**module** [*module*]] **—** 送受信された TCP パケットをデバッグします。
- **state** [**module** [*module*]] **—** TCP ステートをデバッグします。
- **timers** [**module** [*module*]] **—** TCP タイマーをデバッグします。

platform tunnel キーワードには次の値を使用できます。

- **hash —** トンネル ハッシュ エントリ
- **trace —** トンネル接続のトレース パケット

例

次に、トンネル デバッギングをオンにする例を示します。

```
webvpn# debug webvpn tunnel
webvpn#
```

次に、App デバッギングをオンにする例を示します。

```
webvpn# debug webvpn platform app
webvpn#
```

次に、FDU デバッギングをオンにする例を示します。

```
webvpn# debug webvpn platform fdu
webvpn#
```

次に、IPC デバッギングをオンにする例を示します。

```
webvpn# debug webvpn platform ipc
webvpn#
```

次に、PKI デバッギングをオンにする例を示します。

```
webvpn# debug webvpn platform pki
webvpn#
```

次に、SSL デバッギングをオンにする例を示します。

```
ssl-proxy# debug webvpn platform ssl
ssl-proxy#
```

次に、TCP デバッギングをオンにする例を示します。

```
ssl-proxy# debug webvpn platform tcp
ssl-proxy#
```

次に、TCP デバッギングをオフにする例を示します。

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

do

グローバル コンフィギュレーション モード、他のコンフィギュレーション モード、またはサブモードで 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*

シンタックスの説明

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がありません。

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 モード、他のコンフィギュレーション モード、またはサブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

注意　EXEC モードで **do** コマンドを入力しないでください。サービスが中断される可能性があります。

do コマンドを使用して、**configure terminal** コマンドを実行することはできません。**configure terminal** コマンドを入力すると、コンフィギュレーション モードにモード変更されるためです。

グローバル コンフィギュレーション モード、他のコンフィギュレーション モード、またはサブモードで、**copy** または **write** コマンドを実行するために、**do** コマンドを使用することはできません。

例

次に、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例を示します。

```
wwbvpn(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
.
.
.
wwbvpn(config)#
```

nbns-list

nbnslist サブモードを開始して、NetBIOS Name Service（NBNS）サーバを設定するには、**nbns-list** コマンドを使用します。コンフィギュレーションから指定したリストを削除するには、このコマンドの **no** 形式を使用します。

nbns-list *name*

no nbns-list *name*

シンタックスの説明

name	NBNS リストの名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

WebVPN コンテキスト サブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

listname 引数では、大文字と小文字が区別され、最大長は 64 文字です。

nbns-list コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-nbnslist)#
```

nbnslist サブモードを開始した場合、次のコマンドを使用して NBNS サーバを設定できます。表 2-2 に、nbnslist サブモード コマンドを示します。

表 2-2　nbnslist サブモード コマンド

コマンド	目的および注意事項	デフォルト
nbns-server *ip_addr* [**master**] [**timeout** *timeout*][**retry** *retries*]	Common Internet File System（CIFS）名前解決用の NBNS リストとサーバ アドレスを指定します。最大 3 つのサーバを設定できます。 （注）　Linux 実行環境の Windows 2000 および Samba サーバだけでサポートされています。 *ip_addrs* 値は、Windows ネットワークの Primary Domain Controller（PDC）を指定します。 **master** キーワードは、マスター ブラウザであることを指定します。Windows Internet Naming Service（WINS）サーバの場合は、master キーワードを入力しないでください。 *timeout* 値は、クエリーを次のサーバに送信するまでの、NBNS クエリーの応答を待機する初期時間（秒単位）を指定します。デフォルトのタイムアウト値は 2 秒です。範囲は 1 ～ 30 です。 *retries* 値は、設定したサーバに NBNS クエリーを再送信する回数を指定します。この値は、エラーを返すまでに、リスト内のすべてのサーバへの再試行を繰り返す回数を示します。デフォルトの再試行値は 2 です。範囲は 0 ～ 10 です。	タイムアウトは 2 秒です。 再試行は 2 回です。
exit	コンテキスト サブモードに戻ります。	

例

次に、nbnslist サブモードを開始して、NBNS リストとサーバ アドレスを設定する例を示します。

```
webvpn(config)# webvpn context c1
webvpn(config-webvpn-context)# nbns-list list2
webvpn(config-webvpn-nbnslist)# nbns-server 10.1.1.2
webvpn(config-webvpn-nbnslist)# exit
webvpn(config-webvpn-context)#
```

関連コマンド

webvpn context

policy group

グループ ポリシーを定義して、グループ ポリシー サブモードを開始するには、コンテキスト サブコマンド モードで **policy group** コマンドを使用します。WebVPN サブコマンド モードで入力したコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

policy group *group-policy-name*

no policy group *group-policy-name*

シンタックスの説明

group-policy-name	グループ ポリシーの名前

デフォルト

サブモード コマンドのデフォルトについては、「使用上のガイドライン」を参照してください。

コマンド モード

WebVPN コンテキスト サブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	Citrix をイネーブルまたはディセーブルにするコマンドが追加されました。
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

group-policy-name 引数では、大文字と小文字が区別されます。

webvpn policy group コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-group)#
```

グループ ポリシー サブモードを開始した場合、次のコマンドを使用してグループ ポリシー テンプレートを設定できます。表 2-3 に、グループ ポリシー サブモード コマンドを示します。

表 2-3　グループ ポリシー コマンド

コマンド	目的および注意事項	デフォルト
banner value *string*	ユーザまたはグループのバナー ストリングを指定します。*string* 値には、7 ビット ASCII 値、HTML タグ、エスケープ シーケンスを使用できます。このストリングは、ログインのあとに表示されます。	ストリングは指定されていません。
citrix enabled	Citrix 機能をイネーブルにします。	Citrix はディセーブルです。
exit	グループ ポリシー コンフィギュレーション モードを終了します。	
filter tunnel {*ip-acl* | *ip-expanded-acl* | *name*}	トンネルに固有のアクセス リストを定義します。 • *ip-acl* — IP アクセス リスト（標準または拡張）。有効値は 1 ～ 199 です。 • *ip-expanded-acl* — IP 拡張アクセス リスト（標準または拡張）。有効値は 1300 ～ 2699 です。 • *name* — アクセス リスト名	名前は指定されていません。

表 2-3　グループ ポリシー コマンド（続き）

コマンド	目的および注意事項	デフォルト
functions {**file-access** | **file-browse** | **file-entry**| **svc-enabled**| **svc-required**}	ファイル機能を次のように指定します。 （注）　**file-browse** または **file-entry** をイネーブルにする前に、**file-access** をイネーブルにする必要があります。 • **file-access** — ユーザはホーム ページに表示されているファイル サーバにアクセスできます。 • **file-browse** — ユーザはファイル サーバを閲覧できます。このオプションをディセーブルにすると、ファイル サーバへのアクセスが拒否されます。 • **file-entry** — ユーザはファイル サーバのファイルを変更できます。 • **svc-enabled** — ユーザ グループがトンネル モードを使用できます。エンド ユーザ PC への SVC のインストールが失敗した場合、エンド ユーザはクライアントレス モードまたはシンクライアント モードを使用し続けることができます。 • **svc-required** — 常にトンネル モードが使用されます。エンド ユーザ PC への SVC のインストールが失敗した場合、エンド ユーザは他のモードを使用することができません。	すべての値はディセーブルです。
hide-url-bar	ポータル ページの URL バーをディセーブルにします。 （注）　このコマンドは、クライアントレス モードにのみ適用されます。	
nbns-list *name*	コンテキスト コンフィギュレーションに定義されている CIFS の NBNS リストを指定します。 Windows 2000 サーバおよび Linux/UNIX でのみサポートされています。 （注）　このコマンドは、クライアントレス モードにのみ適用されます。	
no	コマンドを無効にするか、またはデフォルトに設定します。	
port-forward *name*	コンテキスト コンフィギュレーションに定義されているポートフォワーディングのリストを指定します。コマンドを再入力すると、以前の設定が無効になります。デフォルトでは、リストが指定されません。 （注）　このコマンドは、シンクライアント モードにのみ適用されます。	リストは指定されていません。ポートフォワーディングはディセーブルです。
timeout {**idle** | **session**} *seconds*	エンド ユーザのアイドル タイムアウト値とユーザまたはグループ セッションの最大タイムアウト値を指定します。 **idle** *seconds* — エンド ユーザの非アクティビティ時間を指定します。アイドル タイムアウトの有効値は 0（ディセーブル）～ 3600 秒です。 **session** *seconds* — アクティビティに関係なく、合計セッション時間を指定します。セッション タイムアウトの有効値は 1 ～ 1209600 秒です。	**idle** *seconds* — 2100 秒（35 分） **session** *seconds* — 43200 秒（12 時間）

表 2-3　グループ ポリシー コマンド（続き）

コマンド	目的および注意事項	デフォルト
svc	トンネルの設定を指定します。詳細については、**svc** コマンドを参照してください。	
url-list *name*	コンテキスト コンフィギュレーションに定義されている URL リストを指定します。コマンドを再入力すると、以前の設定が無効になります。 **（注）** このコマンドは、クライアントレス モードにのみ適用されます。	リストは指定されていません。

例

次に、WebVPN コンテキストと WebVPN グループ ポリシーを設定する例を示します。

```
webvpn(config)# webvpn context cisco
webvpn(config-webvpn-context)# policy group cisco_tunl
webvpn(config-webvpn-group)# function svc-enabled
webvpn(config-webvpn-group)# timeout idle 36000
webvpn(config-webvpn-group)# timeout session 144000
webvpn(config-webvpn-group)# svc address-pool "cisco_tunl_pool"
webvpn(config-webvpn-group)# svc keep-client-installed
webvpn(config-webvpn-group)# svc rekey time 40000
webvpn(config-webvpn-group)# svc rekey method new-tunnel
webvpn(config-webvpn-group)# svc dpd-interval gateway 0
webvpn(config-webvpn-group)# svc dpd-interval client 300
webvpn(config-webvpn-group)# exit
webvpn(config-webvpn-context)#
```

port-forward

ポートフォワーディング サブモードを開始して、ポートフォワーディング エントリを設定するには、**port-forward** コマンドを使用します。コンフィギュレーションから所定のリストを削除するには、このコマンドの **no** 形式を使用します。

port-forward *listname*

no port-forward *listname*

シンタックスの説明

listname	転送されるポートのリスト名

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

WebVPN コンテキスト サブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

listname 引数では、大文字と小文字が区別され、最大長は 64 文字です。

port-forward コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-port-fwd)#
```

ポートフォワーディング サブモードを開始した場合、次のコマンドを使用してポートフォワーディング サービスを設定できます。表 2-4 に、ポートフォワーディング サブモード コマンドを示します。

表 2-4　ポートフォワーディング サブモード コマンド

コマンド	目的および注意事項	デフォルト
default local-port *port-number*	デフォルトのローカル ポートを指定します。有効値は 1 ～ 65535 です。	
exit	WebVPN ポートフォワーディング サブモードを終了して、WebVPN コンテキスト サブモードに戻ります。	
local *localport*	待ち受けるローカル ポートを指定します。*localport* 値は、所定のリスト名内で 1 回だけ使用できます。有効値は 1 ～ 65535 です。ローカル ポートを指定した場合、次のキーワードと引数を使用できます。 • **remote-server** *remoteserver* — リモート サーバ上で接続する DNS 名または IP アドレスを指定します。 • **remote-port** *remoteport* — リモート サーバ上で接続するポートを指定します。有効値は 1 ～ 65535 です。 • **description** *description* — エンド ユーザのアプレット ウィンドウに表示するアプリケーション名または簡単な説明を指定します。*description* 値の最大長は、64 文字です。	
no	一致する行をコンフィギュレーションから削除します。	

所定の *listname* 値に複数のエントリを指定できます。ユーザ名またはグループ ポリシーに適用されるリストにポートフォワーディング エントリをグルーピングするために、*listname* 値が使用されます。

no を指定すると、コンフィギュレーションから一致する行が削除されます。リモート サーバとリモート ポートを含める必要はありません。

例

次に、ポートフォワーディング サブモードを開始して、ポートフォワーディング エントリを設定する例を示します。

```
webvpn(config-webvpn-context)# port-forward abc
webvpn(config-webvpn-port-fwd)# local-port 25 remote-server "mailman" remote-port 25
description "SMTP server"
webvpn(config-webvpn-port-fwd)# local-port 110 remote-server "pop3-ny" remote-port 110
description "POP3-server"
webvpn(config-webvpn-port-fwd)# local-port 143 remote-server "imap-ny" remote-port 143
description "IMAP server"
webvpn(config-webvpn-port-fwd)#
```

関連コマンド

url-list
webvpn context

show webvpn context

特定のコンテキストの情報を表示するには、**show webvpn context** コマンドを使用します。

show webvpn context *name*

シンタックスの説明

name	コンテキストの名前を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、ソフトウェア強制リセットに関する情報を収集する例を示します。

```
webvpn# show webvpn context tunnel

Admin Status: up
Operation Status: up
CSD Status: Enabled
TCP Policy not configured
SSL Policy not configured
Certificate authentication type: peer certificate is always accepted
AAA Authentication List: webvpn
AAA Authentication Domain not configured
Default Group Policy: tunnel
Associated WebVPN Gateway: s2
Domain Name and Virtual Host not configured
Maximum Users Allowed: 2560
Maximum Concurrent Logins Allowed: 0 (default)
NAT Address Range: 10.81.12.4-10.81.12.9 mask 255.255.255.0
VRF Name not configured

webvpn#
```

show webvpn dispatch

WebVPN ディスパッチ情報を表示するには、**show webvpn dispatch** コマンドを使用します。

show webvpn dispatch {**algorithm** | **member** | **stats**}

シンタックスの説明

algorithm	現在の Content Load Balancing（CLB）アルゴリズムを表示します。
member	CLB メンバー テーブルの情報を表示します。
stats	ディスパッチ統計情報を表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN ディスパッチ統計情報を表示する例を示します。

```
webvpn# show webvpn dispatch stat
SSLVPN: Dispatching Statistics:
--------------------------------
  Total packets dispatched = 2827
  Total packets need multiple buffers = 12
  Total packets with no core id = 93
  Total packets with embedded core id = 2722
  Per Core Dispatching Statistics:
  --------------------------------
                      Assigned
  Core-ID Symbolic-ID Connections
  ------- ----------- -----------
    1     SwCidIos          43
    7     SwCidVpn1         51
```

次に、現在の CLB アルゴリズムを表示する例を示します。

