여러 WebVPN 컨텍스트 간의 사용자 연결을 구분하는 데 사용하는 Cisco IOS 라우터 인증서 맵 컨피그레이션 예

목차

소개

이 문서에서는 SSL(Secure Sockets Layer) VPN 컨피그레이션에 대한 Cisco IOS® 라우터의 샘플 컨피그레이션을 제공합니다. 여기서 인증서 맵은 라우터의 특정 WebVPN 컨텍스트에 대한 사용자 연결을 인증하는 데 사용됩니다.이중 인증을 사용합니다.인증서 및 사용자 ID 및 비밀번호.

사전 요구 사항

요구 사항

Cisco에서는 Cisco IOS 라우터에서 SSL VPN 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

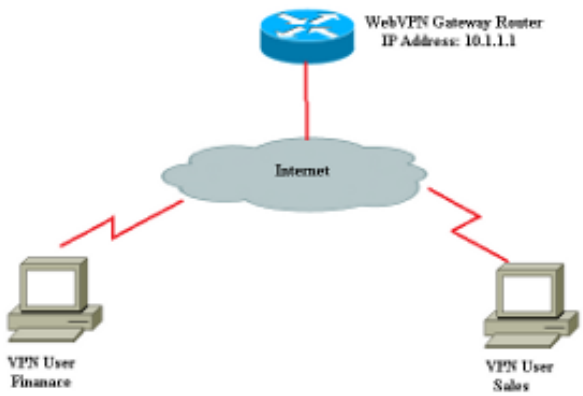
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

> **주의:**인증서 맵의 알려진 문제는 인증서 맵에 지정된 기준과 일치하지 않는 인증서를 가진 사용자가 여전히 연결할 수 있다는 것입니다.이는 Cisco 버그 ID CSCug39152에 설명되어 있습니다. 이 구성은 이 버그에 대한 수정 사항이 있는 Cisco IOS 소프트웨어 버전에서만 작동합니다.

구성

이 섹션의 샘플 컨피그레이션에서는 소개에 설명된 요구 사항을 충족하기 위해 여러 WebVPN 컨텍스트를 사용합니다.다양한 그룹의 각 사용자는 자신을 인증하는 두 가지 요인을 갖습니다.인증서 및 사용자 ID 및 비밀번호.이 특정 컨피그레이션에서 사용자가 자신을 인증하면 라우터는 인증서에 있는 고유한 OU(Organizational Unit)를 기준으로 최종 사용자를 구별합니다.

네트워크 다이어그램



1단계. 라우터 ID 인증서 생성

라우터는 ID 인증서를 사용하여 SSL VPN에 연결하는 최종 사용자에게 ID를 표시합니다.사용자 요구 사항에 따라 라우터에서 생성한 자체 서명 인증서 또는 서드파티 인증서를 사용할 수 있습니다.

```
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)#
```

2단계. 인증서 맵 구성

인증서 맵은 특정 WebVPN 컨텍스트에 대한 수신 VPN 클라이언트 연결을 분류하는 데 사용됩니다 .이 분류는 인증서 맵에 구성된 일치 기준에 따라 수행됩니다.이 구성은 최종 사용자 인증서의 OU 필드를 확인하는 방법을 보여줍니다.

```
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
```

참고:인증서 맵을 구성할 때 동일한 인증서 맵의 여러 인스턴스가 있는 경우 OR 작업이 해당 맵에 적용됩니다.그러나 인증서 맵의 동일한 인스턴스 아래에 여러 규칙이 구성된 경우 AND 작업이 해당 인스턴스에 적용됩니다.예를 들어, 이 컨피그레이션에서는 "Company" 문자열을 포함하고 주체 이름에 "DIAL" 문자열을 포함하거나 OrganizationUnit 구성 요소에 "WAN"을 포함하는 서버에서 발급한 인증서가 수락됩니다.

crypto pki certificate map group 10M
발급자 이름 공동 회사
주체 이름 공동 다이얼
crypto pki 인증서 맵 그룹 20
발급자 이름 공동 회사
subject-name co ou=WAN

3단계. WebVPN 게이트웨이 구성

WebVPN 게이트웨이는 VPN 사용자가 연결을 설정하는 곳입니다.가장 간단한 컨피그레이션에서는 IP 주소와 연결된 신뢰 지점이 필요합니다.연결된 신뢰 지점 "RTR-ID"는 WebVPN 게이트웨이 아래의 1단계에서 생성되었습니다.

```
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
```

4단계. WebVPN 컨텍스트 구성

WebVPN 컨텍스트는 VPN에 연결될 때 최종 사용자에게 특정 정책을 적용하는 데 사용됩니다.이 특정 예에서는 "finance"와 "sales"라는 두 개의 다른 컨텍스트가 생성되어 각 그룹에 서로 다른 정책을 적용합니다.

```
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#
```

5단계. 로컬 사용자 구성

두 번째 인증 메커니즘에 대한 요구 사항을 충족하려면 로컬 사용자 이름과 비밀번호를 구성합니다
.

```
username cisco password 0 cisco
```

최종 라우터 컨피그레이션

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

인증서 확인

```
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
```

최종 사용자 VPN 연결 확인

```
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
```

문제 해결

문제를 해결하려면 debug 명령을 사용합니다.

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

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- Cisco IOS SSL VPN 게이트웨이 및 컨텍스트
- 기술 지원 및 문서 – Cisco Systems