複数の WebVPN コンテキスト間でユーザ接続を区別するために使われる Cisco IOS ルータ証明書マップの設定例

目次

概要

このドキュメントでは、証明書マップを使用してルータ上の特定の WebVPN コンテキストへのユーザ接続を認証するセキュア ソケット レイヤ（SSL）VPN 設定のための、Cisco IOS® ルータのサンプル設定を示します。 これは次の二重認証を使用します。 証明書、ユーザ ID とパスワードです。

前提条件

要件

Cisco IOS ルータの SSL VPN 設定に関する知識があることが推奨されます。

使用するコンポーネント

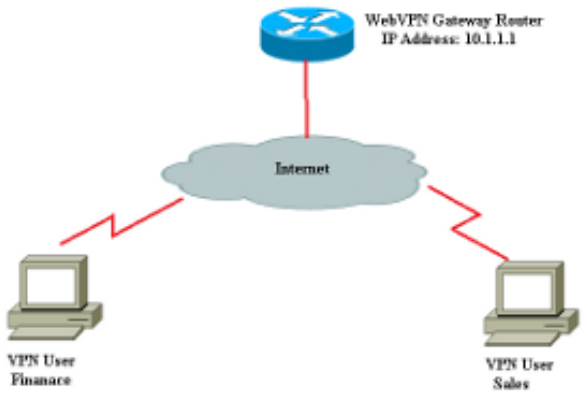
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

> **注意**： 証明書マップの既知の問題には、証明書マップで指定された条件に一致しない証明書を持つユーザが接続可能であるというものがあります。 これは、Cisco Bug ID CSCug39152 に記述されています。 この設定は、このバグの修正が含まれている Cisco IOS ソフトウェア バージョンでのみ動作します。

設定

この項の設定例は、概要に記載された要件を満たすために WebVPN の複数のコンテキストを使用します。 さまざまなグループの各ユーザを認証するには 2 つの要素があります。 証明書、ユーザ ID とパスワードです。 この特定の設定では、ユーザが自身を認証すると、ルータは証明書に設定されている一意の組織単位（OU ）に基づいてエンド ユーザを区別します。

ネットワーク図



ステップ 1： ルータの ID 証明書の生成

ルータは ID 証明書を使用して、SSL VPN に接続するエンド ユーザに自らの ID を示します。 要件に基づいて、ルータが生成した自己署名証明書またはサードパーティの証明書のいずれかを使用できます。

```
Router(config)#crypto key generate rsa label RTR-ID modulus 1024 exportable
The name for the keys will be: RTR-ID

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
Router(config)#
! Generates 1024 bit RSA key pair. "label" defines
! the name of the Key Pair.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(ca-trustpoint)#crypto pki trustpoint RTR-ID
Router(ca-trustpoint)#rsakeypair RTR-ID
Router(ca-trustpoint)#enrollment terminal
Router(ca-trustpoint)#revocation-check none
Router(ca-trustpoint)#exit

Router(config)#crypto pki enroll RTR-ID
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=webvpn.cisco.com,
OU=TSWEB,O=Cisco Systems,C=US,St=California,L=San Jose
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIBjTCB9wIBADAtMRYwFAYDAQQDEw0xNzIuMTYuMTQ2LjE5MRMwEQYJKoZIhvcN
AQkCFgQyODIxMIGfMA0GCSqNSIb3DQEBAQUAA4GNADCBiQKBgQDsdvVNkblT9YkA
0Lthi2fiAeRbyAYRa98kxD5mSHQ3U0gojQ2nvWbI6yqhNP8AZxlC4PNRu0+AyYiY
r44Fst1E3RY0QQVkGjQ7nwlJD7pVi2cFi/SFZssZ/GJmQj6eL8F+YPwU4yzyyEOv
dQtl5Q2aTblOOFe1tVwCdEZqkThKVQIDAQABoCEwHwYJKoZIhvcNAQkOMRIwEDAO
BgNVHQ8BAf8EBAMCBaAwD9YJKoZIhvcNAQEFBQA1gYEAEtnBJDlbu4jReLia6fZH
UlFmFD4Pr0ZhPJsCUSL/CwGYnLjuSWEZkacA2IaG2w6RZWbX/UlEydwYON2I3XiW
z3DIDrygf5YGamkG4DmmO24IHxvkFQd5XKqbIamjWFGwhhLPJxO40MM9CCHSFrYe
dm27yrPawX3aaiHNWn2gatYNBN=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
Router(config)#
```