```
webvpn# show webvpn dispatch algorithm
SSLVPN: Current CLB algorithm:
-------------------------------
   Weighted Round Robin (Master Weight = 5 Slave Weight = 6)
```

次に、CLB メンバー テーブルの情報を表示する例を示します。

```
webvpn# show webvpn dispatch member
SSLVPN: CLB Member Table
(Current RR Index 1):
Member-Index  Core-ID  Symbolic-ID  Weight  Quota
------------  -------  -----------  ------  -----
    0           1        SwCidIos      5     3
    1           7        SwCidVpn1     6     2

webvpn#
```

show webvpn gateway

ゲートウェイの情報を表示するには、**show webvpn gateway** コマンドを使用します。

show webvpn gateway [*name*]

シンタックスの説明

name	（任意）ゲートウェイの名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、すべてのゲートウェイの情報を表示する例を示します。

```
webvpn# show webvpn gateway

Gateway Name                    Admin  Operation
------------                    -----  ---------
s1                              up     up
s2                              up     up
gateway1                        down   down
tunnel                          down   down
```

次に、特定のゲートウェイの情報を表示する例を示します。

```
webvpn# show webvpn gateway s1
Admin Status: up
Operation Status: up
IP: 10.1.2.140, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp1
  Certificate chain for new connections:
    Certificate:
       Key Label: tp1, 1024-bit, not exportable
       Key Timestamp: 12:09:27 UTC Dec 25 2004
       Serial Number: 0FE5
    Root CA Certificate:
       Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete
```

show webvpn log-level

現在の WebVPN ログ レベルの情報を表示するには、**show webvpn log-level** コマンドを使用します。

show webvpn log-level

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、現在のログ レベルを表示する例を示します。

```
webvpn# show webvpn log-level
The current SSLVPN log level is "Normal"
```

show webvpn nbns

WebVPN NetBIOS Name Service（NBNS）キャッシュの情報を表示するには、**show webvpn nbns** コマンドを使用します。

show webvpn nbns context {*name* | **all**}

シンタックスの説明

name	コンテキストの名前
all	すべてのコンテキストの情報を表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、指定したコンテキストの NBNS キャッシュに関するステータス情報を表示する例を示します。

```
webvpn# show web nbns context tunnel
NetBIOS name        IP Address       Timestamp

0 total entries
webvpn#
```

次に、すべてのコンテキストの NBNS キャッシュに関するステータス情報を表示する例を示します。

```
webvpn# show web nbns context all
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
webvpn#
```

show webvpn package

インストールされた WebVPN ファイルとパッケージの情報を表示するには、**show webvpn package** コマンドを使用します。

show webvpn package {**csd** | **svc**} [{**file** *filename* | **status**}]

シンタックスの説明

csd	Cisco Secure Desktop（CSD）を指定します。
svc	SSL VPN Client（SVC）を指定します。
file	（任意）ファイルの内容を表示します。
filename	（任意）ファイルの名前
status	（任意）パッケージのステータスを表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	このコマンドの構文が **show webvpn install** から **show webvpn package** に変更されました。
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、SVC に関するステータス情報を表示する例を示します。

```
webvpn# show web package svc status
SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,1,1
Tue 04/08/2005 15:31:20.43
```

次に、SVC パッケージに含まれるファイルに関する情報を表示する例を示します。

```
webvpn# show web package svc
SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 164216
File: \webvpn\stc\1\binaries\stc.exe, size: 90104
File: \webvpn\stc\1\binaries\stcjava.cab, size: 6154
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4053
File: \webvpn\stc\1\binaries\stcweb.cab, size: 12668
File: \webvpn\stc\1\binaries\update.txt, size: 9
File: \webvpn\stc\1\empty.html, size: 214
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

次に、CSD パッケージに関するステータス情報を表示する例を示します。

```
webvpn# show webvpn package csd status
SSLVPN Package Cisco-Secure-Desktop version installed:
CISCO CSD CAT6K
3,1,0,18
Mon 09/12/2005 11:58:25.31 p
```

次に、CSD パッケージに含まれるファイルに関する情報を表示する例を示します。

```
webvpn# show webvpn package csd
SSLVPN Package Cisco-Secure-Desktop installed:
File: \sdesktop\data.xml, size: 54
File: \sdesktop\globals.js, size: 587
File: \sdesktop\install\binaries\InfoExtr.exe, size: 53248
File: \sdesktop\install\binaries\InfoExtr.exp, size: 2159
File: \sdesktop\install\binaries\InfoExtr.lib, size: 4298
File: \sdesktop\install\binaries\Logging.exe, size: 24576
File: \sdesktop\install\binaries\cache.jar, size: 4385
File: \sdesktop\install\binaries\cachedlg.zip, size: 63190
File: \sdesktop\install\binaries\cleaner.cab, size: 167847
File: \sdesktop\install\binaries\detectvm.class, size: 555
File: \sdesktop\install\binaries\inst.exe, size: 96256
File: \sdesktop\install\binaries\instfull.exe, size: 681472
File: \sdesktop\install\binaries\instjava.cab, size: 7804
File: \sdesktop\install\binaries\instjava.jar, size: 4643
File: \sdesktop\install\binaries\instweb.cab, size: 14379
File: \sdesktop\install\binaries\java.htm, size: 328
File: \sdesktop\install\binaries\java2.htm, size: 659
File: \sdesktop\install\binaries\main.js, size: 18206
File: \sdesktop\install\binaries\ocx.htm, size: 245
File: \sdesktop\install\binaries\setup.cab, size: 418780
File: \sdesktop\install\binaries\update.txt, size: 8
File: \sdesktop\install\empty.htm, size: 155
File: \sdesktop\install\help\ccml\index.htm, size: 2736
File: \sdesktop\install\help\ccml\yes.gif, size: 3250
File: \sdesktop\install\help\ccw\index.htm, size: 3653
File: \sdesktop\install\help\ccw\taskbar.gif, size: 136
File: \sdesktop\install\help\ccw\yes.gif, size: 3250
File: \sdesktop\install\help\sd\index.htm, size: 6695
...
(テキスト出力は省略)
...
File: \sdesktop\manager\js\xtree.js, size: 24087
File: \sdesktop\manager\main.htm, size: 62436
File: \sdesktop\manager\template.xml, size: 2741
File: \sdesktop\manager\xlat.txt, size: 1284
File: \sdesktop\version.txt, size: 55
Total files: 83
```

次に、特定のファイルの内容を表示する例を示します。

```
webvpn# show webvpn package csd file \sdesktop\version.txt
SSLVPN File \sdesktop\version.txt installed:
CISCO CSD CAT6K
3,1,0,18
Mon 09/12/2005 11:58:25.31
webvpn#
```

show webvpn platform buffers

TCP バッファの使用状況に関する情報を表示するには、**show webvpn platform buffers** コマンドを使用します。

show webvpn platform buffers [**module** *module*]

シンタックスの説明

module *module*	（任意）*module* の有効値は次のとおりです。 **all** — すべての CPU **fdu** — FDU CPU **ssl1** — SSL1 CPU **tcp1** — TCP1 CPU

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、TCP サブシステムのバッファの使用状況と他の情報を表示する例を示します。

```
webvpn# show webvpn platform buffers module all
Buffers info for TCP module 1
    TCP data buffers used 3340 limit 88064
    TCP ingress buffer pool size 44032 egress buffer pool size 44032
    TCP ingress data buffers min-thresh 5636096 max-thresh 9017344
    TCP ingress data buffers used Current 0 Max 27
    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 115
    Conns consuming egress data buffers 0
    In-sequence queue bufs 0 OOO bufs 0
    Per-flow avg qlen 0 Global avg qlen 0
webvpn#
```

関連コマンド

webvpn policy tcp

show webvpn platform context

WebVPN コンテキストの情報を表示するには、**show webvpn platform context** コマンドを使用します。

show webvpn platform context *name* [**module** *module*]

シンタックスの説明

name	コンテキストの名前
module *module*	（任意）*module* の有効値は次のとおりです。 **all —** すべての CPU **fdu —** FDU CPU **ssl1 —** SSL1 CPU **tcp1 —** TCP1 CPU **tcp2 —** TCP2 CPU

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、指定したコンテキストに関するステータス情報を表示する例を示します。

```
webvpn# show webvpn platform context tunnel
Certificate authentication type: peer certificate is always accepted
Admin Status: up
Operation Status: up
webvpn#
```

次に、指定したコンテキストに関するすべてのモジュールのステータス情報を表示する例を示します。

```
webvpn# show webvpn platform context tunnel module all
FDU Service Entry
    Service ID   : 8               Protocol     : 0
    Virtual IP   : 0.0.0.0    Virtual port : 0
    HTTP-redirect: 0

    Hash Index   : 0               Conn Count   : 0
    Bound ID     : 0               State        : DOWN
Service ID 8
  IP address : 116.117.110.110 Port : 0
  MSS : 1460
  SYN timeout (s): 75
  Idle timeout (s) : 600
  FIN wait timeout (s) : 75
  Reassembly timeout (s) : 60
  Connection Rx Buffer Size : 32768
  Connection Tx Buffer Size : 65536
  TOS Carryover Disabled

Service entry in cpu 1:
    Cipher suites: 0xF
    Versions: 0x3
    Options: 0x6
    Current Certificate Index:  0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 0 location:   0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 1 location:   0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Flags: 0x202
    Handshake timeout: 0 secs
    Session timeout: 0 secs
    Session cache size: 262144
```

show webvpn platform crash-info

WebVPN サービス モジュールからソフトウェア強制リセットに関する情報を収集するには、**show webvpn platform crash-info** コマンドを使用します。

show webvpn platform crash-info [**brief** | **details**]

シンタックスの説明

brief	(任意) プロセッサ レジスタのみに関する、ソフトウェア強制リセット情報のごく一部分を収集します。
details	(任意) ソフトウェア強制リセット情報をすべてまとめて収集します。例外および割り込みスタックのダンプを含みます (印刷が終了するまで 10 分程度かかることがあります)。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、ソフトウェア強制リセット情報をごく一部だけ収集する例を示します。

```
webvpn# show webvpn platform crash-info brief

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


------------- COMPLEX 0 [VPN_IOS] ----------------------

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

++++++++++ CORE 0 (VPN (slave)) ++++++++++++++++++++++++

   HW_CID: 0
   APPLICATION VERSION: SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(7.11
)VA(0.117)  INTERIM SOFTWARE \nCompiled Wed 13-Apr-05 02:20 by integ
   APPROXIMATE TIME WHEN CRASH HAPPENED: 02:56:38 UTC Sep 1 2005
   THIS CORE DIDN'T CRASH
   TRACEBACK: 374110 375C0C
   CPU CONTEXT  ----------------------------

$0 : 00000000, AT : 01050000, v0 : 00000000, v1 : 01050000
a0 : 0104F3E0, a1 : 0208A390, a2 : 00000000, a3 : 00000000
t0 : 00000000, t1 : 032B8BC8, t2 : 00000001, t3 : FFFF00FF
t4 : 00368100, t5 : 74696F6E, t6 : 00000000, t7 : 39353438
s0 : 01050000, s1 : 01051F40, s2 : 028E16E0, s3 : 00BA0000
s4 : 00BA0000, s5 : 00BA0000, s6 : 01050000, s7 : 01050000
t8 : 0D0D0D0D, t9 : 00000000, k0 : 00400001, k1 : 00000000
gp : 00FC65E0, sp : 028E16D0, s8 : 00000000, ra : 00374160
LO : F88923EA, HI : DA46BB94, BADVADDR : B60ED79D
EPC : 00374110, ErrorEPC : BFC00C70, SREG : 3400FD03
Cause 00004000 (Code 0x0): Interrupt exception
```

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

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


++++++++++ CORE 1 (IOS (master)) ++++++++++++++++++++++++

   HW_CID: 1
   APPLICATION VERSION: SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(7.11
)VA(0.117)  INTERIM SOFTWARE \nCompiled Wed 13-Apr-05 02:51 by integ
   APPROXIMATE TIME WHEN CRASH HAPPENED: 02:56:36 UTC Sep 1 2005
   THIS CORE CRASHED
   TRACEBACK: 1C6C7EC 1CC1B20 1CBEC14 1CBEDA8 1CC16EC 1CC1E7C 1CC96C4 1CC9930 1C
C94DC 1CCA570 1CBDF58 1CB69FC 1CB1898 1C7F964 1CE3618 1CE431C
   CPU CONTEXT  ----------------------------

$0 : 00000000, AT : 021D0000, v0 : 00000001, v1 : 00000000
a0 : 0CFA6952, a1 : 00000000, a2 : 00000002, a3 : 00000062
t0 : 00000001, t1 : 00000000, t2 : 00000001, t3 : 00000062
t4 : 00000048, t5 : 0A0D0A0D, t6 : 0A0D0A0A, t7 : 090A0A0A
s0 : 00000000, s1 : 0CFA6950, s2 : 0D583008, s3 : 0CFA6950
s4 : 0CFA6953, s5 : 02270000, s6 : 17394FC8, s7 : 0D4708B8
t8 : 00000005, t9 : 00000001, k0 : 00000000, k1 : 00000000
gp : 021D4080, sp : 0CCE3840, s8 : FFFFFFFF, ra : 01CC1B20
LO : 00000003, HI : 0238A2C0, BADVADDR : 00000000
EPC : 01C6C7EC, ErrorEPC : 01572900, SREG : 3400FD03
Cause 0000000C (Code 0x3): TLB (store) exception

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

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

------------- COMPLEX 1 [FDU_TCP_SSL_1] ----------------------

NVRAM CHKSUM: 0x3C34
NVRAM MAGIC: 0xC8A514F0
NVRAM VERSION: 1

++++++++++ CORE 0 (TCP/FDU Processor #1) ++++++++++++++++++++++++

   HW_CID: 2
   APPLICATION VERSION: 2005.03.15 22:14:57 built for mahesh
   APPROXIMATE TIME WHEN CRASH HAPPENED: 11:28:14 UTC Aug 1 2005
   THIS CORE CRASHED
   TRACEBACK: 20A994 20B000 243C54 2444C8 24FF90 21A088 219970 2263B0 2523FC
   CPU CONTEXT  ----------------------------

$0 : 00000000, AT : 00270000, v0 : 0000005C, v1 : 00285760
a0 : 12630E54, a1 : 00000000, a2 : 00000000, a3 : 00000000
t0 : 00000000, t1 : 34007E01, t2 : 34007100, t3 : FFFF00FF
t4 : 0020A9C0, t5 : 82602460, t6 : 00000002, t7 : 00000001
s0 : 12630E54, s1 : 002824DC, s2 : 12630C5C, s3 : 12630C5C
s4 : 002E0000, s5 : 00000003, s6 : 12630C20, s7 : 0026B258
t8 : FFFFFFFF, t9 : 0160A2A0, k0 : 00400001, k1 : 00000000
gp : 00273320, sp : 09DFFD40, s8 : 12630C20, ra : 0020B000
LO : 00000000, HI : 0000004E, BADVADDR : 12630E54
EPC : 0020A994, ErrorEPC : F7EF23EA, SREG : 34007E03
Cause 00008014 (Code 0x5): Address Error (store) exception

