

Configuring a LAN-to-LAN Tunnel Between Two VPN 5000 Concentrators with One Acting as a Certificate Generator

Document ID: 5704

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End-of-Sales Announcement.

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram

Generating and Importing Certificates

- Step-by-Step Instructions

Verify

- LAN-to-LAN VPN Tunnel Sample Configurations
- Verification Commands

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

The Cisco VPN 5000 Concentrator can generate certificates for itself and for other VPN 5000 Concentrators instead of having a separate Certificate Authority (CA) server. This document explains how to configure a LAN-to-LAN tunnel between two VPN 5000 Concentrators with one acting as a certificate generator.

Prerequisites

Requirements

There are no specific requirements for this document.

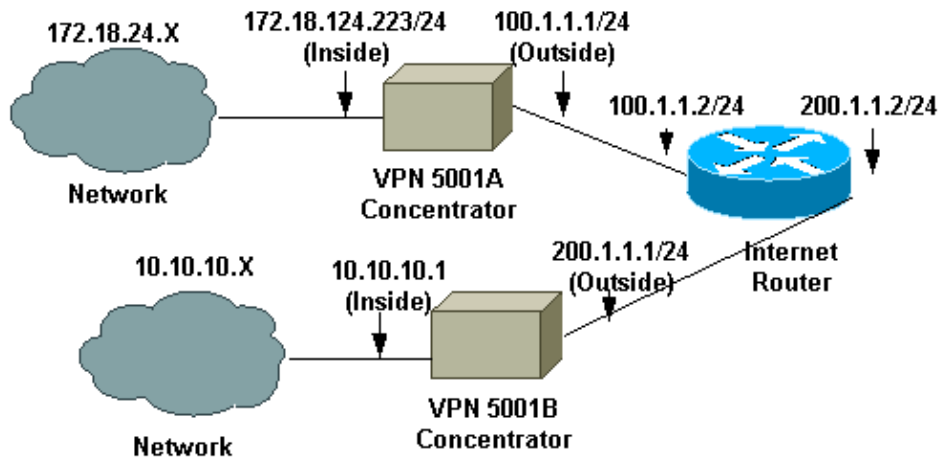
Components Used

The information in this document is based on the Cisco VPN 5000 Concentrator software version 5.2.20US.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram

This document uses the network setup shown in the diagram below.



Generating and Importing Certificates

Step-by-Step Instructions

This example shows how to configure VPN 5001A as a certificate generator.

Note: Ensure that the time and date are set up correctly in your VPN Concentrator before proceeding with your implementation. The time and date can be set using the `sys clock` command.

```
sys clock mm/dd/yy hh:mm
```

1. Configure the certificate generator using the following commands.

The validity period of certificate generator certificates is between 1 and 9999 days. The default is 365 days. You can override this value when you request a certificate using the `certificate generate` command.

```
VPN 5001A# configure certificates
[ Certificates ]# certificategenerator = On
[ Certificates ]# validityperiod = 365
```

2. Use the `certificate generate` command to generate the root certificate in the VPN 5000 Concentrator that is configured as a certificate generator.

```
VPN 5001A# certificate generate root 512 locality rtp state nc country
US organization cisco commonname cisco days 365
Generating Root Certificate
```

Note: The optional days, locality, state, country, organization, and commonname values do not need to match the values in the root certificate or in the certificate requests on the VPN Concentrator.

3. Generate the server certificate in the VPN 5000 Concentrator that is configured as a certificate generator.

```
VPN 5001A# certificate generate server 512 locality rtp state nc country
```

```
US organization cisco commonname cisco days 365
Generating Server Certificate
```

4. Enter the **certificate verify** command to check that the server certificate is valid.

```
VPN 5001A# certificate verify
The certificate has been successfully verified.
```

