ASA 8.x：自己署名証明書を使用した AnyConnect VPN Client と VPN Access 併用の設定例クライアント

内容

概要

このドキュメントでは、自己署名証明書を使用して、Cisco AnyConnect 2.0クライアントからASAへのリモートアクセスSSL VPN接続を許可する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ソフトウェア バージョン 8.0 が稼働する基本的な ASA の設定
- ASDM 6.0(2)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 8.0(2)、ASDM 6.0 (2)
- Cisco AnyConnect 2.0

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Cisco AnyConnect 2.0 のクライアントは SSL ベースの VPN クライアントになります。AnyConnect のクライアントは、Windows 2000、XP、Vista、Linux (複数のディストリビューション ベンダー) 、MAC OS X. などの多様な OS でのインストールと利用が可能です。AnyConnect のクライアントは、管理者によるリモート PC での手動インストールが可能です。セキュリティ アプライアンスにロードして、リモート ユーザにダウンロードできるようにすることも可能です。このアプリケーションがダウンロードされたら、接続が終了した際に自動的にアンインストールされるようにもできますし、今後の SSL VPN 接続用にリモート PC に残しておくようにすることもできます。この例では、ブラウザベースの SSL 認証が成功すると、AnyConnect のクライアントをダウンロードできるようになっています。

AnyConnect 2.0 のクライアントについての詳細は、『AnyConnect 2.0 リリース ノート』を参照してください。

注：MSターミナルサービスは、AnyConnectクライアントと組み合わせてサポートされません。RDP を使用してコンピュータにアクセスした場合、AnyConnect のセッションを開始できません。また、AnyConnect を介して接続されたクライアントには RDP にてコンピュータにアクセスできません。

注：AnyConnectの最初のインストールでは、ユーザに管理者権限が必要です (スタンドアロンの AnyConnect msiパッケージを使用するか、ASAからpkgファイルをプッシュするか) 。 管理者権限がない場合は、これが必要であることを通知するダイアログ ボックスが表示されます。AnyConnect をインストールしたユーザには、以降のアップグレードでは、管理者権限は不要です。

設定

AnyConnect のクライアントを使用して VPN アクセス用に ASA を設定するには、次の手順を実行します。

1. 自己発行証明書を設定する.。
2. SSL VPN Client イメージをアップロードして識別する。
3. Anyconnect アクセスをイネーブルにする。
4. 新規グループ ポリシーを作成する。
5. VPN 接続用にアクセス リスト バイパスを設定する。
6. AnyConnect Client の接続用に接続プロファイルとトンネル グループを作成する。
7. AnyConnect クライアント用に NAT 免除を設定する。

8. ローカル データベースにユーザを追加する。

ステップ 1：自己発行証明書を設定する

デフォルトでは、セキュリティ アプライアンスには、デバイスのリブート時に毎回作成される自己発行証明書が備わっています。Verisign や EntTrust などのベンダーから自身の証明書を購入することもできますが、自身にアイデンティティ証明書を発行するように ASA を設定することもできます。デバイスがリブートしても、この証明書はそのまま残ります。デバイスがリブートしても残る自己発行証明書を作成するには、次の手順を実行します。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. [Certificate Management] を展開し、[Identity Certificates] を選択します。
3. **Add** をクリックし、次に **Add a new identity certificate** オプション ボタンをクリックする。
4. [New] をクリックします。
5. Add Key Pair ダイアログ ボックスで、**Enter new key pair name** オプション ボタンをクリックする。
6. キーペアを識別する名前を入力する。この例では、*sslvpnkeypair* を使用しています。
7. [Generate Now] をクリックします。
8. Add Identity Certificate ダイアログ ボックスで、新しく作成されたキーペアが選択されていることを確認する。
9. Certificate Subject DN には、VPN 終端インターフェイスへの接続に使用される完全修飾のドメイン名（FQDN）を入力する。**CN=sslvpn.cisco.com**
10. **Advanced** をクリックして、Certificate Subject DN フィールドで使用されている FQDN を入力する。例：**FQDN**:sslvpn.cisco.com
11. [OK] をクリックします。
12. **Generate Self Signed Certificate** チェック ボックスをクリックして、次に **Add Certificate** をクリックする。
13. [OK] をクリックします。
14. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
15. **Advanced** を開いて、**SSL Settings** を選択する。
16. Certificates 領域で、SSL VPN（Outside）を終端するのに使用されるインターフェイスを選択し、**Edit** をクリックする。.
17. Certificate ドロップダウン リストで、あらかじめ作成してある自己署名証明書を選択する。
18. [OK] をクリックして、[Apply] をクリックします。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#crypto key generate rsa label
sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
Keypair generation process begin. Please wait...
!--- Generate an RSA key for the certificate. (The name
should be unique. !--- For example, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
!--- Create a trustpoint for the self-issued
certificate. ciscoasa(config-ca-trustpoint)#enrollment
self
```