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

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

```
++++++++++ CORE 1 (SSL Processor #1) ++++++++++++++++++++++++

   HW_CID: 3
   APPLICATION VERSION: 2005.03.15 22:14:57 built for mahesh
   APPROXIMATE TIME WHEN CRASH HAPPENED: 11:28:14 UTC Aug 1 2005
   THIS CORE DIDN'T CRASH
   TRACEBACK: 449F70 433458 42D0A0 422694
   CPU CONTEXT  ----------------------------

$0 : 00000000, AT : 00490000, v0 : 00000000, v1 : 0E1743D8
a0 : 09E0A534, a1 : 00000002, a2 : 00000002, a3 : 00000002
t0 : 00006100, t1 : 00000000, t2 : B0060100, t3 : FFFF00FF
t4 : 0040A9C0, t5 : A295B1CD, t6 : B22AEDDB, t7 : F9D0B2AC
s0 : 09E0A4E8, s1 : 0048F698, s2 : 00000000, s3 : 0048F600
s4 : 00000000, s5 : 00000000, s6 : 00480000, s7 : 00480000
t8 : 00000002, t9 : 00000001, k0 : 00000000, k1 : 00000000
gp : 004965E0, sp : 123FFF30, s8 : 00000001, ra : 00433458
LO : 999999C9, HI : 0000001F, BADVADDR : 644E427A
EPC : 00449F70, ErrorEPC : FFDF6777, SREG : 34007E03
Cause 0000C000 (Code 0x0): Interrupt exception

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

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



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

show webvpn platform gateway

WebVPN のゲートウェイ情報を表示するには、**show webvpn platform gateway** コマンドを使用します。

show webvpn platform gateway *name* [**debug** | **module** *module*]

シンタックスの説明

name	ゲートウェイの名前
debug	（任意）ゲートウェイのデバッグ情報を表示します。
module *module*	（任意）*module* の有効値は次のとおりです。 **all —** すべての CPU **fdu —** FDU CPU **ssl1 —** SSL1 CPU **tcp1 —** TCP1 CPU **tcp2 —** TCP2 CPU

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、特定のゲートウェイのステータス情報を表示する例を示します。

```
webvpn# show webvpn platform gateway tunnel
IP: 10.1.2.14, port: 443
rsa-general-purpose certificate trustpoint: mytp
  Certificate chain for new connections:
    Certificate:
       Key Label: mytp, 1024-bit, not exportable
       Key Timestamp: 12:09:27 UTC Dec 25 2004
       Serial Number: 0FE5
    Root CA Certificate:
       Serial Number: 01
  Certificate chain complete
Admin Status: up
Operation Status: up
webvpn#
```

次に、特定のゲートウェイのデバッグ情報を表示する例を示します。

```
webvpn# show webvpn platform gateway s1 debug
IP: 10.1.2.14, port: 443
rsa-general-purpose certificate trustpoint: mytp
  Certificate chain for new connections:
    Certificate:
       Key Label: mytp, 1024-bit, not exportable
       Key Timestamp: 12:09:27 UTC Dec 25 2004
       Serial Number: 0FE5
    Root CA Certificate:
       Serial Number: 01
  Certificate chain complete
Admin Status: up
Operation Status: up

Service ID: 1        Bound  ID: -1
Virtual IP: 10.1.2.14             Port     : 443
VLAN ID   : 0          MAC Address : 0000.0000.0000
State     : PROXY VALID
Enabled   : Yes
Secondary : No
Client NAT: disable
Server NAT: disable
webvpn#
```

次に、特定のゲートウェイの全 CPU に関するステータス情報を表示する例を示します。

```
webvpn# show web platform gateway s1 module all
FDU Service Entry
    Service ID   : 1               Protocol     : 6
    Virtual IP   : 64.102.223.140    Virtual port : 443
    HTTP-redirect: 0

    Hash Index   : 896             Conn Count   : 0
    Bound ID     : -1              State        : UP
Service ID 1
  IP address : 10.1.2.14 Port : 443
  MSS : 1460
  SYN timeout (s): 75
  Idle timeout (s) : 600
  FIN wait timeout (s) : 75
  Reassembly timeout (s) : 60
  Connection Rx Buffer Size : 32768
  Connection Tx Buffer Size : 65536
  TOS Carryover Disabled

Service entry in cpu 1:
    Cipher suites: 0xF
    Versions: 0x3
    Options: 0x6
    Current Certificate Index:  0x0 0x1 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 0 location:   0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 1 location:   0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Flags: 0x201
    Handshake timeout: 0 secs
    Session timeout: 0 secs
    Session cache size: 262144

webvpn#
```

show webvpn platform license

現在のライセンス レベルを表示するには、**show webvpn platform license** コマンドを使用します。

show webvpn platform license

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN サービス モジュールの各種のライセンスに対する現在のライセンス レベルを表示する例を示します。

- 8000 ユーザの場合

```
webvpn# show webvpn platform licnese
MaxUsers:8000
Type:Permanent
```

- 5000 ユーザの場合

```
webvpn# show webvpn platform license
MaxUsers:5000
Type:Permanent
```

- 2560 ユーザの場合

```
MaxUsers:2560
Type:Permanent
```

- デモ ライセンスの場合

```
webvpn# show webvpn platform license
MaxUsers:8000
Type:Demo(expiring in 30 days ..)
```

たとえば、デモ ライセンスの場合、Type フィールドではライセンスの期限が切れるまでの日数をカウント ダウンします。

```
Type:Demo(expiring in 29 days ..)

Type:Demo(Expired) System restored to previous levels (2560/5000)
```

show webvpn platform mac address

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

show webvpn platform mac address

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN サービス モジュールで使用されている現在の MAC アドレスを表示する例を示します。

```
webvpn# show webvpn platform mac address
SVCWEBVPN module MAC address: 000d.29f0.c24c

webvpn#
```

show webvpn platform policy

SSL または TCP ポリシーの情報を表示するには、**show webvpn platform policy** コマンドを使用します。

show webvpn platform policy {**ssl** | **tcp**} *name*

シンタックスの説明

ssl	SSL ポリシーを指定します。
tcp	TCP ポリシーを指定します。
name	SSL または TCP ポリシーの名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN サービス モジュールの SSL ポリシーの情報を表示する例を示します。

```
webvpn# show webvpn platform policy ssl
SSL Policy Name                              Usage-Count

webvpn#
```

show webvpn platform version

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

show webvpn platform version

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN サービス モジュールで現在実行されているイメージ バージョンを表示する例を示します。

```
webvpn# show webvpn platform version
Cisco IOS Software, SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(8)VA(1.1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 26-May-05 02:44 by integ

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

webvpn-alpha uptime is 5 days, 19 hours, 51 minutes
System returned to ROM by power-on
System image file is "tftp://10.1.1.1/unknown"
AP Version 1.1(0.97)

webvpn#
```

show webvpn platform vlan

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

show webvpn platform vlan [*vlan-id*]

シンタックスの説明

vlan-id	（任意）VLAN ID。特定の VLAN の情報を表示します。有効値は 2 ～ 1005 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、WebVPN サービス モジュールに設定されているすべての VLAN を表示する例を示します。

```
webvpn# show webvpn platform vlan
Vlan-id  IP address      NetMask          VRF
-------  ----------      -------          ------
10       10.81.12.3      255.255.255.0    -
20       20.102.223.139  255.255.255.248  -
```

次に、WebVPN サービス モジュールの特定の VLAN に関する情報を表示する例を示します。

```
webvpn# show webvpn platform vlan 10
Vlan-id  IP address      NetMask          VRF
-------  ----------      -------          ------
10       10.81.12.3      255.255.255.0    -
------ FDU module info ----
FDU Vlan Entry
    VLAN ID        : 10
    My IP Addr     : 10.81.12.3
    My Net Mask    : 255.255.255.0
    VRF ID         : 0
```

show webvpn policy

設定された WebVPN ポリシーを表示するには、**show webvpn policy** コマンドを使用します。

show webvpn policy {**group** *name* **context** *name* | **tcp** [*name*] | **ssl** [*name*]}

シンタックスの説明

group *name* **context** *name*	指定されたコンテキストのグループ 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。
ssl	設定された SSL 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がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、HTTP ヘッダー ポリシーに関する情報を表示する例を示します。

```
webvpn# show web policy group tunnel context tunnel
WEBVPN: group policy = tunnel ; context = tunnel
      idle timeout = 2100 sec
      session timeout = 43200 sec
      functions = svc-enabled
      citrix disabled
      address pool name = "addr"
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 43200 sec
      DNS primary server = 64.102.6.247
      WINS primary server = 171.68.235.228

webvpn#
```

関連コマンド

webvpn policy ssl
webvpn policy tcp

show webvpn session

WebVPN セッションに関する情報を表示するには、**show webvpn session** コマンドを使用します。

show webvpn session {**context** {*name* | **all**} | **user** *name* **context** {*name* | **all**}}

シンタックスの説明

context *name*	コンテキスト名を指定します。
user *name*	ユーザ名を指定します。
all	すべてのコンテキストを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、指定したコンテキストに関するセッション情報を表示する例を示します。

```
webvpn# show webvpn session context ssl-vpn
WebVPN context name: ssl-vpn
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.2.1.220                2         04:47:16  00:01:26
user2              10.2.1.221                2         04:48:36  00:01:56
```

次に、特定のユーザのセッション情報を表示する例を示します。

```
webvpn# show webvpn session user user1 context all
WWebVPN user name = user1 ; IP address = 10.2.1.220; context = ssl-vpn
    No of connections: 0
    Created 00:00:19, Last-used 00:00:18
    CSD enabled
    CSD Session Policy
       CSD Web Browsing Allowed
       CSD Port Forwarding Allowed
       CSD Full Tunneling Disabled
       CSD FILE Access Allowed
    User Policy Parameters
      Group name = ssl-vpn
    Group Policy Parameters
      url list name = "cisco"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "email"
      tunnel mode = disabled
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep stc installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 3600 sec
```

show webvpn stats

統計情報のカウンタに関する情報を表示するには、**show webvpn stats** コマンドを使用します。

show webvpn stats [*type*]

シンタックスの説明

type	（任意）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がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	Citrix 固有の統計情報を表示する **citrix** オプションが追加されました。 HTTP 認証の統計情報を表示する **httpauth** オプションが追加されました。
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

type の有効なオプションは次のとおりです。

- **cifs** [**detail**][**context** {*name* | **all**}]
- **citrix**
- **context** {*name* | **all**}
- **detail** [**context** {*name* | **all**}]
- **httpauth**
- **mangle** [**detail**][**context** {*name* | **all**}]
- **port-forward** [**detail**][**context** {*name* | **all**}]
- **socket** [**detail**][**context** {*name* | **all**}]
- **tunnel** [**detail**][**context** {*name* | **all**}]

例

次に、WebVPN サービス モジュールで収集されるすべての統計情報のカウンタを表示する例を示します。

```
webvpn# show webvpn stats
User session statistics:
    Active user sessions     : 1          AAA pending reqs          : 0
    Peak user sessions       : 6          Peak time                 : 17:22:16
    Active user TCP conns    : 2          Terminated user sessions : 29
    Session alloc failures   : 0          Authentication failures  : 3
    VPN session timeout      : 1          VPN idle timeout          : 9
    User cleared VPN sessions: 0          Exceeded ctx user limit   : 0
    Exceeded total user limit: 0

Mangling statistics:
    Relative urls            : 15705      Absolute urls             : 41850
    Non-http(s) absolute urls: 9306       Non-standard path urls    : 1005
    Interesting tags         : 200329     Uninteresting tags        : 398899
    Interesting attributes   : 164642     Uninteresting attributes : 272669
    Embedded script statement: 10226      Embedded style statement : 2800
    Inline scripts           : 34868      Inline styles             : 26475
    HTML comments            : 6018       HTTP/1.0 requests         : 148
    HTTP/1.1 requests        : 8115       Unknown HTTP version      : 0
    GET requests             : 6290       POST requests             : 95
    CONNECT requests         : 0          Other request methods     : 1878
    Through requests         : 6172       Gateway requests          : 2091
    Pipelined requests       : 7          Req with header size >1K : 1
    Processed req hdr bytes  : 5320280    Processed req body bytes : 529871
    HTTP/1.0 responses       : 797        HTTP/1.1 responses        : 6277
    HTML responses           : 1919       CSS responses             : 80
    XML responses            : 2476       JS responses              : 171
    Other content type resp  : 1435       Chunked encoding resp     : 1926
    Resp with encoded content: 0          Resp with content length : 3926
    Close after response     : 1222       Resp with header size >1K: 0
    Processed resp hdr size  : 1870948    Processed resp body bytes: 65670616
    Backend https response   : 245        Chunked encoding requests: 0

HTTP Authentication stats :
    Successful NTLM Auth     : 0          Failed NTLM Auth          : 0
    Successful Basic Auth    : 1          Failed Basic Auth         : 1
    Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
    NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
    Oversize NTLM Type3 cred : 0          Internal Error            : 0
    Num 401 responses        : 3          Num non-401 responses     : 97
    Num Basic forms served   : 2          Num NTLM forms served     : 0
    Num Basic Auth sent      : 3          Num NTLM Auth sent        : 0

Admission Control stats :
    Users Denied             : 0          Requests Dropped          : 0
    CPU util exceeded        : 0          Memory util exceeded      : 0
    Appl Buf util exceeded   : 0
CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                  : 0
    Active VC's              : 0          Active Contexts           : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies              : 0
    NB DGM Requests          : 0          NB DGM Replies            : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  SMB related Global:
    Sessions in use          : 0          Mbufs in use              : 0
    Mbuf Chains in use       : 0          Active VC's               : 0
    Active Contexts          : 0          Browse Errors             : 0
    Empty Browser List       : 0          NetServEnum Errors        : 0
    Empty Server List        : 0          NBNS Config Errors        : 0
    NetShareEnum Errors      : 0
  HTTP related Per Context:
    Requests                 : 24         Request Bytes RX          : 8508
    Request Packets RX       : 0          Response Bytes TX         : 1465966
```

