Cisco IOS路由器证书地图使用区分多个WebVPN上下文配置示例之间的用户连接

目录

简介

本文为证书地图用于授权对sepecific WebVPN上下文的用户连接路由器的安全套接字协议层(SSL) VPN配置的一个Cisco IOS路由器提供一配置示例。它利用双重验证：证书和用户ID和密码。

先决条件

要求

思科建议您有SSL VPN配置知识在Cisco IOS路由器的。

使用的组件

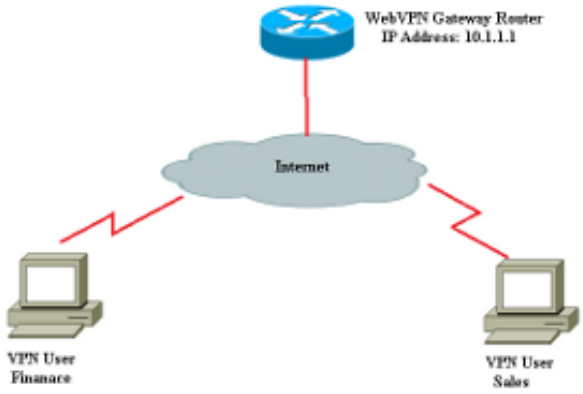
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> **Caution**:一个已知问题用证书地图是有不匹配在证书地图指定的标准的证书的用户能连接。这在Cisco Bug ID CSCug39152描述。此配置只研究有此bug的修正的Cicso IOS软件版本。

配置

在此部分的配置示例使用多个WebVPN上下文为了满足在介绍描述的要求。每个用户以多种组有验证两个的要素：证书和用户ID和密码。在此特定配置中，一旦用户验证，在证书区分最终用户根据他们的唯一组织单位(OU)归档的路由器。

网络图



步骤1.生成路由器身份证书

路由器使用一身份证书提交其标识对连接对SSL VPN的最终用户。您能使用根据您的需求或一第三方证书的一路由器生成的自签名证书。

```
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)#
```

步骤2.配置证书地图

证书地图用于分类对特定WebVPN上下文的流入VPN客户端连接。此分类进行根据在证书地图配置的匹配标准。此配置显示如何检查最终用户证书的OU字段。

```
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
```

Note:当您配置证书地图时，如果有同一张证书地图的多个实例，然后或操作在他们间应用。然而，如果有多个规则配置在证书地图的同一实例下，然后和操作在他们间应用。例如，在此配置方面，包含字符串“公司”的服务器发出的所有证书和包含字符串“拨号”在主题名称或包含“广域网”在OrganizationUnit组件将接受：

crypto pki证书地图组10M
签发方名称co公司

subject-name co拨号
crypto pki证书地图组20
签发方名称co公司
subject-name co ou=WAN

步骤3.配置Webvpn gateway

Webvpn gateway是VPN用户登陆他们的连接的地方。在其简单配置中，它要求IP地址和信任点关联与它。相关的信任点“RTR-ID”在Webvpn gateway下的Step1创建。

```
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
```

步骤4.配置WebVPN上下文

WebVPN上下文用于运用特定策略对最终用户，当连接对VPN。在此特定示例中，名为“金融”和“销售的”两不同的上下文创建运用不同的策略对每组。

```
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#
```

步骤5.配置本地用户

为了满足第二个认证机制的要求，请配置本地用户名和密码。

```
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#
```

最终路由器配置

```
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#
```

验证

使用本部分可确认配置能否正常运行。

证书验证

```
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
```

最终用户VPN连接验证

```
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
```

故障排除

请使用**debug命令**为了排除故障问题。

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

Note:使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- Cisco IOS SSL VPN网关和上下文
- 技术支持和文档 - Cisco Systems