```
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name
CN=sslvpn.cisco.com
!--- The fully qualified domain name is used for both
fqdn and CN. !--- The name should resolve to the ASA
outside interface IP address. ciscoasa(config-ca-
trustpoint)#keypair sslvpnkeypair
!--- The RSA key is assigned to the trustpoint for
certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm
% The fully-qualified domain name in the certificate
will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside
!--- Assign the trustpoint to be used for SSL
connections on the outside interface.
```

ステップ 2：SSL VPN クライアント イメージをアップロードして識別する

このドキュメントでは、AnyConnect SSL 2.0 のクライアントが使用されています。このクライアントは、Cisco ソフトウェア ダウンロード Web サイトで入手できます。リモート ユーザが使用を計画している各 OS に応じて、別の Anyconnect イメージが必要です。詳細は、『Cisco AnyConnect 2.0 リリース ノート』を参照してください。

AnyConnect クライアントを入手したら、次の手順を実行します。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. **Network (Client) Access** を開いて、次に **Advanced** を開く。
3. **SSL VPN** を開いて、**Client Settings** を選択する。
4. SSL VPN Client Images 領域で、**Add** をクリックし、次に **Upload** をクリックする。
5. AnyConnect のクライアントをダウンロードした場所を表示する。
6. ファイルを選択して、次に **Upload File** をクリックする。クライアントがアップロードされたら、ファイルがフラッシュに正しくアップロードされたことを通知するメッセージが受信されます。
7. [OK] をクリックします。新しくアップロードされたイメージを現在の SSL VPN クライアント イメージとして使用することを確認するダイアログ ボックスが表示されます。
8. [OK] をクリックします。
9. [OK] をクリックして、[Apply] をクリックします。
10. 使用する各 OS 特定の Anyconnect について、このセクションの手順を繰り返します。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-
win-2.0.0343-k9.pkg flash

Address or name of remote host [192.168.50.5]?

Source filename [anyconnect-win-2.0.0343-k9.pkg]?

Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-
k9.pkg...!!!!!!!!!!!!!
```

```
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)
!--- AnyConnect image is downloaded to ASA via TFTP.
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1
!--- Specify the AnyConnect image to be downloaded by
users. The image that is !--- downloaded the most should
have the lowest number. This image uses 1 for the !---
AnyConnect Windows image.
```