```
    Response Packets TX      : 975        Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0
  HTTP related Global:
    Server User data         : 0          CIFS User data           : 0
    Net Handles              : 0          Active CIFS context      : 0
    Authentication Fails     : 0          Operations Aborted       : 0
    Timers Expired           : 0          Pending Close            : 0
    Net Handles Pending SMB  : 0          File Open Fails          : 0
    Browse Network Ops       : 0          Browse Network Fails     : 0
    Browse Domain Ops        : 0          Browse Domain Fails      : 0
    Browse Server Ops        : 0          Browse Server Fails      : 0
    Browse Share Ops         : 0          Browse Share Fails       : 0
    Browse Dir Ops           : 0          Browse Network Fails     : 0
    File Read Ops            : 0          File Read Fails          : 0
    File Write Ops           : 0          File Write Fails         : 0
    Folder Create Ops        : 0          Folder Create Fails      : 0
    File Delete Ops          : 0          File Delete Fails        : 0
    File Rename Ops          : 0          File Rename Fails        : 0

Socket statistics:
    Sockets in use           : 2          Sock Usr Blocks in use   : 2
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 2          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 49         Sock Tx Unblocked        : 49
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 5

Port Forward statistics:
  Client                                 Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0

WEBVPN Citrix statistics:

               Client                    Server
  Packets in   : 0                        0
  Packets out  : 0                        0
  Bytes in     : 0                        0
  Bytes out    : 0                        0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 1          Peak time                : 5d16h
    Connect succeed          : 6          Connect failed           : 0
    Reconnect succeed        : 1          Reconnect failed         : 0
    DPD timeout              : 0
  Client                                 Server
    in  CSTP frames          : 23098      out IP pkts              : 23093
    in  CSTP data            : 23093
    in  CSTP control         : 5
    in  CSTP bytes           : 4956832    out IP bytes             : 4771852
    out CSTP frames          : 32086      in  IP pkts              : 32084
    out CSTP data            : 32084
    out CSTP control         : 2
    out CSTP bytes           : 16136526   in  IP bytes             : 16512477
```

ほとんどのカウンタは文字通りの意味です。以下に、内容がわかりにくいカウンタの説明を示します。

- ユーザ セッションの統計情報（User session statistics）
  - Terminated user sessions ― 最後に **clear** キーワードが実行されてからログアウトしたセッション数
  - Session alloc failures ― システムのメモリ不足を表示

- Authentication failures — 指定されたユーザ名またはパスワードに対して AAA（認証、許可、アカウンティング）からエラー ステータスが返された回数
- VPN session timeout — セッション タイムアウトが発生したためにクリアされたセッション数
- VPN idle timeout — アイドル タイムアウトが発生したためにクリアされたセッション数
- User cleared vpn sessions — **clear webvpn session** コマンドによってクリアされたセッション数
- Exceeded ctx user limit — コンテキストに設定された最大ユーザ数を超えたために拒否されたセッション数
- Exceeded total user limit — システムの最大ユーザ数（現在 8000）を超えたために拒否されたセッション数

• マングリングの統計情報（Mangling statistics）

- Close after response — コンテント長が不足しているために応答の送信後に閉じられた接続数

• CIFS の統計情報（CIFS statistics）

- コンテキスト単位の SMB 関連カウンタ

  TCP/UDP VCs — この時点までに正常に確立されたバックエンド TCP/UDP 接続数

  Active VCs — 現在アクティブな TCP/UDP 接続数

  Active Contexts — 現在アクティブな SMB コンテキスト数

  Aborted Conns — ピアによって打ち切られた TCP 接続数

- コンテキスト単位の NetBIOS 関連カウンタ

  Name Queries — 送信された NBNS 名クエリー数

  Name Query Replies — 受信された NBNS 名クエリーの応答数。一致しない場合、ブラウザ、PDC、およびサーバにアクセスできなかったことを示します。

  NBDGM requests — 送信された NB データグラム サービス関連のゲット バックアップ ブラウザ リストのクエリー数

  NBDGM replies — 受信された NB データグラム サービス関連のゲット バックアップ ブラウザ リストの応答数。要求と応答が一致しない場合、ドメイン ブラウズが機能していないことを示します。

  NB TCP connect fails — 失敗した NB TCP 接続の回数。PDC とファイル サーバの接続機能に問題があることを示します。

- すべてのコンテキストに対する SMB 関連カウンタ

  Sessions in Use — 使用中（アクティブな）バックエンド SMB セッション数

  Mbufs in use — 使用中のアプリケーション バッファ記述子の数

  Mbuf Chains in use — 使用中のアプリケーション バッファ数

  Active VCs — システム内のアクティブなバックエンド SMB 接続の合計数

  Active Context — システム内のアクティブなバックエンド SMB コンテキストの合計数

  Browse Errors — ドメイン ブラウズに失敗した回数

  Empty Browse list — 空のバックアップ ブラウズ リストの応答が受信された回数

  NetServEnum errors — 特定のドメインでサーバ リストの受信に失敗した回数

  NetShareEnum errors — 特定の共有領域でファイルとフォルダのリストの受信に失敗した回数を示します。

- コンテキスト単位の HTTP 関連カウンタ

  Active Connections — CIFS 要求が処理されている接続数

  Active CIFS Context — CIFS 要求が処理されている CIFS アプリケーション モジュール コンテキスト数

- すべてのコンテキストに対する HTTP 関連カウンタ

  Server User Data — 各サーバのユーザ名およびパスワード キャッシュのエントリ数

  CIFS User Data — デフォルトのユーザ名とパスワード キャッシュのエントリ数

  Net Handles — システム内の合計接続数（アクティブおよびアイドル状態の接続）

  Active CIFS context — アクティブな CIFS アプリケーション モジュール コンテキストのグローバル カウント

  Authentication fails — WebVPN クッキーを使用しないか、または期限切れの WebVPN クッキーを使用して処理された CIFS HTTP 要求の数

  Operations Aborted — HTTP 接続が切断したために打ち切られたバックエンド操作の数。CIFS トランザクションが正常に完了しないことを示します。

  Pending Close — 終了を保留にし、保留中のデータの送信を再開して終了するのを待機している数

- ソケットの統計情報（Socket statistics）
  - Tx Blocked — アプリケーションの送信が TCP 輻輳制御によってブロックされた回数
  - Tx Unblocked — TCP 輻輳制御によってブロックされた後、アプリケーションの送信を再開した回数。十分な時間が経ってからも Tx Blocked と Tx Unblocked が一致しない場合は、トランザクションが停止しています。
  - Rx Blocked — アプリケーションが TCP 層から送信されるデータの受信をブロックした回数。これは、アプリケーション バッファが不足しているか、処理の限界であることを示します。
  - Rx Unblocked — アプリケーションが TCP 層から送信されるデータの受信を再開した回数。十分な時間が経ってからも Rx Blocked と Rx Unblocked が一致しない場合は、トランザクションが停止しています。
  - Premature Close — 接続が確立される前にアプリケーションが接続を閉じた回数
  - Select Timeouts — 要求および応答の交換に対する応答を待機している間、または TCP 接続が確立されるのを待機している間にアプリケーションがタイムアウトした回数

次に、WebVPN サービス モジュールの CIFS の統計情報を表示する例を示します。

```
webvpn# show webvpn stats cifs
CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies             : 0
    NB DGM Requests          : 0          NB DGM Replies           : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  SMB related Global:
    Sessions in use          : 0          Mbufs in use             : 0
    Mbuf Chains in use       : 0          Active VC's              : 0
    Active Contexts          : 0          Browse Errors            : 0
    Empty Browser List       : 0          NetServEnum Errors       : 0
    Empty Server List        : 0          NBNS Config Errors       : 0
    NetShareEnum Errors      : 0
  HTTP related Per Context:
    Requests                 : 24         Request Bytes RX         : 8508
    Request Packets RX       : 0          Response Bytes TX        : 1465966
    Response Packets TX      : 975        Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0
  HTTP related Global:
    Server User data         : 0          CIFS User data           : 0
    Net Handles              : 0          Active CIFS context      : 0
    Authentication Fails     : 0          Operations Aborted       : 0
    Timers Expired           : 0          Pending Close            : 0
    Net Handles Pending SMB  : 0          File Open Fails          : 0
    Browse Network Ops       : 0          Browse Network Fails     : 0
    Browse Domain Ops        : 0          Browse Domain Fails      : 0
    Browse Server Ops        : 0          Browse Server Fails      : 0
    Browse Share Ops         : 0          Browse Share Fails       : 0
    Browse Dir Ops           : 0          Browse Network Fails     : 0
    File Read Ops            : 0          File Read Fails          : 0
    File Write Ops           : 0          File Write Fails         : 0
    Folder Create Ops        : 0          Folder Create Fails      : 0
    File Delete Ops          : 0          File Delete Fails        : 0
    File Rename Ops          : 0          File Rename Fails        : 0
```

次に、HTTP 認証の統計情報を表示する例を示します。

```
webvpn# show webvpn stats httpauth
HTTP Authentication stats :
    Successful NTLM Auth     : 0          Failed NTLM Auth         : 0
    Successful Basic Auth    : 1          Failed Basic Auth        : 1
    Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
    NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
    Oversize NTLM Type3 cred : 0          Internal Error           : 0
    Num 401 responses        : 3          Num non-401 responses    : 97
    Num Basic forms served   : 2          Num NTLM forms served    : 0
    Num Basic Auth sent      : 3          Num NTLM Auth sent       : 0
```

次に、Citrix の統計情報を表示する例を示します。

```
webvpn# show web stats citrix
WEBVPN Citrix statistics:
               Client                    Server
  Packets in  : 0                          0
  Packets out : 0                          0
  Bytes in    : 0                          0
  Bytes out   : 0                          0
```

次に、特定のコンテキストの統計情報を表示する例を示します。

```
webvpn# show web stats context tunnel
WebVPN context name : tunnel
User session statistics:
    Active user sessions     : 0          AAA pending reqs          : 0
    Peak user sessions       : 1          Peak time                 : 5d16h
    Active user TCP conns    : 0          Terminated user sessions : 5
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 1          VPN idle timeout          : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit   : 0

Mangling statistics:
    Relative urls            : 0          Absolute urls             : 0
    Non-http(s) absolute urls: 0          Non-standard path urls    : 0
    Interesting tags         : 0          Uninteresting tags        : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles             : 0
    HTML comments            : 0          HTTP/1.0 requests         : 0
    HTTP/1.1 requests        : 111        Unknown HTTP version      : 0
    GET requests             : 106        POST requests             : 5
    CONNECT requests         : 0          Other request methods     : 0
    Through requests         : 0          Gateway requests          : 111
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 43741      Processed req body bytes : 265
    HTTP/1.0 responses       : 0          HTTP/1.1 responses        : 0
    HTML responses           : 0          CSS responses             : 0
    XML responses            : 0          JS responses              : 0
    Other content type resp  : 0          Chunked encoding resp     : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0

HTTP Authentication stats :
    Successful NTLM Auth     : 0          Failed NTLM Auth          : 0
    Successful Basic Auth    : 0          Failed Basic Auth         : 0
    Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
    NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
    Oversize NTLM Type3 cred : 0          Internal Error            : 0
    Num 401 responses        : 0          Num non-401 responses     : 0
    Num Basic forms served   : 0          Num NTLM forms served     : 0
    Num Basic Auth sent      : 0          Num NTLM Auth sent        : 0

Admission Control stats :
    Users Denied             : 0          Requests Dropped          : 0
    CPU util exceeded        : 0          Memory util exceeded      : 0
    Appl Buf util exceeded   : 0
CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                  : 0
    Active VC's              : 0          Active Contexts           : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies              : 0
    NB DGM Requests          : 0          NB DGM Replies            : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  HTTP related Per Context:
    Requests                 : 5          Request Bytes RX          : 1840
    Request Packets RX       : 0          Response Bytes TX         : 1435222
    Response Packets TX      : 938        Active Connections        : 0
    Active CIFS context      : 0          Requests Dropped          : 0
```

```
Socket statistics:
    Sockets in use           : 0          Sock Usr Blocks in use   : 0
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 0          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 0          Sock Tx Unblocked        : 0
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 0

Port Forward statistics:
  Client                                 Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0

WEBVPN Citrix statistics:

               Client                    Server
  Packets in  : 0                        0
  Packets out : 0                        0
  Bytes in    : 0                        0
  Bytes out   : 0                        0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 1          Peak time                : 5d16h
    Connect succeed          : 6          Connect failed           : 0
    Reconnect succeed        : 1          Reconnect failed         : 0
    DPD timeout              : 0
  Client                                 Server
    in  CSTP frames          : 23098      out IP pkts              : 23093
    in  CSTP data            : 23093
    in  CSTP control         : 5
    in  CSTP bytes           : 4956832    out IP bytes             : 4771852
    out CSTP frames          : 32086      in  IP pkts              : 32084
    out CSTP data            : 32084
    out CSTP control         : 2
    out CSTP bytes           : 16136526   in  IP bytes            : 16512477

webvpn#
```

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。

[no] snmp-server enable {**informs** | **traps** {**ipsec** | **isakmp** | **snmp** | **tty**}}

シンタックスの説明

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。追加のオプションについては、「使用上のガイドライン」を参照してください。
isakmp	ISAKMP トラップをイネーブルにします。追加のオプションについては、「使用上のガイドライン」を参照してください。
snmp	SNMP トラップをイネーブルにします。追加のオプションについては、「使用上のガイドライン」を参照してください。
tty	TCP 接続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がありません。

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が Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

ipsec キーワードには次のオプションがあります。

- **ipsec crptomap** {**add** | **attach** | **delete** | **detach**}
- **ipsec too-many-sas**
- **ipsec tunnel** {**start** | **stop**}

isakmp キーワードには次のオプションがあります。

- **isakmp** {**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}}

snmp キーワードには次のオプションがあります。

- **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]

例

次に、SNMP 通知をイネーブルにする例を示します。

```
wwbvpn(config)# snmp-server enable informs
wwbvpn(config)#
```

次に、トラップをイネーブルにする例を示します。

```
wwbvpn(config)# snmp-server enable traps
wwbvpn(config)#
```

次に、認証トラップをイネーブルにする例を示します。