ステップ 2： 証明書マップの設定

証明書マップを使用して、特定の WebVPN コンテキストへの VPN クライアントの着信接続を分類します。 この分類は証明書マップに設定されている一致基準に基づいて実行されます。 この設定は、エンド ユーザー証明書の OU フィールドを確認する方法を示します。

```
Router#configure terminal
Router(config)#crypto pki certificate map sales 10
Router(ca-certificate-map)# subject-name eq ou = sales
Router(ca-certificate-map)#!
Router(ca-certificate-map)#crypto pki certificate map finance 10
```

```
Router(ca-certificate-map)# subject-name eq ou = finance
Router(ca-certificate-map)#exit
Router(config)#exit
```

注: 証明書マップを設定するときに、同じ証明書マップに複数のインスタンスがある場合は、それらに OR 演算が適用されます。 ただし、証明書マップの同じインスタンスに複数のルールが設定されている場合は、それらに AND 演算が適用されます。 たとえば、この設定では、文字列「Company」を含むサーバによって発行され、サブジェクト名に文字列「DIAL」を含むか、OrganizationUnit コンポーネントに「WAN」を含む証明書が受け入れられます。

crypto pki certificate map Group 10M
issuer-name co Company
subject-name co DIAL
crypto pki certificate map Group 20
issuer-name co Company
subject-name co ou=WAN

ステップ 3： WebVPN ゲートウェイの設定

WebVPN ゲートウェイは、VPN ユーザが接続を開始する場所です。 最も単純な設定では、IP アドレスとこれに関連付けられるトラストポイントが必要です。 関連付けられるトラストポイント「RTR-ID」は、ステップ 1 で WebVPN ゲートウェイで作成されました。

```
Router#configure terminal
Router(config)#webvpn gateway ssl-vpn
Router(config-webvpn-gateway)#ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)#ssl trustpoint RTR-ID
Router(config-webvpn-gateway)#inservice
Router(config-webvpn-gateway)#exit
Router(config)#exit
```

ステップ 4： WebVPN コンテキストの設定

WebVPN コンテキストを使用して、VPN に接続するときに特定のポリシーをエンド ユーザに適用します。 この特定の例では、各グループに異なるポリシーを適用するために「finance」と「sales」という名前の 2 つの異なるコンテキストが作成されました。

```
Router#configure terminal
Router(config)#
Router(config)#webvpn context finance
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group finance-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "finance-vpn-pool" netmask 255.255.255.0
```

```
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)#default-group-policy finance-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain finance
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate finance
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
Router(config)#
Router(config)#webvpn context sales
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group sales-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "sales-vpn-pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)# default-group-policy sales-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain sales
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate sales
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
Router(config)#exit
Router#
```

ステップ 5：ローカル ユーザの設定

2 番目の認証メカニズムの要件を満たすには、ローカル ユーザ名とパスワードを設定します。

```
Router#configure terminal
Router(config)#
Router(config)#webvpn context finance
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group finance-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "finance-vpn-pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)#default-group-policy finance-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain finance
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate finance
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
```

```
Router(config)#
Router(config)#webvpn context sales
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group sales-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "sales-vpn-pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)# default-group-policy sales-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain sales
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate sales
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
Router(config)#exit
Router#
```

最終ルータ設定

```
Router#configure terminal
Router(config)#
Router(config)#webvpn context finance
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group finance-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "finance-vpn-pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)#default-group-policy finance-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain finance
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate finance
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
Router(config)#
Router(config)#webvpn context sales
Router(config-webvpn-context)# secondary-color white
Router(config-webvpn-context)# title-color #669999
Router(config-webvpn-context)# text-color black
Router(config-webvpn-context)# ssl authenticate verify all
Router(config-webvpn-context)#
Router(config-webvpn-context)# policy group sales-vpn-policy
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# timeout idle 3600
Router(config-webvpn-group)# svc address-pool "sales-vpn-pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc keep-client-installed
```

```
Router(config-webvpn-group)# svc split include 10.10.10.0 255.255.255.0
Router(config-webvpn-group)# default-group-policy sales-vpn-policy
Router(config-webvpn-context)# aaa authentication list ClientAuth
Router(config-webvpn-context)# gateway ssl-vpn domain sales
Router(config-webvpn-context)# authentication certificate aaa
Router(config-webvpn-context)# match-certificate sales
Router(config-webvpn-context)# ca trustpoint RTR-ID
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#exit
Router(config)#exit
Router#
```