ステップ 3：Anyconnect アクセスをイネーブルにする

AnyConnect のクライアントが ASA に接続できるようにするには、SSL VPN 接続を終端するインターフェイスでアクセスをイネーブルする必要があります。この例では、Anyconnect 接続を終端するのに Outside インターフェイスを使用しています。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. **Network (Client) Access** を開いて、次に **SSL VPN Connection Profiles** を選択する。
3. **Enable Cisco AnyConnect VPN Client** チェックボックスにチェックマークを付けます。
4. Outside インターフェイスの **Allow Access** チェック ボックスにチェック マークを入れて、**Apply** をクリックする。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#svc enable
!--- Enable AnyConnect to be downloaded to remote
computers.
```

ステップ 4：新規グループ ポリシーを作成する

グループ ポリシーでは、接続時にクライアントに適用される設定パラメータが指定されます。この例では、*SSLClientPolicy* という名前のグループ ポリシーを作成しています。.

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN をクリックする。**
2. **Network (Client) Access を開いて、Group Policies を選択する。**
3. [Add] をクリックします。
4. **General** を選択して、Name フィールドに **SSLClientPolicy** と入力する、
5. Address Pools の **Inherit** チェックボックスのチェック マークを外す。
6. **Select** をクリックし、次に **Add** をクリックする。[Add IP Pool] ダイアログボックスが表示されます。
7. 現在、ネットワークでは使用されていない IP の範囲からアドレス プールを設定する。この例では、次の値を使用します。**[Name]**：SSLClientPool**Starting IP**

Address：192.168.25.1**Ending IP Address**：192.168.25.50**サブネットマスク**：255.255.255.0

8. [OK] をクリックします。
9. 新しく作成したプールを選択し、**Assign** をクリックする。
10. **OK** をクリックし、次に More Options をクリックする。
11. Tunneling Protocols の **Inherit** チェックボックスのチェック マークを外す。
12. **SSL VPN Client** にチェック マークを入れる。
13. 左側のペインで **Servers** を選択する。
14. DNS Servers の **Inherit** チェックボックスのチェック マークを外し、AnyConnect のクライアントが使用する内部 DNS サーバの IP アドレスを入力する。この例では、*192.168.50.5* を使用しています。
15. **More Options** をクリックする。
16. Default Domain の **Inherit** チェックボックスのチェック マークを外す。
17. 内部ネットワークで使用されているドメインを入力する。例：*tsweb.local*
18. [OK] をクリックして、[Apply] をクリックします。

コマンドラインの例

CiscoASA
ciscoasa(config)#**ip local pool SSLClientPool 192.168.25.1-192.168.25.50 mask 255.255.255.0** *!--- Define the IP pool. The IP pool should be a range of IP addresses !--- not already in use on the internal network.* ciscoasa(config)#**group-policy SSLCLientPolicy internal** ciscoasa(config)#**group-policy SSLCLientPolicy attributes** ciscoasa(config-group-policy)#**dns-server value 192.168.50.5** *!--- Specify the internal DNS server to be used.* ciscoasa(config-group-policy)#**vpn-tunnel-protocol svc** *!--- Specify VPN tunnel protocol to be used by the Group Policy.* ciscoasa(config-group-policy)#**default-domain value tsweb.local** *!--- Define the default domain assigned to VPN users.* ciscoasa(config-group-policy)#**address-pools value SSLClientPool** *!--- Assign the IP pool created to the SSLClientPolicy group policy.*

ステップ 5：VPN 接続用にアクセス リスト バイパスを設定する

このオプションをイネーブルにすると、SSL/IPSec クライアントではインターフェイスのアクセス リストをバイパスできるようになります。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. **Network (Client) Access** を開いて、次に **Advanced** を開く。
3. **SSL VPN** を開いて、**Bypass Interface Access List** を選択する。
4. **Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists** チェック ボックスにチェック マークが入っていることを確認して、Apply をクリックする。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#sysopt connection permit-vpn
!--- Enable interface access-list bypass for VPN
connections. !--- This example uses the vpn-filter
command for access control.

ciscoasa(config-group-policy)#
```