```
wwbvpn(config)# snmp-server enable traps snmp authnetication
wwbvpn(config)#
```

svc

グループ ポリシー コンテキストのトンネル機能を設定するには、**svc** コマンドを使用します。入力した **svc** コマンドのいずれかを削除するには、このコマンドの **no** 形式を使用します。

svc *command*

シンタックスの説明

command	コンフィギュレーション コマンドを指定します。使用可能なコマンドのリストについては、表 2-5 を参照してください。

デフォルト

デフォルト設定については、表 2-5 を参照してください。

コマンド モード

WebVPN グループ コンテキスト サブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

svc コマンドのプロンプトは、グループ ポリシーのプロンプトと同じです。

表 2-5 に、グループ コンテキストでトンネル モード機能の設定に使用するコマンドを示します。

表 2-5　トンネル モード コンフィギュレーション コマンド

コマンド	目的および注意事項	デフォルト
address-pool *address-pool-name*	プールからアドレスをリモート ユーザに割り当てます。	
default-domain *default-domain-name*	ユーザ / グループに対してトンネル モードの WebVPN がイネーブルの場合、ユーザ / グループで使用されるデフォルトのドメインを指定します。	
dns-server {**primary** | **secondary**} *ip-address*	Web ブラウジング用にプライマリ DNS サーバおよびセカンダリ DNS サーバを指定します。SSL VPN Client（SVC）がインストールされると、アクティブな Web ブラウザが非アクティブになり、新しいブラウザが起動します。ここで指定する DNS サーバの情報は、新しく起動されるブラウザで使用されます。接続が閉じられると、以前の DNS 設定が再適用されます。	
dpd-interval {**client** *timeout*} | {**gateway** *timeout*}	ユーザまたはグループでトンネル モードの WebVPN がイネーブルの場合、ゲートウェイまたはクライアントの Dead Peer Detection（DPD）タイムアウト値を指定します。ピアに DPD パケットを送信する必要があるかどうかを判別する際に DPD タイマーが使用されます。ピアから Cisco SSL Tunnel Protocol（CSTP）フレームを受信するたびに、DPD タイマーがリセットされます。 **gateway** *timeout* — SG の DPD タイムアウト値を指定します。有効値は 0（ディセーブル）～ 3600 秒です。 **client** *timeout* — クライアントの DPD タイムアウト値を指定します。有効値は 0（ディセーブル）～ 3600 秒です。	ゲートウェイおよびクライアントに対してディセーブルです。

表 2-5　トンネル モード コンフィギュレーション コマンド（続き）

コマンド	目的および注意事項	デフォルト
homepage *url*	ログイン時にユーザに表示される Web ページの URL を設定します。URL ストリングは、URL のパスを指定します。URL ストリングの最大長は 255 文字です。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を入力します。	Web ページは指定されていません。
keep-client-installed	接続が閉じられた後も SVC をインストールした状態にしておきます。	
msie-proxy exception {*ip-address* | *dns-name*}	Microsoft Internet Explorer（MSIE）ブラウザのプロキシを設定します。 （注）　このコマンドは、MSIE ブラウザでのみサポートされています。 **exception** キーワードは、プロキシ経由で送信されないトラフィックの単一の DNS 名または IP アドレスを指定します。	ディセーブル
msie-proxy server {*ip-address* | *dns_name*}[**:** *port*]	MSIE ブラウザのプロキシを設定します。 （注）　このコマンドは、MSIE ブラウザでのみサポートされています。 **server** キーワードは、Socks 以外のブラウザのすべてのプロキシ設定（HTTP、Secure、FTP、Gopher）で使用される IP アドレスまたは DNS 名を指定します（任意で、IP アドレスまたは DNS 名のあとにコロンとポート番号を指定できます）。	ディセーブル
msie-proxy option {**auto** | **bypass-local** | **none**}	MSIE ブラウザのプロキシを設定します。 （注）　このコマンドは、MSIE ブラウザでのみサポートされています。 **option none** キーワードは、ブラウザがプロキシを使用しないように指定します。 **option auto** キーワードは、ブラウザのプロキシ設定が自動検出されるように指定します。 **option bypass-local** キーワードは、ローカル アドレスがプロキシをバイパスするように指定します。	**option none**
rekey method {**new-tunnel** | **ssl**} **no rekey method**	鍵の再生成方法を指定します。このコマンドの **no** 形式を入力すると、鍵の再生成がディセーブルになります。 • **new-tunnel** — 既存のトンネルを終了して、新しいトンネルを要求します。 • **ssl** — SSL 再ハンドシェイクを開始します。	鍵の再生成がイネーブルの場合、デフォルトの方法は **ssl** です。

表 2-5　トンネル モード コンフィギュレーション コマンド（続き）

コマンド	目的および注意事項	デフォルト
rekey {**time** *interval*} **no rekey time**	VPN クライアントが SSL トンネルの鍵の再生成を行う間隔を指定します。この間隔は、時間をベースにしています。このコマンドの **no** 形式を入力すると、鍵の再生成時間の間隔がディセーブルになります。 *interval* ― 有効値は 0 ～ 43200 秒です。	21600 秒（6 時間）
split dns *string*	スプリット トンネル パラメータを指定します。 *string* ― DNS サーバの名前または IP アドレス	
split exclude {*ip-address netmask* | **local-lans**}	このコマンドを使用すると、内部ネットワークをトンネリングされずに外部 Web サイトに直接送信されるトラフィックを指定できます。他のすべてのトラフィックはトンネリングされます。 **（注）** 指定できるのは **split include** または **split exclude** コマンドのいずれかです。両方のキーワードは同時に指定できません。コマンドを複数回入力して、**split include** または **split exclude** キーワードのいずれかに最大 200 個のアドレスを指定できます。 • *ip-address netmask* ― トンネリングされないトラフィックのアドレス • **local-lans** ― エンド ユーザのローカル LAN トラフィックがトンネリングされないように指定します。	
split include *ip-address netmask*	このコマンドを使用すると、トンネリングされるトラフィックを指定できます。他のすべてのトラフィックは、内部ネットワークでトンネリングされません。 **（注）** 指定できるのは **split include** または **split exclude** コマンドのいずれかです。両方のキーワードは同時に指定できません。コマンドを複数回入力して、**split include** または **split exclude** キーワードのいずれかに最大 200 個のアドレスを指定できます。 *ip-address netmask* ― トンネリングされるトラフィックのアドレス	
wins-server {**primary** | **secondary**} *ip-address*	プライマリまたはセカンダリ WINS サーバを指定します。	

url-list

URL サブモードを開始して、URL リストを設定するには、**url-list** コマンドを使用します。コンフィギュレーションから所定のリストを削除するには、このコマンドの **no** 形式を使用します。

url-list *listname*

no url-list *listname*

シンタックスの説明

listname	URL リストの名前

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

WebVPN コンテキスト サブモード

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

listname 引数では、大文字と小文字が区別され、最大長は 64 文字です。

url-list コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-url)#
```

URL サブモードを開始した場合、次のコマンドを使用して URL リストを設定できます。表 2-6 に、URL サブモード コマンドを示します。

表 2-6　URL サブモード コマンド

コマンド	目的および注意事項	デフォルト
exit	WebVPN URL サブモードを終了して、WebVPN コンテキスト サブモードに戻ります。	
heading *text*	URL のグループに対する見出しテキストを指定します。見出しにスペースが含まれる場合は、引用符で *text* 値を囲みます。 各リスト名に指定できるのは 1 つの見出しだけです。	
url-text *text* **url-value** *url*[**/exchage**]	ホーム ページ上でリンクとして表示されるテキストを指定します。*text* の値は、所定のリスト名内で一意である必要があります。テキストにスペースが含まれる場合は、引用符で *text* 値を囲みます。	

url-value *url* キーワードおよび引数は、リンク先の URL を指定します。Web ベースの E メールで Outlook Web Access（OWA）を使用するには、**/exchange** キーワードを使って URL を追加します（Exchange サーバへの認証が必要）。

所定のリスト名に対して複数の URL を指定できます。

例

次に、URL リストを設定する例を示します。

```
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# url-text payroll url-value http://10.1.2.215/payroll
webvpn(config-webvpn-url)# url-text finance url-value https://finance.cisco.com
webvpn(config-webvpn-url)# url-text "OWA server" url-value
http://mail.cisco.com/exchange
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
```

関連コマンド

webvpn context

webvpn context

WebVPN コンテキスト サブモードを開始して、仮想 WebVPN コンテキストを定義するには、**webvpn context** コマンドを使用します。WebVPN サブコマンド モードで入力したコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

webvpn context [*vpn-name*]

no webvpn context *vpn-name*

シンタックスの説明

vpn-name	（任意）WebVPN インスタンスの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.2	Cisco Secure Desktop（CSD）をイネーブルまたはディセーブルにするコマンドが追加されました。
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

