

Cisco IOS路由器證書對映用於區分多個WebVPN情景之間的使用者連線配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[步驟1.生成路由器身份證書](#)

[步驟2.設定憑證對應](#)

[步驟3.配置WebVPN網關](#)

[步驟4.配置WebVPN上下文](#)

[步驟5.配置本地使用者](#)

[最終路由器配置](#)

[驗證](#)

[憑證驗證](#)

[終端使用者VPN連線驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案為安全套接字層(SSL)VPN設定的Cisco IOS[®]路由器提供範例組態，其中憑證對映用於授權使用者連線到路由器上的特定WebVPN情景。它使用雙重身份驗證：證書、使用者ID和密碼。

必要條件

需求

思科建議您瞭解Cisco IOS路由器上的SSL VPN配置。

採用元件

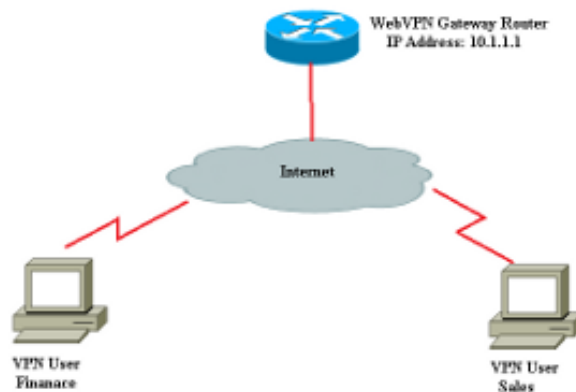
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

注意：證書對映的一個已知問題是，證書與證書對映中指定的條件不匹配的使用者仍然能夠連線。此錯誤記錄在Cisco錯誤ID [CSCug39152](#)中。此設定僅對具有此錯誤的修正程式的Cisco IOS軟體版本有效。

設定

本節中的示例配置使用多個WebVPN上下文以滿足簡介中描述的要求。不同組中的每個使用者都有兩個因素來進行身份驗證：證書、使用者ID和密碼。在此特定組態中，使用者自行驗證後，路由器會根據憑證中檔案中的唯一組織單位(OU)來區分最終使用者。

網路圖表



步驟1.生成路由器身份證書

路由器使用身份證書向連線到SSL VPN的終端使用者顯示其身份。根據您的要求，您可以使用路由器生成的自簽名證書或第三方證書。

```
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)#rsa keypair 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:

MIIBjTCB9wIBADAtMRYwFAYDAQDEw0xNzIuMTYuMTQ2LjE5MRMwEQYJKoZIhvcN
AQkCFgQyODIxMIGfMA0GCSqSIB3DQEBAQUAA4GNADCBiQKBgQDsdvVNkblT9YkA
0Lthi2fiAerbyAYRa98kxD5mSHQ3U0gojQ2nvWbI6yqhNP8AZxlC4PNRu0+AyYiY
r44Fst1E3RY0QQVkjQ7nwlJD7pVi2cFi/SFZssZ/GJmQj6eL8F+YPwU4zyzyEOv
dQt15Q2aTb100FeltVwCdEZqkThKVQIDAQABoCEwHwYJKoZIhvcNAQkOMRIwEDAO
BgNVHQ8BAf8EBAMCBAwD9YJKoZIhvcNAQEFBQA1gYEAETnBJDlbu4jReLia6fZH
UlFmFD4Pr0ZhPJsCUSL/CwGYnLjuSWEZkacA2IaG2w6RZWbX/UlEydwYON2I3XiW
z3DIDrygf5YGamkG4DmmO24IHxvkFQd5XKqbIamjWFGwhhLPJxO40MM9CCHSFrYe
dm27yrPawX3aaiHNWn2gatYBNB=

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

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

```

步驟2.設定憑證對應

證書對映用於將傳入的VPN客戶端連線分類到特定WebVPN上下文。此分類基於證書對映中配置的匹配條件執行。此組態顯示如何檢查終端使用者憑證的OU欄位。

```

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

```

附註：配置證書對映時，如果同一證書對映有多個例項，則跨這些例項應用OR操作。但是，如果在證書對映的同一例項下配置了多個規則，則跨這些規則應用AND操作。例如，在此配置中，將接受由伺服器頒發的任何證書，該證書包含字串"Company"，並且在使用者名稱中包含字串"DIAL"或在OrganizationUnit元件中包含"WAN"：

crypto pki certificate map Group 10M
發行商名稱公司

```
subject-name co DIAL
crypto pki certificate map Group 20
發行商名稱公司
subject-name co ou=WAN
```

步驟3.配置WebVPN網關

WebVPN網關是VPN使用者建立連線的地方。在最簡單的配置中，它需要一個IP地址和一個與之關聯的信任點。關聯的信任點「RTR-ID」是在步驟1中的WebVPN網關下建立的。

```
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
```

