Instalar certificado raiz em bordas SDWAN

Contents

Introdução

Este documento descreve como instalar um certificado raiz em SD-WAN Edges com ferramentas diferentes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida pelo software Cisco Catalyst (SD-WAN)
- Certificados
- Linux básico

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

- Validador Cisco Catalyst SD-WAN 20.6.3
- Cisco vEdge 20.6.3

Problema

Um certificado digital é um arquivo eletrônico que certifica a autenticidade de um dispositivo, servidor ou usuário através do uso de criptografia e infraestrutura de chave pública (PKI). A

autenticação de certificação digital ajuda as organizações a garantir que apenas dispositivos e usuários confiáveis possam se conectar a suas redes.

A identidade para roteadores de hardware vEdge é fornecida por um certificado de dispositivo assinado pela Avnet, gerado durante o processo de fabricação e gravado no chip Trusted Platform Module (TPM). Os certificados raiz Symantec/DigiCert e Cisco são pré-carregados em software para confiabilidade dos certificados dos componentes de controle. Certificados raiz adicionais devem ser carregados manualmente, distribuídos automaticamente pelo SD-WAN Manager ou instalados durante o processo de provisionamento automatizado.

Um dos problemas mais comuns na SD-WAN é a falha das conexões de controle devido a um certificado inválido. Isso acontece porque o certificado nunca foi instalado ou porque ele está corrompido.

Para validar a legenda de erro Control Connection, use o comando EXEC show control connections-history.

<#root>

```
vEdge #

show control connections-history


Legend for Errors
ACSRREJ    - Challenge rejected by peer.              NOVMCFG   - No cfg in vmanage for device.
BDSGVERFL  - Board ID Signature Verify Failure.       NOZTPEN   - No/Bad chassis-number entry in ZTP.
BIDNTPR    - Board ID not Initialized.                OPERDOWN  - Interface went oper down.
BIDNTVRFD  - Peer Board ID Cert not verified.         ORPTMO    - Server's peer timed out.
BIDSIG    - Board ID signing failure.                 RMGSPR    - Remove Global saved peer.
CERTEXPRD  - Certificate Expired                      RXTRDWN   - Received Teardown.
CRTREJSER  - Challenge response rejected by peer.     RDSIGFBD  - Read Signature from Board ID failed.


CRTVERFL   - Fail to verify Peer Certificate.

          SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.           SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.                 STNMODETD - Teardown extra vBond in STUN server
DEVALC     - Device memory Alloc failures.            SYSIPCHNG - System-IP changed
DHSTMO     - DTLS HandShake Timeout.                  SYSPRCH   - System property changed
DISCVBD    - Disconnect vBond after register reply.   TMRALC    - Timer Object Memory Failure.
DISTLOC    - TLOC Disabled.                           TUNALC    - Tunnel Object Memory Failure.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer.  TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.                 UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                     UNAUTHEL  - Recd Hello from Unauthenticated peer
HAFAIL     - SSL Handshake failure.                   VBDEST    - vDaemon process terminated.
IP_TOS     - Socket Options failure.                  VECRTREV  - vEdge Certification revoked.
LISFD      - Listener Socket FD Error.                VSCRTREV  - vSmart Certificate revoked.
MGRTBLCKD  - Migration blocked. Wait for local TMO.   VB_TMO    - Peer vBond Timed out.
MEMALCFL   - Memory Allocation Failure.               VM_TMO    - Peer vManage Timed out.
NOACTVB    - No Active vBond found to connect.        VP_TMO    - Peer vEdge Timed out.
NOERR      - No Error.                                VS_TMO    - Peer vSmart Timed out.
NOSLPRCRT  - Unable to get peer's certificate.        XTVMTRDN  - Teardown extra vManage.
NTPRVMINT  - Not preferred interface to vManage.      XTVSTRDN  - Teardown extra vSmart.
STENTRY    - Delete same tloc stale entry.
```

```
PEER     PEER     PEER             SITE       DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP        ID         ID     PRIVATE IP       PORT     PUBLIC IP        PORT
-------------------------------------------------------------------------------------------------------
vbond    dtls     -                0          0      10.10.10.1       12346    10.10.10.1       12346   pu
vbond    dtls     -                0          0      10.10.10.2       12346    10.10.10.2       12346   pu
```

Algumas causas comuns para o rótulo de erro CRTVERFL são:

- A hora de expiração do certificado.
- Root-ca é diferente.
  - Se uma atualização de raiz-ca acontece nos controladores.
  - Uma Autoridade de Certificação (CA) diferente da da Cisco é usada e os dispositivos precisam da instalação manual da CA raiz.
- Alteração da autoridade de certificação na sobreposição.

Observação: para obter mais informações sobre erros de conexões de controle, visite Solução de problemas de conexões de controle SD-WAN.

O arquivo raiz-ca precisa ser exatamente o mesmo em todos os componentes na Sobreposição. Há duas maneiras de validar o arquivo de autoridade de certificação raiz em uso que não é o correto

1. Revise o tamanho do arquivo, o que é útil em situações em que a autoridade de certificação raiz tinha uma atualização.