ステップ 6：AnyConnect クライアントの接続用に接続プロファイルとトンネル グループを作成する

VPN クライアントが ASA に接続する際には、接続プロファイルあるいはトンネル グループに接続します。IPSec L2L、IPSec リモート アクセス、クライアントレス SSL、クライアント SSL. などの特定のタイプの VPN 接続のための接続パラメータを定義するためにトンネル グループが使用されます。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. **Network (Client) Access** を開いて、次に **SSL VPN** を開く。
3. **Connection Profiles** を選択し、**Add** をクリックする。
4. **Basic** を選択して、次の値を入力する。**[Name]**：SSLClientProfile**認証**：LOCAL**Default Group Policy**：SSLClientPolicy
5. **SSL VPN Client Protocol** チェックボックスにチェックマークが付いていることを確認する。
6. 左側のペインで **Advanced** を開いて、**SSL VPN** を選択する。
7. Connection Aliases の下で、**Add** をクリックして、ユーザが VPN 接続を関連付けできる名前を入力する。例：*SSLVPNClient*
8. **OK** をクリックし、さらに **OK** をクリックする。
9. ASDM **ウィンドウの下部で Allow user to select connection, identified by alias in the table above at login page** チェック ボックスにチェック マークを入れて、Apply をクリックする。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access
!--- Define tunnel group to be used for VPN remote
access connections. ciscoasa(config)#tunnel-group
SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy
ciscoasa(config-tunnel-general)#tunnel-group
SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable
!--- Assign alias for tunnel group. ciscoasa(config-
tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
!--- Enable alias/tunnel group selection for SSL VPN
connections.
```

ステップ 7：AnyConnect クライアント用に NAT 免除を設定する

SSL VPN クライアントのアクセスを許可する任意の IP アドレスとその範囲には NAT 免除を設定する必要があります。この例では、SSL VPN クライアントは内部 IP の 192.168.50.5 にだけアクセスする必要があります。

注：NAT制御が有効になっていない場合、この手順は必要ありません。確認には **show run nat-control** コマンドを使用します。ASDM で確認するには、**Configuration** をクリックし、**Firewall** をクリックして、**Nat Rules** を選択します。**Enable traffic through the firewall without address translation チェック ボックスにチェック マークが入っている場合は、このステップは省略できます。**

ASDM の手順

1. **Configuration** をクリックし、次に **Firewall** をクリックする。
2. **Nat Rules** を選択し、**Add** をクリックする。
3. **Add NAT Exempt Rule** を選択して、次の値を入力する。**Action:**Exempt**Interface:**内部**送信元**：192.168.50.5**送信先:**192.168.25.0/24**NAT Exempt Direction**：NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (Default)
4. [OK] をクリックして、[Apply] をクリックします。

コマンドラインの例

CiscoASA
ciscoasa(config)#**access-list no_nat extended permit ip host 192.168.50.5 192.168.25.0 255.255.255.0** *!--- Define access list to be used for NAT exemption.* ciscoasa(config)#**nat (inside) 0 access-list no_nat** *!--- Allow external connections to untranslated internal* *!--- addresses defined by access lisy no_nat.* ciscoasa(config)#

ステップ 8：ローカル データベースにユーザを追加する

ローカル認証（デフォルト）を使用している場合、ユーザ認証用のローカル データベースにユーザ名とパスワードを定義する必要があります。

ASDM の手順

1. **Configuration** をクリックし、次に **Remote Access VPN** をクリックする。
2. **AAA Setup** を展開し、**Local Users** を選択する。
3. **Add** をクリックして、次の値を入力する。**ユーザ名:**matthewp**パスワード**：p@ssw0rd**Confirm Password**：p@ssw0rd
4. **No ASDM, SSH, Telnet or Console Access** オプション ボタンを選択する。
5. [OK] をクリックして、[Apply] をクリックします。
6. 追加ユーザに対してこのステップを繰り返し、**Save** をクリックする。

コマンドラインの例

CiscoASA

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
!--- Assign user remote access only. No SSH, Telnet,
ASDM access allowed. ciscoasa(config-username)#write
memory
!--- Save the configuration.
```

確認

このセクションを使用して、SSL VPN 設定が正しく行われたことを確認します。

AnyConnect クライアントで ASA に接続する

クライアントを PC に直接インストールして、ASA の Outside インターフェイスに接続するか、Web ブラウザで https と ASA の FQDN/IP アドレスを入力します。Web ブラウザを使用する場合は、ログインに成功するとクライアントがインストールされます。

SSL VPN クライアント接続を確認する

接続された SSL VPN クライアントを確認するには、**show vpn-sessiondb svc** コマンドを使用します。

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp               Index        : 6
Assigned IP  : 192.168.25.1           Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 35466                  Bytes Rx     : 27543
Group Policy : SSLClientPolicy        Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

ciscoasa(config-group-policy)#
```

vpn-sessiondb logoff name *username* コマンドでは、ユーザ名でユーザをログオフします。接続解除されると、*Administrator Reset* メッセージがユーザに送信されます。

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "matthewp" logged off : 1

ciscoasa(config)#
```

AnyConnect 2.0 のクライアントについての詳細は、『Cisco AnyConnect VPN 管理者ガイド』を参照してください。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティング コマンド (オプション)

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

- **debug webvpn svc 255：WebVPN での SSL VPN クライアントへの接続に関するデバッグ メッセージが表示されます。AnyConnect ログインの成功例**

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:
 SSLVPNClientAccess
, Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host:
10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting
user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE' Processing CSTP header line: 'Cookie:
webvpn=3338474156@28672@119 2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN
cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
164F790435897AC72EE70AE' IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line:
'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-
CSTP-Hostname: wkstation1' - !--- Client desktop hostname Processing CSTP header line: 'X-
CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
                          49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
       B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
                             DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
```

```
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

AnyConnect ログインの失敗例（誤ったパスワード）

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180]
WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749]
webvpn_portal.c:http_webvpn_kill_cookie[627]
```

関連情報

- Cisco AnyConnect VPN Client アドミニストレータ ガイド、バージョン 2.0
- AnyConnect VPN クライアント リリース 2.0 のリリース ノート
- テクニカル サポートとドキュメント – Cisco Systems