vpn-name 引数では、大文字と小文字が区別されます。

webvpn context コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-context)#
```

コンテキスト サブモードを開始した場合、次のコマンドを使用してコンテキスト サービスを設定できます。表 2-7 に、仮想コンテキスト サブモード コマンドを示します。

表 2-7　仮想 WebVPN コンテキスト サブモード コマンド

コマンド	目的および注意事項	デフォルト
aaa authentication {{**domain** *domain-list*} | {**list** *listname*}}	コンテキストの AAA（認証、許可、アカウンティング）コンフィギュレーション パラメータを指定します。 • **domain** *domain-list* — 認証用に使用するドメイン名を指定します。 • **list** *listname* — 認証リストの名前を指定します。	
charset-encoding {**shift-jis** | **iso-8859-1**}	WebVPN ゲートウェイでの日本語 Shift-JIS エンコードのサポートをイネーブルにします。	**iso-8859-1**
csd-enable **no csd-enable**	仮想 WebVPN コンテキストの CSD をイネーブルにします。	イネーブルにされていません。
default-group-policy *default-policy-name*	仮想 WebVPN コンテキスト インスタンスが使用するデフォルトのグループ ポリシーを指定します。グループ ポリシーについては、**policy group** コマンドを参照してください。	

表 2-7　仮想 WebVPN コンテキスト サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
exit	コンテキスト サブモードを終了して、グローバル コンフィギュレーション モードに戻ります。	
gateway *gateway-name* {{**domain-name** *domain-name*} | {**virtual-host** *hostname*}}	セキュア ゲートウェイに設定されている対応する仮想ゲートウェイ インスタンスとマッピング方式（たとえば、IP アドレス、URL、およびドメイン名）を次のように指定します。 • *gateway-name* — システムに設定されている仮想ゲートウェイの名前 • **domain-name** *domain-name* — （任意）特定のドメイン名にマッピングします。*domain-name* 引数は ASCII ストリングで、仮想 WebVPN インスタンスの企業固有のドメイン名（たとえば、cisco.com）を指定する際に使用されます。 • **virtual-host** *hostname* — （任意）特定の仮想ホストにマッピングします。	仮想化は、一意の IP アドレスを使用して実行されます。
inservice	コンテキストを有効にします。	
login-message *string* **no login-message**	ユーザのログインを求めるテキストを指定します。このテキストは 255 文字に制限されています。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。	*string* は、「Please enter your username and password.」です。
logo [**file** *filename* | **none**]	ログイン ページとホーム ページに表示されるカスタム ロゴ イメージを指定します。 **file** *filename* — （任意）管理者がセキュリティ ゲートウェイにアップロードするファイルのファイル名を指定します。	
nat-address *start-address end-address* {**netmask** *netmask*}	サーバ接続を開くときに使用される NAT アドレスを指定します。**nat-address** コマンドで指定したアドレスは、WebVPN サブインターフェイスで設定されたいずれかのサブネットに一致する必要があります。 • *start-address* — アドレス プールのアドレス範囲を定義する先頭の IP アドレス • *end-address* — アドレス プールのアドレス範囲を定義する末尾の IP アドレス • **netmask** *netmask* — どのアドレス ビットがネットワーク フィールドおよびサブネットワーク フィールドに属し、どのビットがホスト フィールドに属しているかを示すネットワーク マスク。プール アドレスが属しているネットワークのネットマスクを指定します。	
nbns-list *name*	nbnslist サブモードを開始します。このモードでは、NBNS リスト名を作成できます。NBNS リストの設定方法については、**nbns-list** コマンドを参照してください。	
password-prompt *prompt*	初回の WebVPN ログイン パスワードのプロンプトを設定します。プロンプトの最大長は 16 文字です。	*prompt* は「Password:」です。

表 2-7　仮想 WebVPN コンテキスト サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
policy group *policy-name*	グループ サブモードを開始します。このモードでは、グループ ポリシーを設定できます。グループ ポリシーの設定方法については、**policy group** コマンドを参照してください。	
policy ssl *policy-name*	SSL プロトコルが使用する SSL ポリシーを指定します。	
policy tcp *policy-name*	TCP プロトコルが使用する TCP ポリシーを指定します。	
port-forward *listname*	ポートフォワーディング サブモードを開始します。このモードでは、ユーザがアクセス権を所有するポートのリストを設定できます。ポートフォワーディングの設定方法については、**port-forward** コマンドを参照してください。	
secondary-color *color* **no secondary-color**	ログイン ページ、ホーム ページ、およびファイル アクセス ページのセカンダリ タイトル バーの色を指定します。有効値については、表 2-8 を参照してください。	デフォルトの色はパープルです。
secondary-text-color [**black** | **white**] **no secondary-text-color**	セカンダリ バーのテキストの色を指定します。タイトル バーのテキストの色に一致させる必要があります。有効値は **black** および **white** 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。	**black**
ssl authenticate verify {**all** | **none**}	SSL プロトコルの使用方法を設定します。 • **authenticate verify** — SSL 証明書の検証方法を指定します。 – **all** — すべての CRL とシグニチャの信頼性を検証します。 – **none** — ピアからの証明書を検証しません。	**all**
text-color [**black** | **white**] **no text-color**	タイトル バーのテキストの色を指定します。ツールバーに表示させる必要があるアイコン数を制限するために、2 つの値だけに制限されています。有効値は **black** および **white** 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。	**white**
title *string* **no title**	ブラウザ タイトルおよびタイトル バーの HTML タイトル ストリングを指定します。このストリングは 255 文字に制限されています。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。	*string* は「WebVPN Service」です。
title-color *color* **no title-color**	ログイン ページ、ホーム ページ、およびファイル アクセス ページのタイトル バーの色を指定します。有効値については、表 2-8 を参照してください。	デフォルトの色はパープルです。
username-prompt *prompt*	初回の WebVPN ログイン ユーザ名のプロンプトを設定します。プロンプトの最大長は 16 文字です。	*prompt* は「Login:」です。
url-list *listname*	URL サブモードを開始します。このモードでは、ポータル Web ページに表示する URL のリストを設定できます。URL エントリの設定方法については、**url-list** コマンドを参照してください。	
vrf-name *vrf-name*	仮想 WebVPN コンテキストに設定されている VRF ドメインを指定します。	

WebVPN コンテキストは、事前に設定されたアドレス解決、ゲートウェイ、および認証の設定にリンクします。

クライアントレス モードを設定するには、URL リストとグループ ポリシーを設定します。Outlook Web Access（OWA）を使用して E メールにアクセスするには、Microsoft Exchange サーバ（たとえば、**http://***ipaddr*/**exchange**）を参照する URL リストを設定します。

シンクライアント モードを設定するには、転送するポートのリストとグループ ポリシーを設定します。

Common Internet File System（CIFS）を使用してファイル共有を設定するには、NetBIOS Name Service（NBNS）リスト、サーバ アドレス、およびグループ ポリシーを設定します。

表 2-8 に、WebVPN コンテキストで **title-color** *color* コマンドと **secondary-color** *color* コマンドを入力するときの *color* の有効値を示します。デフォルトの色はパープルです。

値には、HTML で認識される色の名前（単語または文字の間にスペースは不要）または RGB（レッド、グリーン、ブルー）値をカンマで区切って指定できます。値は、32 文字に制限されています。

（注） すべてのブラウザが RGB 値をサポートしていますが、色の名前をサポートしていないブラウザもあります。色の名前を入力し、期待した結果が得られなかった場合は、RGB 値を使用してください。

表 2-8　色の名前および RGB 値

色の名前	R	G	B
AliceBlue	240	248	255
AntiqueWhite	250	235	215
AntiqueWhite1	255	239	219
AntiqueWhite2	238	223	204
AntiqueWhite3	205	192	176
AntiqueWhite4	139	131	120
Aquamarine	127	255	212
Aquamarine1	127	255	212
Aquamarine2	118	238	198
Aquamarine3	102	205	170
Aquamarine4	69	139	116
Azure	240	255	255
Azure1	240	255	255
Azure2	224	238	238
Azure3	193	205	205
Azure4	131	139	139
Beige	245	245	220
Bisque	255	228	196
Bisque1	255	228	196
Bisque2	238	213	183
Bisque3	205	183	158
Bisque4	139	125	107
Black	0	0	0
BlanchedAlmond	255	235	205

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Blue	0	0	255
Blue1	0	0	255
Blue2	0	0	238
Blue3	0	0	205
Blue4	0	0	139
BlueViolet	138	43	226
Brown	165	42	42
Brown1	255	64	64
Brown2	238	59	59
Brown3	205	51	51
Brown4	139	35	35
Burlywood	222	184	135
Burlywood1	255	211	155
Burlywood2	238	197	145
Burlywood3	205	170	125
Burlywood4	139	115	85
CadetBlue	95	158	160
CadetBlue1	152	245	255
CadetBlue2	142	229	238
CadetBlue3	122	197	205
CadetBlue4	83	134	139
Chartreuse	127	255	0
Chartreuse1	127	255	0
Chartreuse2	118	238	0
Chartreuse3	102	205	0
Chartreuse4	69	139	0
Chocolate	210	105	30
Chocolate1	255	127	36
Chocolate2	238	118	33
Chocolate3	205	102	29
Chocolate4	139	69	19
Coral	255	127	80
Coral1	255	114	86
Coral2	238	106	80
Coral3	205	91	69
Coral4	139	62	47
CornflowerBlue	100	149	237
Cornsilk	255	248	220
Cornsilk1	255	248	220
Cornsilk2	238	232	205
Cornsilk3	205	200	177

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Cornsilk4	139	136	120
Cyan	0	255	255
Cyan1	0	255	255
Cyan2	0	238	238
Cyan3	0	205	205
Cyan4	0	139	139
DarkBlue	0	0	139
DarkCyan	0	139	139
DarkGoldenrod	184	134	11
DarkGoldenrod1	255	185	15
DarkGoldenrod2	238	173	14
DarkGoldenrod3	205	149	12
DarkGoldenrod4	139	101	8
DarkGray	169	169	169
DarkGreen	0	100	0
DarkKhaki	189	183	107
DarkMagenta	139	0	139
DarkOliveGreen	85	107	47
DarkOliveGreen1	202	255	112
DarkOliveGreen2	188	238	104
DarkOliveGreen3	162	205	90
DarkOliveGreen4	110	139	61
DarkOrange	255	140	0
DarkOrange1	255	127	0
DarkOrange2	238	118	0
DarkOrange3	205	102	0
DarkOrange4	139	69	0
DarkOrchid	153	50	204
DarkOrchid1	191	62	255
DarkOrchid2	178	58	238
DarkOrchid3	154	50	205
DarkOrchid4	104	34	139
DarkRed	139	0	0
DarkSalmon	233	150	122
DarkSeaGreen	143	188	143
DarkSeaGreen1	193	255	193
DarkSeaGreen2	180	238	180
DarkSeaGreen3	155	205	155
DarkSeaGreen4	105	139	105
DarkSlateBlue	72	61	139
DarkSlateGray	47	79	79

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
DarkSlateGray1	151	255	255
DarkSlateGray2	141	238	238
DarkSlateGray3	121	205	205
DarkSlateGray4	82	139	139
DarkTurquoise	0	206	209
DarkViolet	148	0	211
DeepPink	255	20	147
DeepPink1	255	20	147
DeepPink2	238	18	137
DeepPink3	205	16	118
DeepPink4	139	10	80
DeepSkyBlue	0	191	255
DeepSkyBlue1	0	191	255
DeepSkyBlue2	0	178	238
DeepSkyBlue3	0	154	205
DeepSkyBlue4	0	104	139
DimGrey	105	105	105
DodgerBlue	30	144	255
DodgerBlue1	30	144	255
DodgerBlue2	28	134	238
DodgerBlue3	24	116	205
DodgerBlue4	16	78	139
Firebrick	178	34	34
Firebrick1	255	48	48
Firebrick2	238	44	44
Firebrick3	205	38	38
Firebrick4	139	26	26
FloralWhite	255	250	240
ForestGreen	34	139	34
Gainsboro	220	220	220
GhostWhite	248	248	255
Gold	255	215	0
Gold1	255	215	0
Gold2	238	201	0
Gold3	205	173	0
Gold4	139	117	0
Goldenrod	218	165	32
Goldenrod1	255	193	37
Goldenrod2	238	180	34
Goldenrod3	205	155	29
Goldenrod4	139	105	20

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Gray0	0	0	0
Gray1	3	3	3
Gray10	26	26	26
Gray100	255	255	255
Gray11	28	28	28
Gray12	31	31	31
Gray13	33	33	33
Gray14	36	36	36
Gray15	38	38	38
Gray16	41	41	41
Gray17	43	43	43
Gray18	46	46	46
Gray19	48	48	48
Gray2	5	5	5
Gray20	51	51	51
Gray21	54	54	54
Gray22	56	56	56
Gray23	59	59	59
Gray24	61	61	61
Gray25	64	64	64
Gray26	66	66	66
Gray27	69	69	69
Gray28	71	71	71
Gray29	74	74	74
Gray3	8	8	8
Gray30	77	77	77
Gray31	79	79	79
Gray32	82	82	82
Gray33	84	84	84
Gray34	87	87	87
Gray35	89	89	89
Gray36	92	92	92
Gray37	94	94	94
Gray38	97	97	97
Gray39	99	99	99
Gray4	10	10	10
Gray40	102	102	102
Gray41	105	105	105
Gray42	107	107	107
Gray43	110	110	110
Gray44	112	112	112

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Gray45	115	115	115
Gray46	117	117	117
Gray47	120	120	120
Gray48	122	122	122
Gray49	125	125	125
Gray5	13	13	13
Gray50	127	127	127
Gray51	130	130	130
Gray52	133	133	133
Gray53	135	135	135
Gray54	138	138	138
Gray55	140	140	140
Gray56	143	143	143
Gray57	145	145	145
Gray58	148	148	148
Gray59	150	150	150
Gray6	15	15	15
Gray60	153	153	153
Gray61	156	156	156
Gray62	158	158	158
Gray63	161	161	161
Gray64	163	163	163
Gray65	166	166	166
Gray66	168	168	168
Gray67	171	171	171
Gray68	173	173	173
Gray69	176	176	176
Gray7	18	18	18
Gray70	179	179	179
Gray71	181	181	181
Gray72	184	184	184
Gray73	186	186	186
Gray74	189	189	189
Gray75	191	191	191
Gray76	194	194	194
Gray77	196	196	196
Gray78	199	199	199
Gray79	201	201	201
Gray8	20	20	20
Gray80	204	204	204
Gray81	207	207	207

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Gray82	209	209	209
Gray83	212	212	212
Gray84	214	214	214
Gray85	217	217	217
Gray86	219	219	219
Gray87	222	222	222
Gray88	224	224	224
Gray89	227	227	227
Gray9	23	23	23
Gray90	229	229	229
Gray91	232	232	232
Gray92	235	235	235
Gray93	237	237	237
Gray94	240	240	240
Gray95	242	242	242
Gray96	245	245	245
Gray97	247	247	247
Gray98	250	250	250
Gray99	252	252	252
Green	0	255	0
Green1	0	255	0
Green2	0	238	0
Green3	0	205	0
Green4	0	139	0
GreenYellow	173	255	47
Grey	190	190	190
Grey0	0	0	0
Grey1	3	3	3
Grey10	26	26	26
Grey100	255	255	255
Grey11	28	28	28
Grey12	31	31	31
Grey13	33	33	33
Grey14	36	36	36
Grey15	38	38	38
Grey16	41	41	41
Grey17	43	43	43
Grey18	46	46	46
Grey19	48	48	48
Grey2	5	5	5
Grey20	51	51	51

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Grey21	54	54	54
Grey22	56	56	56
Grey23	59	59	59
Grey24	61	61	61
Grey25	64	64	64
Grey26	66	66	66
Grey27	69	69	69
Grey28	71	71	71
Grey29	74	74	74
Grey3	8	8	8
Grey30	77	77	77
Grey31	79	79	79
Grey32	82	82	82
Grey33	84	84	84
Grey34	87	87	87
Grey35	89	89	89
Grey36	92	92	92
Grey37	94	94	94
Grey38	97	97	97
Grey39	99	99	99
Grey4	10	10	10
Grey40	102	102	102
Grey41	105	105	105
Grey42	107	107	107
Grey43	110	110	110
Grey44	112	112	112
Grey45	115	115	115
Grey46	117	117	117
Grey47	120	120	120
Grey48	122	122	122
Grey49	125	125	125
Grey5	13	13	13
Grey50	127	127	127
Grey51	130	130	130
Grey52	133	133	133
Grey53	135	135	135
Grey54	138	138	138
Grey55	140	140	140
Grey56	143	143	143
Grey57	145	145	145
Grey58	148	148	148

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Grey59	150	150	150
Grey6	15	15	15
Grey60	153	153	153
Grey61	156	156	156
Grey62	158	158	158
Grey63	161	161	161
Grey64	163	163	163
Grey65	166	166	166
Grey66	168	168	168
Grey67	171	171	171
Grey68	173	173	173
Grey69	176	176	176
Grey7	18	18	18
Grey70	179	179	179
Grey71	181	181	181
Grey72	184	184	184
Grey73	186	186	186
Grey74	189	189	189
Grey75	191	191	191
Grey76	194	194	194
Grey77	196	196	196
Grey78	199	199	199
Grey79	201	201	201
Grey8	20	20	20
Grey80	204	204	204
Grey81	207	207	207
Grey82	209	209	209
Grey83	212	212	212
Grey84	214	214	214
Grey85	217	217	217
Grey86	219	219	219
Grey87	222	222	222
Grey88	224	224	224
Grey89	227	227	227
Grey9	23	23	23
Grey90	229	229	229
Grey91	232	232	232
Grey92	235	235	235
Grey93	237	237	237
Grey94	240	240	240
Grey95	242	242	242

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Grey96	245	245	245
Grey97	247	247	247
Grey98	250	250	250
Grey99	252	252	252
Honeydew	240	255	240
Honeydew1	240	255	240
Honeydew2	224	238	224
Honeydew3	193	205	193
Honeydew4	131	139	131
HotPink	255	105	180
HotPink1	255	110	180
HotPink2	238	106	167
HotPink3	205	96	144
HotPink4	139	58	98
IndianRed	205	92	92
IndianRed1	255	106	106
IndianRed2	238	99	99
IndianRed3	205	85	85
IndianRed4	139	58	58
Ivory	255	255	240
Ivory1	255	255	240
Ivory2	238	238	224
Ivory3	205	205	193
Ivory4	139	139	131
Khaki	240	230	140
Khaki1	255	246	143
Khaki2	238	230	133
Khaki3	205	198	115
Khaki4	139	134	78
Lavender	230	230	250
LavenderBlush	255	240	245
LavenderBlush1	255	240	245
LavenderBlush2	238	224	229
LavenderBlush3	205	193	197
LavenderBlush4	139	131	134
LawnGreen	124	252	0
LemonChiffon	255	250	205
LemonChiffon1	255	250	205
LemonChiffon2	238	233	191
LemonChiffon3	205	201	165
LemonChiffon4	139	137	112

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
LightBlue	173	216	230
LightBlue1	191	239	255
LightBlue2	178	223	238
LightBlue3	154	192	205
LightBlue4	104	131	139
LightCoral	240	128	128
LightCyan	224	255	255
LightCyan1	224	255	255
LightCyan2	209	238	238
LightCyan3	180	205	205
LightCyan4	122	139	139
LightGoldenrod	238	221	130
LightGoldenrod1	255	236	139
LightGoldenrod2	238	220	130
LightGoldenrod3	205	190	112
LightGoldenrod4	139	129	76
LightGoldenrodYellow	250	250	210
LightGreen	144	238	144
LightGrey	211	211	211
LightPink	255	182	193
LightPink1	255	174	185
LightPink2	238	162	173
LightPink3	205	140	149
LightPink4	139	95	101
LightSalmon	255	160	122
LightSalmon1	255	160	122
LightSalmon2	238	149	114
LightSalmon3	205	129	98
LightSalmon4	139	87	66
LightSeaGreen	32	178	170
LightSkyBlue	135	206	250
LightSkyBlue1	176	226	255
LightSkyBlue2	164	211	238
LightSkyBlue3	141	182	205
LightSkyBlue4	96	123	139
LightSlateBlue	132	112	255
LightSlateGray	119	136	153
LightSteelBlue	176	196	222
LightSteelBlue1	202	225	255
LightSteelBlue2	188	210	238
LightSteelBlue3	162	181	205

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
LightSteelBlue4	110	123	139
LightYellow	255	255	224
LightYellow1	255	255	224
LightYellow2	238	238	209
LightYellow3	205	205	180
LightYellow4	139	139	122
LimeGreen	50	205	50
Linen	250	240	230
Magenta	255	0	255
Magenta1	255	0	255
Magenta2	238	0	238
Magenta3	205	0	205
Magenta4	139	0	139
Maroon	176	48	96
Maroon1	255	52	179
Maroon2	238	48	167
Maroon3	205	41	144
Maroon4	139	28	98
MediumAquamarine	102	205	170
MediumBlue	0	0	205
MediumOrchid	186	85	211
MediumOrchid1	224	102	255
MediumOrchid2	209	95	238
MediumOrchid3	180	82	205
MediumOrchid4	122	55	139
MediumPurple	147	112	219
MediumPurple1	171	130	255
MediumPurple2	159	121	238
MediumPurple3	137	104	205
MediumPurple4	93	71	139
MediumSeaGreen	60	179	113
MediumSlateBlue	123	104	238
MediumSpringGreen	0	250	154
MediumTurquoise	72	209	204
MediumVioletRed	199	21	133
MidnightBlue	25	25	112
MintCream	245	255	250
MistyRose	255	228	225
MistyRose1	255	228	225
MistyRose2	238	213	210
MistyRose3	205	183	181

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
MistyRose4	139	125	123
Moccasin	255	228	181
NavajoWhite	255	222	173
NavajoWhite1	255	222	173
NavajoWhite2	238	207	161
NavajoWhite3	205	179	139
NavajoWhite4	139	121	94
Navy	0	0	128
NavyBlue	0	0	128
OldLace	253	245	230
OliveDrab	107	142	35
OliveDrab1	192	255	62
OliveDrab2	179	238	58
OliveDrab3	154	205	50
OliveDrab4	105	139	34
Orange	255	165	0
Orange1	255	165	0
Orange2	238	154	0
Orange3	205	133	0
Orange4	139	90	0
OrangeRed	255	69	0
OrangeRed1	255	69	0
OrangeRed2	238	64	0
OrangeRed3	205	55	0
OrangeRed4	139	37	0
Orchid	218	112	214
Orchid1	255	131	250
Orchid2	238	122	233
Orchid3	205	105	201
Orchid4	139	71	137
PaleGoldenrod	238	232	170
PaleGreen	152	251	152
PaleGreen1	154	255	154
PaleGreen2	144	238	144
PaleGreen3	124	205	124
PaleGreen4	84	139	84
PaleTurquoise	175	238	238
PaleTurquoise1	187	255	255
PaleTurquoise2	174	238	238
PaleTurquoise3	150	205	205
PaleTurquoise4	102	139	139

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
PaleVioletRed	219	112	147
PaleVioletRed1	255	130	171
PaleVioletRed2	238	121	159
PaleVioletRed3	205	104	137
PaleVioletRed4	139	71	93
PapayaWhip	255	239	213
PeachPuff	255	218	185
PeachPuff1	255	218	185
PeachPuff2	238	203	173
PeachPuff3	205	175	149
PeachPuff4	139	119	101
Peru	205	133	63
Pink	255	192	203
Pink1	255	181	197
Pink2	238	169	184
Pink3	205	145	158
Pink4	139	99	108
Plum	221	160	221
Plum1	255	187	255
Plum2	238	174	238
Plum3	205	150	205
Plum4	139	102	139
PowderBlue	176	224	230
Purple	160	32	240
Purple1	155	48	255
Purple2	145	44	238
Purple3	125	38	205
Purple4	85	26	139
Red	255	0	0
Red1	255	0	0
Red2	238	0	0
Red3	205	0	0
Red4	139	0	0
RosyBrown	188	143	143
RosyBrown1	255	193	193
RosyBrown2	238	180	180
RosyBrown3	205	155	155
RosyBrown4	139	105	105
RoyalBlue	65	105	225
RoyalBlue1	72	118	255
RoyalBlue2	67	110	238

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
RoyalBlue3	58	95	205
RoyalBlue4	39	64	139
SaddleBrown	139	69	19
Salmon	250	128	114
Salmon1	255	140	105
Salmon2	238	130	98
Salmon3	205	112	84
Salmon4	139	76	57
SandyBrown	244	164	96
SeaGreen	46	139	87
SeaGreen1	84	255	159
SeaGreen2	78	238	148
SeaGreen3	67	205	128
SeaGreen4	46	139	87
Seashell	255	245	238
Seashell1	255	245	238
Seashell2	238	229	222
Seashell3	205	197	191
Seashell4	139	134	130
Sienna	160	82	45
Sienna1	255	130	71
Sienna2	238	121	66
Sienna3	205	104	57
Sienna4	139	71	38
SkyBlue	135	206	235
SkyBlue1	135	206	255
SkyBlue2	126	192	238
SkyBlue3	108	166	205
SkyBlue4	74	112	139
SlateBlue	106	90	205
SlateBlue1	131	111	255
SlateBlue2	122	103	238
SlateBlue3	105	89	205
SlateBlue4	71	60	139
SlateGray	112	128	144
SlateGray1	198	226	255
SlateGray2	185	211	238
SlateGray3	159	182	205
SlateGray4	108	123	139
Snow	255	250	250
Snow1	255	250	250

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Snow2	238	233	233
Snow3	205	201	201
Snow4	139	137	137
SpringGreen	0	255	127
SpringGreen1	0	255	127
SpringGreen2	0	238	118
SpringGreen3	0	205	102
SpringGreen4	0	139	69
SteelBlue	70	130	180
SteelBlue1	99	184	255
SteelBlue2	92	172	238
SteelBlue3	79	148	205
SteelBlue4	54	100	139
Tan	210	180	140
Tan1	255	165	79
Tan2	238	154	73
Tan3	205	133	63
Tan4	139	90	43
Thistle	216	191	216
Thistle1	255	225	255
Thistle2	238	210	238
Thistle3	205	181	205
Thistle4	139	123	139
Tomato	255	99	71
Tomato1	255	99	71
Tomato2	238	92	66
Tomato3	205	79	57
Tomato4	139	54	38
Turquoise	64	224	208
Turquoise1	0	245	255
Turquoise2	0	229	238
Turquoise3	0	197	205
Turquoise4	0	134	139
Violet	238	130	238
VioletRed	208	32	144
VioletRed1	255	62	150
VioletRed2	238	58	140
VioletRed3	205	50	120
VioletRed4	139	34	82
Wheat	245	222	179
Wheat1	255	231	186

表 2-8　色の名前および RGB 値（続き）

色の名前	R	G	B
Wheat2	238	216	174
Wheat3	205	186	150
Wheat4	139	126	102
White	255	255	255
WhiteSmoke	245	245	245
Yellow	255	255	0
Yellow1	255	255	0
Yellow2	238	238	0
Yellow3	205	205	0
Yellow4	139	139	0
YellowGreen	154	205	50

例

次に、WebVPN コンテキスト サブモードを開始して、仮想 WebVPN コンテキストを定義する例を示します。