5. After the root and server certificates are generated in the VPN Concentrator that is configured as a certificate generator, import the certificate to the peer concentrator (VPN 5001B in this case). On VPN 5001A, the root certificate was obtained in PKCS#7 format with the **show certificate pem root** command.

```
VPN 5001A# show certificate pem root
-----BEGIN PKCS7-----
MIAGCSqGSIb3DQEHAqCAMIIBlQIBATEAMIAGAQAANKCCAYMwggF/MIIBKaADAgEC
AgEBMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBACATA3J0cDELMaKGA1UECBMxMx
CzAJBgNVBAYTAlVTMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY21zY28wHhcN
MDEwNTIyMTAxOTA5WhcNMDIwNTIzMTAxOTA5WjBIMQwwCgYDVQQHEwNydHhAczAJ
BgNVBAGTAm5jMQswCQYDVQGEwJVUzEOMAwGA1UEChMFY21zY28xDjAMBGNVBAMT
BWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMBFA5f4treFkTGd2FVsPQw6
vmD8jqLTPGNSRihS9uFF0rUhWj3c9KJlmtgJIW7gGuITVD7Grr40t3aV0jtn0C
AwEAATANBgkqhkiG9w0BAQQFAANBAEdHE+Lx2DMg3fURdrA7/mrcQ5cxFDuPsVwu
XeKB4buH8vaB0Z8/GknkiPvk0e+HGORSTNCvAavUk06J+MqcNRcxAAAAAAA
-----END PKCS7-----
VPN 5001A#
```

This root certificate is imported to the VPN 5001B Concentrator by entering the **certificate import** command and pasting the certificate to the concentrator ending with a period (.) on a line all by itself.

```
VPN 5001B# certificate import

Begin Pasting Certificate Now
To terminate input, enter a . on a line all by itself

-----BEGIN PKCS7-----
MIAGCSqGSIb3DQEHAqCAMIIBlQIBATEAMIAGAQAANKCCAYMwggF/MIIBKaADAgEC
AgEBMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBACATA3J0cDELMaKGA1UECBMxMx
CzAJBgNVBAYTAlVTMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY21zY28wHhcN
MDEwNTIyMTAxOTA5WhcNMDIwNTIzMTAxOTA5WjBIMQwwCgYDVQQHEwNydHhAczAJ
BgNVBAGTAm5jMQswCQYDVQGEwJVUzEOMAwGA1UEChMFY21zY28xDjAMBGNVBAMT
BWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMBFA5f4treFkTGd2FVsPQw6
vmD8jqLTPGNSRihS9uFF0rUhWj3c9KJlmtgJIW7gGuITVD7Grr40t3aV0jtn0C
AwEAATANBgkqhkiG9w0BAQQFAANBAEdHE+Lx2DMg3fURdrA7/mrcQ5cxFDuPsVwu
XeKB4buH8vaB0Z8/GknkiPvk0e+HGORSTNCvAavUk06J+MqcNRcxAAAAAAA
-----END PKCS7-----

.
Root Certificate:
  Serial Number: 1

  Issuer: CN=cisco,O=cisco,C=US,ST=nc,L=rtp
  Subject: CN=cisco,O=cisco,C=US,ST=nc,L=rtp
  Validity
    Not Before: May 22 10:19:09 2001 GMT
    Not After : May 23 10:19:09 2002 GMT
  MD5 Fingerprint: F0:B9:45:B4:B9:65:C0:61:D0:78:3C:3C:29:F5:6B:C9
```

```
Do you want to import this certificate? y
```

6. After importing the root certificate, request a server certificate from the VPN Concentrator that is configured as a certificate generator. To generate this request, use the **certificate generate request** command.


```

-----BEGIN PKCS7-----
MIAGCSqGSIB3DQEHAQCAMIIBlQIBATEAMIAGAQAQAAKCCAYMwggF/MIIBKaADAgEC
AgEDMA0GCSqGSIB3DQEBBAUAMEgxDKABgNVBAcTA3J0cDELMaKGA1UECBMxMx
CzAJBgNVBAYTAlVMTQ4wDAYDVQQKEWVjaXNjbzEOMAwGA1UEAxMFY2l2Y28wHhcN
MDEwNTIyMTAyODExWhcNMDIwNTIzMTAyODExWjBIMQwwCgYDVQQHEwNydHAcCzAJ
BgNVBAGTAm5jMQswCQYDVQQGEwJVUzEOMAwGA1UEChMFY2l2Y28xZjAMBgNVBAMT
BWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALSk36F1DtIQPzdVeGx8J+Zo
cHyGkwtzRplIXTlxWqys93xr5vMHs7U1fti2aLVJ8w0jSgVIZCPYTE54mm249LsC
AwEAATANBgkqhkiG9w0BAQQFAANBAP4o7X1TIjTY7Mk1Y7xttPm7RwO6VphwkMw
HnHfo/TDFcZizayJzKWoIxWBkp2uC6efDOCTxMA8CpoWLOq3JOMxAAAAAA=
-----END PKCS7-----