步驟4.配置WebVPN上下文

WebVPN上下文用於在連線到VPN時將特定策略應用於終端使用者。在此特定示例中，建立了兩個名為「finance」和「sales」的不同上下文，以對每個組應用不同的策略。

```
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#

```

步驟5.配置本地使用者

為了滿足第二個身份驗證機制的需求，請配置本地使用者名稱和密碼。

```
username cisco password 0 cisco
```

最終路由器配置

```

aaa new-model
!
!
aaa authentication login default local
aaa authentication login ClientAuth local
crypto pki trustpoint RTR-ID
  enrollment terminal
  revocation-check none
  rsakeypair RTR-ID
!
!
crypto pki certificate map sales 10
  subject-name eq ou = sales
!
crypto pki certificate map finance 10
  subject-name eq ou = finance
!
crypto pki certificate chain RTR-ID
  certificate 6147EE6D000000000009
  308203B1 30820299 A0030201 02020A61 47EE6D00 00000000 09300D06 092A8648
  86F70D01 01050500 30123110 300E0603 55040313 074E6568 616C4341 301E170D
  31333033 32393231 33363138 5A170D31 34303332 39323134 3631385A 302D3113
  30110609 2A864886 F70D0109 02130432 38323131 16301406 03550403 130D3137
  322E3136 2E313436 2E313930 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 EC76F54D 91B953F5 8900D0BB 618B67E2 01E45BC8 06116BDF
  24C43E66 48743753 48288D0D A7BD66C8 EB2AA134 FF006719 42E0F351 BB4F80C9
  8898AF8E 05B2DD44 DD163441 05641A34 3B9F0949 0FBA558B 67058BF4 8566CB19
  FC626642 3E9E2FC1 7E60FC14 E32CF2C8 43AF750B 65E50D9A 4DB94E38 57B5B55C
  0274466A 91384A55 02030100 01A38201 70308201 6C300E06 03551D0F 0101FF04
  04030205 A0301D06 03551D0E 04160414 D47F7666 E765C4B1 F85DC0DA 33487D76
  61AF8C6A 301F0603 551D2304 18301680 14DF05DF A0B1B18D ED472F51 AC8F3EF0
  BF53BBE3 F0306F06 03551D1F 04683066 3064A062 A060862D 68747470 3A2F2F6E

```

65686E61 696B2D36 7935396B 6A372F43 65727445 6E726F6C 6C2F4E65 68616C43
412E6372 6C862F66 696C653A 2F2F5C5C 6E65686E 61696B2D 36793539 6B6A375C
43657274 456E726F 6C6C5C4E 6568616C 43412E63 726C3081 A806082B 06010505
07010104 819B3081 98304906 082B0601 05050730 02863D68 7474703A 2F2F6E65
686E6169 6B2D3679 35396B6A 372F4365 7274456E 726F6C6C 2F6E6568 6E61696B
2D367935 396B6A37 5F4E6568 616C4341 2E637274 304B0608 2B060105 05073002
863F6669 6C653A2F 2F5C5C6E 65686E61 696B2D36 7935396B 6A375C43 65727445
6E726F6C 6C5C6E65 686E6169 6B2D3679 35396B6A 375F4E65 68616C43 412E6372
74300D06 092A8648 86F70D01 01050500 03820101 001AD42F D498D6FE 38F1F5DA
88D0F346 3E4598ED FA2E5AE1 4ECF6802 1B50DDB5 8928849A DE8D3477 3E25A42A
231C111B FF9E56DA 63DA513D FDC7E1A6 451ABD08 1D8B4493 72A5DAFF DFE2A44C
1C2A7D10 8182E4F2 BE223A11 6A833A27 9A07FE8F D65AC9E5 DF03D316 90959E59
D9AFB6A2 E977E5AE 62C31D60 F53097EA A84E7FB4 4BB4DBEB 95A104AA 5ED90A6F
6FC5326C F5364AE2 AC35A465 66F577DD 696E2CEE C0728891 2414244C 5103D211
D7A38C21 4A9B08FA FDFC705D 93578050 56D3C1AC 8631EA71 C043D5DE 6272340C
B7F6F986 785ED5BE 8351F87C 1DE8266A 93818EC5 3121951A 6AAD9414 2564DCEE
D14954CE 847EC66B 53769D60 48D91E1A 2C04638E D2