```
webvpn(config)# webvpn context cisco
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
webvpn(config-webvpn-context)# policy group cisco
webvpn(config-webvpn-group)# url-list cisco
webvpn(config-webvpn-group)# nat-address 172.21.65.73 172.21.65.78 netmask 255.0.0.0
webvpn(config-webvpn-group)# exit
webvpn(config-webvpn-context)# default-group-policy cisco
webvpn(config-webvpn-context)# aaa authentication test
webvpn(config-webvpn-context)# gateway common
webvpn(config-webvpn-context)# inservice
webvpn(config-webvpn-context)# end
webvpn#
```

webvpn gateway

ゲートウェイ サブモードを開始して、仮想ゲートウェイを定義するには、**webvpn gateway** コマンドを使用します。WebVPN サブコマンド モードで入力したコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

webvpn gateway *gateway-name*

no webvpn gateway *gateway-name*

シンタックスの説明

gateway-name	仮想ゲートウェイ サービスの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

gateway-name 引数では、大文字と小文字が区別されます。

webvpn gateway コマンドを入力すると、プロンプトが次のように変わります。

```
webvpn(config-webvpn-gateway)#
```

ゲートウェイ サブモードを開始した場合、次のコマンドを使用して仮想ゲートウェイ サービスを設定できます。表 2-9 に、仮想ゲートウェイ サブモード コマンドを示します。

表 2-9　仮想ゲートウェイ サブモード コマンド

コマンド	目的および注意事項	デフォルト
exit	ゲートウェイ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。	
hostname *hostname*	URL およびクッキー マングリング プロセスで使用されるゲートウェイの名前を指定します。ロードバランシング コンフィギュレーションの場合、ここで指定するホスト名は LB デバイスに設定されている仮想ゲートウェイの IP アドレスになります。	
http-redirect [**port** *port*]	HTTP ポートが開かれており、仮想ゲートウェイへの HTTP 接続では常にセキュア HTTP（HTTPS）を使用するように指定します。 **port** *port* —（任意）リダイレクトされるポート番号を指定します。有効値は 1 ～ 65535 です。	*port* は **80** です。
inservice **no inservice**	WebVPN ゲートウェイをイネーブルにします。WebVPN ゲートウェイ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。	

表 2-9　仮想ゲートウェイ サブモード コマンド（続き）

コマンド	目的および注意事項	デフォルト
ip address *ip-addr* [*netmask*][**port** *port*] [**secondary**]	WebVPN サービス モジュールがプロキシとして機能する仮想 IP アドレスを定義します。 • **port** *port* **—**（任意）WebVPN サービス モジュールがプロキシとして機能するポート番号を指定します。有効値は 1 ～ 65535 です。 • **secondary —**（任意）ゲートウェイをセカンダリ IP として設定します。直接接続されているネットワーク上に仮想 IP アドレスがない場合に、**secondary** キーワードが必要になります。	*port* は **443** です。
policy tcp *tcp-policy-name* **no policy tcp**	(任意) 使用する TCP ポリシーを指定します。デフォルト ポリシーに戻すには、このコマンドの **no** 形式を使用します。	
policy ssl *ssl-policy-name* **no policy ssl**	(任意) 使用する SSL ポリシーを指定します。デフォルト ポリシーに戻すには、このコマンドの **no** 形式を使用します。	
ssl trustpoint *trustpoint-label*	WebVPN ゲートウェイにトラストポイントの設定を適用します。モジュールに組み込まれているテスト証明書をインポートできます。 **（注）** トラストポイントは WebVPN ゲートウェイの Certificate Authority（CA; 認証局）サーバ、鍵パラメータと鍵生成方式、証明書登録方式を定義します。	

ワイルドカードのプロキシ サービスを指定するためにマスク アドレスを設定するには、**ip address** *ip-addr* コマンドを使用して、次の注意事項に従ってください。

- ワイルドカードのプロキシ サービスを設定するには、**secondary** キーワードを入力する必要があります。
- **secondary** キーワードを入力すると、WebVPN サービス モジュールは仮想 IP アドレスの ARP 要求に応答しません。
- WebVPN サービス モジュールがスタンドアロン構成で使用されているか、WebVPN サービス モジュールがディスパッチ モード（MAC アドレスの書き換え）で設定されたロード バランサ上の実サーバとして使用されている（たとえば、CSM）場合は、**secondary** キーワードを入力できます。
- 同じ仮想 IP アドレスを使用して複数のデバイスを設定する場合は、**secondary** キーワードを入力できます。対象の仮想 IP アドレスは、常に正式な IP アドレスとして使用でき、WebVPN サービス モジュールと接続した VLAN（サブネット）内にある必要はありません。

パラメータを指定しないで **webvpn policy tcp** コマンドを入力してポリシーを作成した場合は、デフォルト値を使用してポリシーが作成されます。

512、768、1024、1536、または 2048 以外の鍵（係数）サイズを指定すると、エラーを受信し、トラストポイントの設定が適用されません。鍵を生成するか（同じ *key-label* を使用）、またはサポート対象の係数サイズを指定して鍵を置き換えてから、**gateway-name** *gateway-name* コマンドを使用して、URL およびクッキー マングリング プロセスで使用されるゲートウェイの名前を再入力します。

例

次に、仮想ゲートウェイ（このゲートウェイは WebVPN コンテキストによって参照されます）を定義し、ゲートウェイ サブモードを開始する例を示します。

```
webvpn(config)# webvpn gateway common
webvpn(config-webvpn-gateway)# ip address 172.21.65.71 port 443
webvpn(config-webvpn-gateway)# ssl trustpoint test.p12
webvpn(config-webvpn-gateway)# inservice
webvpn(config-webvpn-gateway)# end
webvpn#
```

webvpn install

Cisco Secure Desktop（CSD）または SSL VPN Client（SVC）パッケージ ファイルをゲートウェイにインストールするには、**webvpn install** コマンドを使用します。ゲートウェイからクライアントをアンインストールするには、このコマンドの **no** 形式を使用します。

webvpn install {**csd** | **svc**} **flash:***path/filename*

no webvpn install {**csd** | **svc**}

シンタックスの説明

csd	CSD をインストールします。
svc	SVC をインストールします。
flash:*path*	パッケージ ファイルへのパス
filename	パッケージ ファイルの名前

デフォルト

このコマンドにはデフォルト設定がありません。

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
WebVPN サービス モジュール Release 1.2	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

SVC ファイルをインストールした場合は、ファイル名が svc.pkg に変わります。CSD ファイルをインストールした場合は、ファイル名が sdesktop.pkg に変わります。

no webvpn install {**csd** | **svc**} コマンドを使用すると、ゲートウェイ上にインストールされたパッケージをアンインストールします。エンド ユーザはパッケージをダウンロードしたり、パッケージを必要とするコンテキストにアクセスしたりできません。ただし、***.pkg** ファイルは WebVPN サービス モジュールのフラッシュにそのまま存在するので、**webvpn install svc flash:**/*path*/{**svc.pkg** | **sdesktop.pkg**} コマンドを入力して、ゲートウェイに再インストールできます。

delete flash:/*path*/{**svc.pkg** | **sdesktop.pkg**} コマンドはフラッシュからパッケージを削除しますが、インストール済みのパッケージには影響しません。エンド ユーザは引き続きパッケージをダウンロードして、パッケージを必要とするコンテキストにアクセスできます。

WebVPN サービス モジュールをリセットまたは再起動し、WebVPN サービス モジュールの flash:/webvpn ディレクトリに svc.pkg または sdesktop.pkg ファイルが存在する場合は、ゲートウェイに SVC または CSD がインストールされています。

例

次に、SVC パッケージをダウンロードし、インストールする例を示します。

```
webvpn# copy tftp: flash:/webvpn
Address or name of remote host [10.1.1.1]?
Source filename []? <username>/sslclient-win-1.0.0.pkg.zip
Destination filename [sslclient-win-1.0.0.pkg.zip]?
Accessing tftp://10.1.1.1/<username>/sslclient-win-1.0.0.pkg.zip...
Loading <username>/sslclient-win-1.0.0.pkg.zip from 10.1.1.1
(via WebVPN0.1): !!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 352117 bytes]
352117 bytes copied in 8.032 secs (37384 bytes/sec)
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