```

Server Certificate:

Serial Number: 3

Issuer: CN=cisco,O=cisco,C=US,ST=nc,L=rtp

Subject: CN=cisco,O=cisco,C=US,ST=nc,L=rtp

Validity

Not Before: May 22 10:28:11 2001 GMT

Not After : May 23 10:28:11 2002 GMT

MD5 Fingerprint: 8E:62:FE:D1:FD:CB:3B:FE:6A:51:B0:84:1F:2B:A0:05

Do you want to import this certificate? y

pn5001A# **certificate request pending**

Identifier	Requested By	Request Date
0	cisco/O=cisco/C=US/S	5/23/01 10:27:34

Verify

This section provides information you can use to confirm your configuration is working properly.

LAN-to-LAN VPN Tunnel Sample Configurations

VPN 5001A Configuration	
[General]	
DeviceName	= "VPN 5001A"
Ether netAddress	= 00:02:4b:9c:ba:80
DeviceType	= VPN 5001 Concentrator
ConfiguredOn	= 5/27/01 8:12:39
ConfiguredFrom	= Command Line, from Console
IPSecGateway	= 100.1.1.2
EnablePassword	=
Password	=
[IP Ethernet 1]	
SubnetMask	= 255.255.255.0
Mode	= Routed
IPAddress	= 100.1.1.1
[IKE Policy]	
Protection	= MD5_DES_G1
[Tunnel Partner VPN 1]	
KeyManage	= Auto
Mode	= Main
Partner	= 200.1.1.1
LocalAccess	= "172.18.124.0/24"
Peer	= "10.10.10.0/24"

```

Authentication          = On
Certificates             = On
BindTo                  = "ethernet1"
Transform               = esp(md5,des)

[ IP VPN 1 ]
Mode                    = Routed
Numbered                = Off

[ IP Static ]
0.0.0.0 0.0.0.0 100.1.1.2 1 redistrib=none

[ Certificates ]
ValidityPeriod          = 365
CertificateGenerator     = On

[ IP Ethernet 0 ]
IPAddress               = 172.18.124.223
Mode                    = Routed
SubnetMask              = 255.255.255.0

[ Logging ]
Enabled                 = On
Level                   = 7

```

VPN 5001B Configuration

```

[ General ]
EthernetAddress         = 00:00:a5:f0:c9:00
DeviceType              = VPN 5001 Concentrator
ConfiguredOn           = 5/23/01 22:00:19
ConfiguredFrom         = Command Line, from Console
IPSecGateway           = 200.1.1.2
DeviceName              = "VPN 5001b"
EnablePassword          =
Password                =

[ IP Ethernet 1 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 200.1.1.1

[ IP Ethernet 0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 10.10.10.1

[ IKE Policy ]
Protection              = MD5_DES_G1

[ Tunnel Partner VPN 1 ]
KeyManage               = Auto
Mode                    = Main
Transform               = ESP(md5,Des)
BindTo                  = "ethernet1"
Certificates            = On
Authentication          = On
Peer                    = "172.18.124.0/24"
LocalAccess             = "10.10.10.0/24"
Partner                 = 100.1.1.1

[ IP VPN 1 ]
Numbered                = Off

```

```
Mode                                = Routed

[ IP Static ]
0.0.0.0 0.0.0.0 200.1.1.2 1 redist=none
172.18.124.0 255.255.255.0 vpn 1 1 redist=none

[ Logging ]
Level                                = 7
Enabled                              = On
```

Note: Ensure that the [Tunnel Partner VPN 1] section is configured for Main mode. Main and Aggressive are the two IPSec standard methods for performing the Phase 1 negotiation. VPN Concentrators using certificates for LAN-to-LAN tunnel authentication must be configured for Main mode.

Verification Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show configuration** Displays the configuration.
- **show vpn statistics verbose** Provides statistics about the LAN-to-LAN tunnel session, including packets encrypted and decrypted.
- **show certificate installed** Shows certificates installed in the VPN Concentrator.
- **certificate verify** Verifies that the server certificate was installed successfully.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show system log buffer** Displays the contents of the internal log buffer.
- **vpn trace dump all** Displays Internet Key Exchange (IKE) negotiation messages.

Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [VPN 5000 Concentrator Software Configuration Guides](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2007

Document ID: 5704