quit

certificate ca 17AAB07F3B05139A40D88D1FD325CBB3

30820372 3082025A A0030201 02021017 AAB07F3B 05139A40 D88D1FD3 25CBB330
0D06092A 864886F7 0D010105 05003012 3110300E 06035504 0313074E 6568616C
4341301E 170D3133 30333238 30303238 30395A17 0D313830 33323830 30333734
375A3012 3110300E 06035504 0313074E 6568616C 43413082 0122300D 06092A86
4886F70D 01010105 00038201 0F003082 010A0282 010100E1 47142E08 7D8D6EF4
80D47525 1A3DBBB2 CBDB487B 1BB79E8C 4205E851 A0DE9958 8AB7B65D D461F8CA
B1FF710B 8A8F60BD 3116B12C 439ADD33 FEE2D383 89672748 9A3D0E18 6A0C3B08
144D1775 C708505D 9FDADBC2 B7932420 339BE558 20970EF1 8C229912 90CC0D27
0459DEB8 7342AE2D EE565BD1 23F877DA 27517E20 6EDADFE8 15DF6B5D 80BD15E8
68CF9E93 C24E315A AA86F55F B22E47D0 75A863B8 1227C6ED A5CBAD2C D98C3009
83F42A11 EB73D887 DA23C85D A4E45779 5F469892 B91CA443 D04E8A9F 31C8FC2C
4342D77A 6A1618EE 8BA1658A 2F2F1CC0 31BAE81A CE1FC437 9D3A0C4D 9B782305
2BD27A83 C7AFB3EC 87C2FFFC D98B0F98 3E2A3FE2 91E1F502 03010001 A381C330
81C0300B 0603551D 0F040403 02018630 0F060355 1D130101 FF040530 030101FF
301D0603 551D0E04 160414DF 05DFA0B1 B18DED47 2F51AC8F 3EF0BF53 BBE3F030
6F060355 1D1F0468 30663064 A062A060 862D6874 74703A2F 2F6E6568 6E61696B
2D367935 396B6A37 2F436572 74456E72 6F6C6C2F 4E656861 6C43412E 63726C86
2F66696C 653A2F2F 5C5C6E65 686E6169 6B2D3679 35396B6A 375C4365 7274456E
726F6C6C 5C4E6568 616C4341 2E63726C 30100609 2B060104 01823715 01040302
0100300D 06092A86 4886F70D 01010505 00038201 01008727 6455D71B B99EF41E
A3783CC2 82AFCB71 D774A5AE 386990E9 96A1F605 A6F31A8C DA9986B4 4B1CC5E9
DB26606F A9FDA997 23276900 DAF3C07A 0A31055E C691E4D4 36D17BD1 46D858A4
9F76D51D 8B758324 9B262FB1 8697B1D2 897DC31B 4DE288D7 70EA00F1 73A8FD5C
CFCAABFB EAAE821D ED530F9E 5DFB9775 7B7D81F5 10837101 8CFED1BA DC22644B
8637BA1B 3E1D2E4C 23780921 5BFB37F5 45FAA721 6CF85027 866FD4CB 19D28D5B
DC7D7A58 DE8855B8 F37703DC FD0B05ED B57D949F 1D8F9D0C DF0FBB4F 011FDC2B
78EFB2FF AF739C75 208CACDB 16BA4179 0414F119 0A33E659 DA9A4D23 155E5BAC
C0814BFB AB1F2A1E 998EE1D4 BA8B2A4D 702B80FB 54AC

quit

!
username cisco password 0 cisco
!
interface GigabitEthernet0/0
ip address 10.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.10.10.1 255.255.255.0
duplex auto
speed auto
!
ip local pool finance-vpn-pool 172.16.0.1 172.16.0.254
ip local pool sales-vpn-pool 172.16.1.1 172.16.1.254
!

```

!
webvpn gateway ssl-vpn
 ip address 10.1.1.1 port 443
 ssl trustpoint RTR-ID
 inservice
!
webvpn context finance
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
!
!
policy group finance-vpn-policy
 functions svc-enabled
 timeout idle 3600
 svc address-pool "finance-vpn-pool" netmask 255.255.255.0
 svc keep-client-installed
 svc split include 10.10.10.0 255.255.255.0
default-group-policy finance-vpn-policy
aaa authentication list ClientAuth
gateway ssl-vpn domain finance
authentication certificate aaa
match-certificate finance
ca trustpoint RTR-ID
inservice
!
!
webvpn context sales
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
!
!
policy group sales-vpn-policy
 functions svc-enabled
 timeout idle 3600
 svc address-pool "sales-vpn-pool" netmask 255.255.255.0
 svc keep-client-installed
 svc split include 10.10.10.0 255.255.255.0
default-group-policy sales-vpn-policy
aaa authentication list ClientAuth
gateway ssl-vpn domain sales
authentication certificate aaa
match-certificate sales
ca trustpoint RTR-ID
inservice
!
end

```

驗證

使用本節內容，確認您的組態是否正常運作。

憑證驗證

```

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

```

終端使用者VPN連線驗證

```

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
```

疑難排解

使用debug命令以排解問題。

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

附註：使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊。](#)

相關資訊

- [Cisco IOS SSL VPN 闡道與環境](#)
- [技術支援與文件 - Cisco Systems](#)