    4  -rwx      352117  Sep 14 2005 13:06:15 -08:00 sslclient-win-1.0.0.pkg.zip

16386048 bytes total (16072704 bytes free)
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn1(config)# webvpn install svc flash:/webvpn/sslclient-win-1.0.0.pkg.zip
SSLVPN Package SSL-VPN-Client : installed successfully
webvpn1(config)# end
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

    4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg

16386048 bytes total (16072704 bytes free)
webvpn#
```

次に、CSD パッケージをダウンロードし、インストールする例を示します。

```
webvpn# copy tftp: flash:/webvpn
Address or name of remote host [10.1.1.1]?
Source filename []? <username>/securedesktop_cat6k_3_1_0_18.pkg.zip
Destination filename [/webvpn/securedesktop_cat6k_3_1_0_18.pkg.zip]?
Accessing tftp://10.1.1.1/<username>/securedesktop_cat6k_3_1_0_18.pkg.zip...
Loading <username>/securedesktop_cat6k_3_1_0_18.pkg.zip from 10.1.1.1 (via
WebVPN0.1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1996130 bytes]

1996130 bytes copied in 33.948 secs (58800 bytes/sec)
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

    4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg
    5  -rwx     1996130  Sep 15 2005 15:14:04 -08:00
securedesktop_cat6k_3_1_0_18.pkg.zip

16386048 bytes total (14020608 bytes free)
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# webvpn install csd flash:/webvpn/securedesktop_cat6k_3_1_0_18.pkg.zip
SSLVPN Package Cisco-Secure-Desktop : installed successfully

webvpn(config)# end
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/

    4  -rwx      352117  Sep 14 2005 13:06:15 -08:00  svc.pkg
    5  -rwx     1996130  Sep 15 2005 15:14:04 -08:00  sdesktop.pkg

16386048 bytes total (14020608 bytes free)
webvpn#
```

webvpn log-level

イベントのシステム メッセージをフィルタリングするには、**webvpn log-level** コマンドを使用します。デフォルトのログ レベルをイネーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **webvpn log-level** {**critical** | **fatal** | **normal**}

シンタックスの説明

critical	クリティカルかつ重大なイベントを記録します。
fatal	重大なイベントだけを記録します。
normal	すべてのシステム イベントを記録します。

デフォルト

デフォルトのログ レベルは critical です。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
WebVPN サービス モジュール Release 1.2	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

fatal オプションは、重大なイベント（システム全体のリソースがなくなりそうな場合など）を記録します。

critical オプションでは、重大なイベントがすべて記録され、次のイベントが含まれます。

- 許可されているグローバル単位の最大ユーザ数またはコンテキスト単位の最大ユーザ数を超えたために、エンド ユーザのログインが拒否された場合
- サイズが超過した NT LAN Manager（NTLM）Type 3 メッセージが受信された場合
- HTTP キープアライブ機能がディセーブルにされた場合
- サポート対象でない基本の HTTP 認証方式が受信された場合

normal オプションは、重大かつクリティカルなイベントがすべて記録され、次のイベントが含まれます。

- VPN セッションに対してエンド ユーザがログイン / ログアウトした場合
- VPN セッションからトンネル ユーザがログアウトした場合
- Cisco Secure Desktop（CSD）管理セッションに対して CSD 管理者がログイン / ログアウトした場合
- アドミッション制御によって、エンド ユーザ ログインが拒否された場合
- クライアント パッケージのインストール中に、エンド ユーザがパッケージ ファイル（SSL VPN Client [SVC] または CSD）を開けない場合
- 仮想コンテキストがアップ / ダウンの状態にされた場合

例

次に、重要なイベントだけを記録する例を示します。

```
webvpn(config)# webvpn log-level fatal
webvpn(config)#
```

webvpn 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、**webvpn 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 プロキシ サービスの SSL ポリシーを定義できます。

webvpn policy ssl *ssl-policy-name*

シンタックスの説明

ssl-policy-name	SSL ポリシー名

デフォルト

デフォルト設定は次のとおりです。

- **cipher** は all です。
- **close-protocol** はイネーブルです。
- **session-caching** はイネーブルです。
- **version** は all 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。
- **tls-rollback** 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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

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 コマンドは、それぞれ別の行に入力します。

表 2-10 に、SSL ポリシー コンフィギュレーション サブモードで利用可能なコマンドを示します。

表 2-10　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

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 サーバで適用可能な暗号スイートのリストを設定できます。
[**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**	セッションのキャッシュ機能をイネーブルにできます。セッションの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。

表 2-10　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（続き）

session-cache size *size*	所定のサービスに割り当てるセッション エントリの最大数を指定します。有効値は 1 ～ 262143 エントリです。
timeout handshake *timeout*	モジュールがハンドシェイク フェーズで接続を維持できる時間を設定できます。有効値は 0 ～ 65535 秒です。
timeout session *timeout* [**absolute**]	セッションのタイムアウトを設定できます。構文の詳細は次のとおりです。 • *timeout* — セッションのタイムアウトです。有効値は 0 ～ 72000 秒です。 • **absolute** —（任意）セッション エントリは、設定したタイムアウトが完了してから削除されます。
tls-rollback [**current** | **any**]	TLS/SSL プリマスタ シークレット メッセージの SSL プロトコル バージョン番号が最大バージョンまたはネゴシエートされたバージョン（**current**）のいずれかであるか、バージョンがチェックされない（**any**）かを指定できます。
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（コマンドライン インターフェイス）を使用して特定のプロキシ サーバに SSL ポリシーを関連付けることができます。SSL ポリシー テンプレートを使用すると、SSL ハンドシェイク スタックに関連付けられた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 メッセージを待ちます。ディセーブルの場合、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が、クライアントからの終了通知メッセージを待たずにセッションを終了します。

暗号スイート名の表記法は、従来の SSL スタックの表記法と同じです。

プロキシ サーバで適用可能な暗号スイートは次のとおりです。

- RSA_WITH_3DES_EDE_CBC_SHA — 3DES-SHA と組み合わせた RSA
- RSA_WITH_DES_CBC_SHA — DES-SHA と組み合わせた RSA
- RSA_WITH_RC4_128_MD5 — RC4-MD5 と組み合わせた RSA
- RSA_WITH_RC4_128_SHA — RC4-SHA と組み合わせた RSA
- all — すべてのサポート対象暗号

timeout session *timeout* **absolute** コマンドを入力すると、セッション エントリは設定されたタイムアウトまでセッション キャッシュに格納され、その後削除されます。セッション キャッシュが満杯で、すべてのエントリに対するタイマーがアクティブであり、**absolute** キーワードが設定されている場合は、以降の新規セッションはすべて拒否されます。

timeout session *timeout* コマンドを **absolute** キーワードなしで入力すると、指定されたタイムアウトは最大タイムアウトとして処理され、セッション エントリをセッション キャッシュ内に維持するよう処理されます。セッション キャッシュのセッション エントリを使い切った場合、現在使用されているセッション エントリは新しい着信接続に備えて削除されます。

cert-req empty コマンドを入力する場合、WebVPN サービス モジュール バックエンド サービスは、常にトラストポイントに関連付けられた証明書を返し、CA 名との一致を検索しません。デフォルトでは、証明書を返す前に、必ず WebVPN サービス モジュールが CA 名との一致を検索します。クライアントの認証時に、SSL サーバの証明書要求に CA 名のリストが含まれていないと、ハンドシェイクが失敗します。

デフォルトでは、WebVPN サービス モジュールは ClientHello メッセージでサポートされている SSL プロトコルの最大バージョン（SSL2.0、SSL3.0、TLS1.0）を使用します。SSL クライアントが ClientHello メッセージに指定されているサポート対象の最大バージョンではなく、ネゴシエートされたバージョンを使用する場合は、**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場合、SSL プロトコル バージョンをサポート対象の最大バージョンまたはネゴシエートされたバージョンのいずれかに設定できます。

tls-rollback any コマンドを入力する場合、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。

```
wwbvpn(config)# webvpn policy ssl sslpl1
wwbvpn(config-ssl-policy)#
```

次に、SSL ポリシーでサポートされる暗号スイートを定義する例を示します。

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

次に、SSL セッション クローズ プロトコルをイネーブルにする例を示します。

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

次に、SSL セッション クローズ プロトコルをディセーブルにする例を示します。

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

次に、特定のコマンドをデフォルトに設定する例を示します。

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

次に、セッション キャッシュをイネーブルにする例を示します。

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

次に、セッション キャッシュををディセーブルにする例を示します。

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

次に、特定のサービスに割り当てるセッション エントリの最大数を設定する例を示します。

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

次に、セッション タイムアウトに絶対値を設定する例を示します。

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

次に、各種の SSL バージョンをサポートできるようにする例を示します。

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

次に、ヘルプ ページを出力する例を示します。

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

関連コマンド

show webvpn stats
show webvpn stats ssl

webvpn 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、**webvpn 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。

webvpn policy tcp *tcp-policy-name*

シンタックスの説明

tcp-policy-name	TCP ポリシー名

デフォルト

デフォルト設定は次のとおりです。

- **buffer-share rx** は 32768 バイトです。
- **buffer-share tx** は 32768 バイトです。
- **delayed-ack-threshold** は 2 パケットです。
- **delay-ack-timeout** は 200 ミリ秒です。
- **mss** は 1460 バイトです。
- **nagle** はイネーブルです。
- **timeout inactivity** は 600 秒です。
- **timeout fin-wait** は 600 秒です。
- **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
WebVPN サービス モジュール Release 1.1	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

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 ポリシーをプロキシ サーバに関連付けることができます。

各プロキシ ポリシー TCP コンフィギュレーション サブモード コマンドは、それぞれ別の行に入力します。

表 2-11 に、プロキシ ポリシー TCP コンフィギュレーション サブモードで利用可能なコマンドを示します。

表 2-11　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**] **buffer-share rx** *buffer-limit-in-bytes*	各接続に対する受信バッファ シェアの最大サイズを設定できます。有効値は 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。
[**no**] **buffer-share tx** *buffer-limit-in-bytes*	各接続に対する送信バッファ シェアの最大サイズを設定できます。有効値は 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。
delayed-ack-threshold	ウィンドウ アップデート ACK（確認応答）が送信されるまでに受信する必要があるフルサイズのセグメント数を指定できます。パケットの有効値は 1 ～ 10 です。デフォルト値は 2 です。
delay-ack-timeout	ウィンドウ アップデート ACK が送信されるまでの時間を指定できます。 このタイマーの期限が切れるまでに **delayed-ack-threshold** コマンドで指定したフルサイズのセグメント数が受信されないと、この時点までに受信されたすべてのデータを確認する ACK が送信されますが、ウィンドウは更新されません。タイマーの有効値は 50 ～ 500 ミリ秒です。デフォルト値は 200 です。
help	対話型ヘルプ システムの説明を表示します。
[**no**] **mss** *max-segment-size-in-bytes*	生成された SYN パケットで接続が識別する最大セグメント サイズを設定できます。有効値は 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**] **nagle**	Nagle のアルゴリズムをイネーブルにできます。 **nagle** キーワードをイネーブルにすると、アプリケーションによって書き込まれた少量のデータが接続送信キューに格納されますが、次のいずれかの状況になるまで送信されません。 • 保留中のデータがあり、送信されたデータを確認する ACK が到着した場合 • アプリケーションによってさらにデータが書き込まれ、フルサイズのセグメントが形成および送信された場合 **nagle** キーワードをディセーブルにすると、データはキューに格納されません。アプリケーションによって書き込まれたすべてのデータがそのまま送信されます。 デフォルトでは、Nagle はイネーブルです。
[**no**] **timeout fin-wait** *timeout-in-seconds*	FIN 待機タイムアウトを設定できます。有効値は 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。
[**no**] **timeout inactivity** *timeout-in-seconds*	非アクティビティ タイムアウトを設定できます。有効値は 0 ～ 960 秒です。このコマンドを使用すると、アイドル状態の接続にエージング タイムアウトを設定して、接続リソースを保護できます。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**] **timeout syn** *timeout-in-seconds*	接続確立のタイムアウトを設定できます。有効値は 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 2-11　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。有効値は 0 ～ 960 秒です（0 = ディセーブル）。指定された時間内にトランザクションが終了しない場合は、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**	フロー内のすべてのパケットに Type of Service（ToS; サービス タイプ）値を転送します。 **（注）** ポリシーがサーバの TCP ポリシーとして設定されている場合、この ToS 値がサーバからクライアントに送信されます。ポリシーが仮想ポリシーとして設定されている場合は、ToS 値がクライアントからサーバに送信されます。 **（注）** ToS 値が学習されてから、伝播される必要があります。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されるように設定されている場合、値が学習され、伝播される前にサーバの接続が確立される必要があります。そのため、初期パケットの一部は ToS 値を伝送しません。

使用上のガイドライン

WebVPN サービス モジュールで入力する TCP コマンドは、グローバルにも、また特定のプロキシ サーバにも適用できます。

プロキシ サーバのクライアント側およびサーバ側に、異なる最大セグメント サイズを設定できます。

TCP ポリシー テンプレートを使用すると、TCP スタックに関連付けられたパラメータを定義できます。

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

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。

```
wwbvpn(config)# webvpn policy tcp tcppl1
wwbvpn(config-tcp-policy)#
```

次に、所定のコマンドをデフォルト値に設定する例を示します。

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

次に、FIN 待機タイムアウトを秒単位で定義する例を示します。

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

次に、非アクティビティ タイムアウトを秒単位で定義する例を示します。

```
wwbvpn(config-tcp-policy)# timeout inactivity 300
wwbvpn(config-tcp-policy)#
```

次に、受信バッファ コンフィギュレーションの最大サイズを定義する例を示します。

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

次に、送信バッファ コンフィギュレーションの最大サイズを定義する例を示します。

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

次に、TCP セグメントの最大サイズを定義する例を示します。

```
wwbvpn(config-tcp-policy)# mss 1460
wwbvpn(config-tcp-policy)#
```

次に、初期接続（SYN）タイムアウト値を定義する例を示します。

```
wwbvpn(config-tcp-policy)# timeout syn 5
wwbvpn(config-tcp-policy)#
```

次に、リアセンブリ タイムアウト値を定義する例を示します。

```
wwbvpn(config-tcp-policy)# timeout reassembly 120
wwbvpn(config-tcp-policy)#
```

次に、フロー内のすべてのパケットに ToS 値がキャリーオーバされるように設定する例を示します。

```
wwbvpn(config-tcp-policy)# tos carryover
wwbvpn(config-tcp-policy)#
```

関連コマンド

show webvpn policy