Utilisation de cartes de certificat de routeur Cisco IOS de distinguer la connexion utilisateur entre le plusieurs exemple de configuration de contextes de webvpn

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour un routeur de Cisco IOS® pour une configuration du VPN de Secure Sockets Layer (SSL) où des cartes de certificat sont utilisées pour autoriser une connexion utilisateur à un contexte sepecific de webvpn sur le routeur. Il se sert de la double authentification : Certificat et user-id et mot de passe.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la configuration de VPN SSL sur des routeurs Cisco IOS.

Composants utilisés

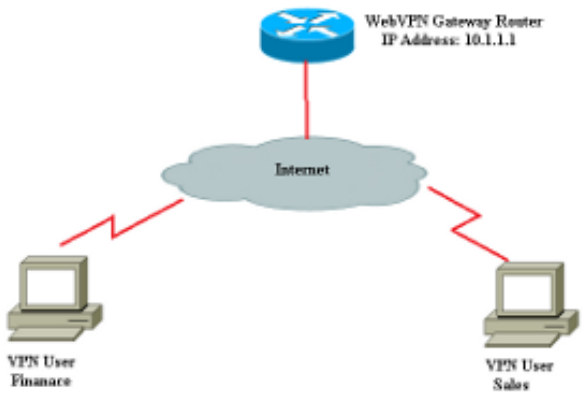
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> **Attention** : Un problème connu avec des cartes de certificat est que les utilisateurs avec les Certificats qui n'apparient pas les critères spécifiés dans les cartes de certificat peuvent encore se connecter. Ceci est documenté dans l'ID de bogue Cisco CSCug39152. Cette configuration travaille seulement sur les versions de logiciel IOS de Cicso qui ont la difficulté pour cette bogue.

Configurez

La configuration d'échantillon dans cette section emploie un plusieurs contexte de webvpn afin de répondre à l'exigence décrite dans l'introduction. Chaque utilisateur dans divers groupes a deux facteurs pour s'authentifier : Certificat et user-id et mot de passe. Dans cette configuration particulière, une fois que les utilisateurs se sont authentifiés, le routeur différencie des utilisateurs finaux basés sur leur seule unité organisationnelle (OU) classée dans le certificat.

Diagramme du réseau



Étape 1. Générez le certificat d'identité de routeur

Le routeur emploie un certificat d'identité pour présenter son identité à l'utilisateur final qui se connecte au VPN SSL. Vous pouvez utiliser un certificat auto-signé routeur-généré ou un tiers certificat basé sur vos conditions requises.

```
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)#
```

Étape 2. Configurez les cartes de certificat

Une carte de certificat est utilisée pour classifier les connexions client VPN entrantes aux contextes spécifiques de webvpn. Cette classification est exécutée a basé sur des critères de correspondance configurés dans la carte de certificat. Cette configuration affiche comment vérifier le champ OU du certificat d'utilisateur.

```
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**: Quand vous configurez des cartes de certificat, s'il y a des multiples instances la de la même carte de certificat, alors OU l'exécution est appliquée à travers elles. Cependant, s'il y a de plusieurs règles configurées sous le même exemple d'une carte de certificat, puis ET l'exécution est appliquée à travers eux. Par exemple, dans cette configuration, n'importe quel certificat délivré par un serveur qui contient la chaîne « société » et contient la chaîne « CADRAN » dans le nom du sujet ou contient le « WAN » dans le composant d'OrganizationUnit sera reçu :
>
> *groupe 10m de crypto pki certificate map*
> *compagnie de l'issuer-name Co*
> *CADRAN du subject-name Co*
> *groupe 20 de crypto pki certificate map*
> *compagnie de l'issuer-name Co*
> *ou=WAN du subject-name Co*

Étape 3. Configurez le webvpn gateway

Le webvpn gateway est où les utilisateurs VPN débarquent leurs connexions. Dans sa configuration plus simple, il exige une adresse IP et un point de confiance associés avec lui. Le point de confiance associé « RTR-ID » a été créé dans l'étape 1 sous le webvpn gateway.

```
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
```

Étape 4. Configurez le contexte de webvpn

Le contexte de webvpn est utilisé pour s'appliquer des stratégies spécifiques à un utilisateur final une fois connecté à un VPN. Dans cet exemple spécifique, deux contextes différents nommés des « finances » et des « ventes » ont été créés pour s'appliquer différentes stratégies à chaque groupe.

```
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#
```

Étape 5. Configurez l'utilisateur local

Afin de répondre à l'exigence pour un deuxième mécanisme d'authentification, configurez le nom d'utilisateur et mot de passe local.

```
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#
```

Configuration de routeur finale

```
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#
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de certificat

```
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
```

Vérification de connexion VPN d'utilisateur 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
```

Dépannez

Employez la commande de **débogage** afin de dépanner le problème.

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

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Informations connexes

- Passerelles et contextes de VPN SSL de Cisco IOS
- Support et documentation techniques - Cisco Systems