

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapa 1. Gere o certificado de identidade do roteador](#)

[Etapa 2. Configurar os mapas do certificado](#)

[Etapa 3. Configurar o gateway WebVPN](#)

[Etapa 4. Configurar o contexto WebVPN](#)

[Etapa 5. Configurar o usuário local](#)

[Configuração de roteador final](#)

[Verificar](#)

[Verificação de certificado](#)

[Verificação da conexão de VPN do utilizador final](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece uma configuração de exemplo para um roteador do [®] do Cisco IOS para uma configuração de VPN do secure sockets layer (SSL) onde os mapas do certificado sejam usados para autorizar uma conexão do usuário a um contexto sepecific WebVPN no roteador. Utiliza a autenticação dupla: Certificado e usuário - identificação e senha.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da configuração de VPN SSL no Roteadores do Cisco IOS.

[Componentes Utilizados](#)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

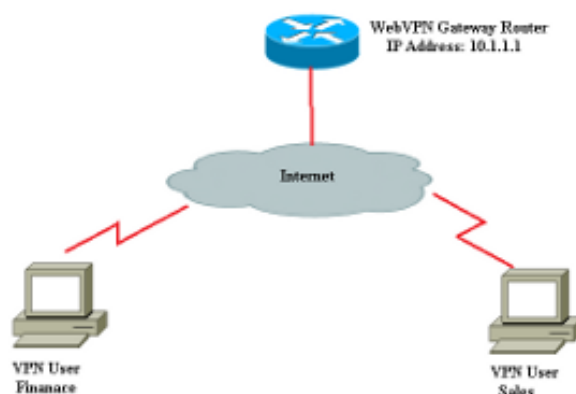
Cuidado: Um problema conhecido com mapas do certificado é que os usuários com Certificados que não combinam os critérios especificados nos mapas do certificado podem

ainda conectar. Isto é documentado na identificação de bug Cisco [CSCug39152](#). Esta configuração trabalha somente nas versões de Software IOS de Cisco que têm o reparo para este erro.

Configurar

A configuração de exemplo nesta seção usa um contexto múltiplo WebVPN a fim satisfazer a exigência descrita na introdução. Cada usuário em vários grupos tem dois fatores para autenticar-se: Certificado e usuário - identificação e senha. Nesta configuração específica, uma vez que os usuários se autenticaram, o roteador diferencia os utilizadores finais baseados em sua unidade organizacional original (OU) arquivada no certificado.

Diagrama de Rede



Etapa 1. Gere o certificado de identidade do roteador

O roteador usa um certificado de identidade para apresentar sua identidade ao utilizador final que conecta ao SSL VPN. Você pode usar um certificado auto-assinado roteador-gerado ou um certificado da terceira baseado em suas exigências.

```
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:

MIIBjTCB9wIBADAtMRYwFAYDAQQDEw0xNzIuMTYuMTQ2LjE5MRMwEQYJKoZIhvcN
AQkCFgQyODIxMIGfMA0GCSqNBSIB3DQEBAQUAA4GNADCBiQKBgQDsdvVNkblT9YkA
0Lthi2fiAeRbyAYRa98kxD5mSHQ3U0gojQ2nvWbI6yqhNP8AZx1C4PNRu0+AyYiY
r44Fst1E3RY0QQVkJGjQ7nwlJD7pVi2cFi/SFzssZ/GJmQj6eL8F+YPwU4yzyyEOv
dQt15Q2aTb100Fe1tVwCgEZqkThKVQIDAQABoCEwHwYJKoZIhvcNAQkOMRIWEDA0
BgNVHQ8BAf8EBAMCBAwAwD9YJKoZIhvcNAQEFBQA1gYEAetnBJD1bu4jReLia6fZHZ
U1FmFD4Pr0ZhPJsCUSL/CwGYNLjuSWEZkacA2IaG2w6RZWBX/U1EydwYON2I3XiW
z3DIDrygf5YGamkG4DmmO24IHxvkFQd5XKqbIamjWFGwhhLPJxO40MM9CCHSFrYe
dm27yrPawX3aaiHNWn2gatYBNB=

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

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

```

Etapa 2. Configurar os mapas do certificado

Um mapa do certificado é usado para classificar conexões de cliente de VPN entrantes aos contextos específicos WebVPN. Esta classificação é executada baseou nos critérios correspondentes configurados no mapa do certificado. Esta configuração mostra como verificar para ver se há o campo OU do certificado do utilizador final.

```

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

```

Nota: Quando você configura mapas do certificado, se há umas múltiplas instâncias o do mesmo mapa do certificado, a seguir OU a operação é aplicada através deles. Contudo, se há umas regras múltiplas configuradas sob a mesma instância de um mapa do certificado, a seguir E a operação é aplicada através delas. Por exemplo, nesta configuração, todo o certificado emitido por um server que contenha a corda “empresa” e contém a corda “SELETOR” no nome do sujeito ou contém “WAN” no componente de OrganizationUnit será

aceitado:

*grupo cripto 10M do mapa do certificado do pki
empresa co do nome de emissor
SELETOR co do assunto-nome
grupo cripto 20 do mapa do certificado do pki
empresa co do nome de emissor
ou=WAN co do assunto-nome*

Etapa 3. Configurar o gateway WebVPN

O gateway WebVPN é onde os usuários VPN aterram suas conexões. Em sua configuração mais simples, exige um endereço IP de Um ou Mais Servidores Cisco ICM NT e um ponto confiável associados com ele. O ponto confiável associado "RTR-ID" foi criado em etapa 1 sob o gateway WebVPN.

```
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
```

Etapa 4. Configurar o contexto WebVPN

O contexto WebVPN é usado para aplicar políticas específicas a um utilizador final quando conectado a um VPN. Neste exemplo específico, dois contextos diferentes nomeados "finança" e "vendas" foram criados para aplicar políticas diferentes a cada grupo.

```
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#

```

Etapa 5. Configurar o usuário local

A fim satisfazer a exigência para um segundo mecanismo da autenticação, configurar o nome de usuário local e a senha.

```

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#
```

Configuração de roteador final

```
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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificação de certificado

```
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
```

Verificação da conexão de VPN do utilizador final

```

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

```

Troubleshooting

Use o comando **debug** a fim pesquisar defeitos o problema.

```

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

```

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Informações Relacionadas

- [Gateways de VPN e contextos do Cisco IOS SSL](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)