確認

ここでは、設定が正常に動作していることを確認します。

証明書の確認

```
Router#show crypto ca certificate
Certificate
 Status: Available
 Certificate Serial Number (hex): 6147EE6D000000000009
 Certificate Usage: General Purpose
 Issuer:
   cn=NehalCA
 Subject:
   Name: Router
   hostname=2821
 CRL Distribution Points:
   http://nehnaik-6y59kj7/CertEnroll/NehalCA.crl
 Validity Date:
   start date: 15:36:18 PST Mar 29 2013
   end   date: 15:46:18 PST Mar 29 2014
 Associated Trustpoints: RTR-ID
 Storage: nvram:NehalCA#9.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 17AAB07F3B05139A40D88D1FD325CBB3
 Certificate Usage: Signature
 Issuer:
   cn=NehalCA
 Subject:
   cn=NehalCA
 CRL Distribution Points:
   http://nehnaik-6y59kj7/CertEnroll/NehalCA.crl
 Validity Date:
   start date: 18:28:09 PST Mar 27 2013
   end   date: 18:37:47 PST Mar 27 2018
 Associated Trustpoints: RTR-ID
 Storage: nvram:NehalCA#CBB3CA.cer
```

エンド ユーザ VPN 接続の検証

```
Router#show webvpn session user cisco context all
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.02040

Username          : cisco                 Num Connection : 1
Public IP         : 172.16.89.128         VRF Name       : None                  CA Trustpoint  :
RTR-ID
Context           : finance               Policy Group   : finance-vpn-policy
Last-Used         : 00:00:22              Created        : *11:55:40.851 PST Mon Apr 15 2013
Session Timeout   : Disabled              Idle Timeout   : 3600
DPD GW Timeout    : 300                   DPD CL Timeout : 300
Address Pool      : finance-vpn-pool          MTU Size       : 1199
Rekey Time        : 3600                  Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 172.16.0.1            Netmask        : 255.255.255.0
Rx IP Packets     : 0                     Tx IP Packets  : 0
CSTP Started      : 00:00:16              Last-Received  : 00:00:16
CSTP DPD-Req sent : 0                     Virtual Access : 1
Msie-ProxyServer  : None                  Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 10.10.10.0 255.255.255.0
Client Ports      : 56420
```

```
Router#show webvpn session user cisco context all
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.02040

Username          : cisco                 Num Connection : 2
Public IP         : 172.16.89.128         VRF Name       : None                  CA Trustpoint  :
RTR-ID
Context           : sales                 Policy Group   : sales-vpn-policy
Last-Used         : 00:00:11              Created        : *11:57:24.851 PST Mon Apr 15 2013
Session Timeout   : Disabled              Idle Timeout   : 3600
DPD GW Timeout    : 300                   DPD CL Timeout : 300
Address Pool      : sales-vpn-pool        MTU Size       : 1199
Rekey Time        : 3600                  Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 172.16.1.1            Netmask        : 255.255.255.0
Rx IP Packets     : 0                     Tx IP Packets  : 0
CSTP Started      : 00:00:06              Last-Received  : 00:00:06
CSTP DPD-Req sent : 0                     Virtual Access : 2
Msie-ProxyServer  : None                  Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 10.10.10.0 255.255.255.0
Client Ports      : 49339 49342
```

トラブルシューティング

問題のトラブルシューティングを行うには debug コマンドを使用します。

```
debug webvpn
debug webvpn sdps level 2
debug webvpn aaa
debug aaa authentication
```

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

-

関連情報

- Cisco IOS SSL VPN ゲートウェイとコンテキスト
- テクニカルサポートとドキュメント - Cisco Systems