<#root>

```
vBond:/usr/share/viptela$ ls -l
total 5
-rw-r--r-- 1 root root   294 Jul 23 2022 ISR900_pubkey.der
-rw-r--r-- 1 root root  7651 Jul 23 2022 TPMRootChain.pem
-rw-r--r-- 1 root root 16476 Jul 23 2022 ViptelaChain.pem
-rwxr-xr-x 1 root root 32959 Jul 23 2022 ios_core.pem

-rw-r--r-- 1 root root 24445 Dec 28 13:59 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$ ls -l
total 6
drwxr-xr-x 2 root root   4096 Aug 28  2022 backup_certs
-rw-r--r-- 1 root root   1220 Dec 28 13:46 clientkey.crt
-rw------- 1 root root   1704 Dec 28 13:46 clientkey.pem
-rw------- 1 root root   1704 Dec 28 13:46 proxy.key
-rw-r--r-- 1 root root      0 Aug 28  2022 reverse_proxy_mapping


-rw-r--r-- 1 root root 23228 Aug 28 2022 root-ca.crt
```

2. A segunda e mais confiável maneira de validar que o arquivo é exatamente o mesmo que o arquivo de origem é com o comando md5sum root-ca.crt vshell. Quando o md5 for fornecido, compare o resultado dos componentes Controlador e Dispositivo de borda.

<#root>

vBond:/usr/share/viptela$

md5sum root-ca.crt

a4f945b9a1f50f1fa68d539dcf2e54f2 root-ca.crt

<#root>

vEdge:/usr/share/viptela$

md5sum root-ca.crt

b36358d01b36254a54db2f8db2266ced root-ca.crt

Observação: como o comando md5sum root-ca.crt vshell é usado para verificar a integridade dos arquivos, como virtualmente qualquer alteração em um arquivo faz com que o hash MD5 seja diferente.

Solução

A cadeia de certificados raiz de um dispositivo pode ser instalada com várias ferramentas. Há duas maneiras de instalá-lo com o uso de comandos do Linux.

Criar root-ca com o comando CAT do Linux no vShell

Observação: esse procedimento se aplica a arquivos de raiz-ca que não têm linhas em branco dentro do conteúdo, para situações com linhas em branco usadas no procedimento do editor vi do Linux.

Etapa 1. Obtenha e copie o arquivo root-ca.crt do validador.

A raiz-ca é a mesma em todos os controladores e pode ser copiada de qualquer um deles no caminho /usr/share/viptela/.

<#root>

vBond#

vshell

vBondvBond:~$

cat /usr/share/viptela/root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5NO6tRn/Arr0PO7gi+s3i+zO16zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Etapa 2. Crie o arquivo root-ca.crt na borda.

No vshell, navegue até /home/admin ou /home/<username> e crie o arquivo root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

cat <<"" >> root-ca.crt

```
> -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5NO6tRn/Arr0PO7gi+s3i+zO16zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
```

```
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
>
vEdge:~$
```

Etapa 3. Valide se ele foi concluído.

```
<#root>
vEdge:~$
cat root-ca.crt

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Observação: é importante validar se o arquivo está completo; se não estiver completo, exclua o arquivo com o comando rm root-ca.crt vshell e crie-o novamente a partir da Etapa 2.

Saia do vshell e continue com a Seção.

```
<#root>
vEdge:~$
exit
```

Criar root-ca com o Editor de Texto VI no vShell

Etapa 1. Obtenha e copie o arquivo root-ca.crt do validador.

A raiz-ca é a mesma em todos os controladores e pode ser copiada de qualquer um deles no caminho /usr/share/viptela/.

<#root>

vBond#

vshell

vBond:~$

cat /usr/share/viptela/root-ca.crt

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJO23tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Etapa 2. Crie o arquivo root-ca.crt na borda.

No vshell, navegue até /home/admin ou /home/<username> e crie o arquivo root-ca.crt.

<#root>

vEdge#

vshell

vEdge:~$

cd /usr/share/viptela/

vEdge:~$

pwd

```
/home/admin
vEdge:~$ vi root-ca.crt
```

Quando você clica em Enter, o prompt do editor é exibido.

Etapa 3. Entre no modo de inserção

- Digite: i e cole o conteúdo do certificado da Etapa 1. Role para baixo e valide se o certificado foi concluído.

Etapa 4. Escapar do modo de inserção e salvar certificado.

- Pressione a tecla ESC.
- Digite :wq! seguido por enter para salvar as alterações e sair do editor.

<#root>

vEdge:/usr/share/viptela$

cat root-ca.crt


```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```


Etapa 5. Valide se ele foi concluído.

<#root>

vEdge:~$

cat root-ca.crt


```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

```
vEdge:~$
```

> Observação: é importante validar se o arquivo está completo; se não estiver completo, exclua o arquivo com o comando rm root-ca.crt vshell e crie-o novamente a partir da Etapa 2.

Saia do vshell e continue com a Seção.

<#root>

```
vEdge:~$
```

exit

Instalar certificado

Etapa 1. Instale o certificado de autoridade de certificação raiz com o comando request root-cert-chain install <caminho>.

<#root>

```
vEdge#
```

request root-cert-chain install /home/admin/root-ca.crt

```
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/PKI.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Etapa 2. Valide se ele está instalado com o comando show control local properties.

<#root>

```
vEdge#
```

show control local-properties

```
personality vedge
organization-name organization-name
root-ca-chain-status Installed

certificate-status Installed
certificate-validity Valid
```

```
certificate-not-valid-before Apr 11 17:57:17 2023 GMT
certificate-not-valid-after Apr 10 17:57:17 2024 GMT
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.