Geração e Instalação de Certificados do Cisco VPN 5000 Series Concentrator

Contents

Introduction

Este documento inclui instruções passo a passo sobre como gerar certificados nos Cisco VPN 5000 Series Concentrators e sobre como instalar certificados nos VPN 5000 Clients.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco VPN 5000 Concentrator versão 5.2.16US
- Cisco VPN Client 5.0.12

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Certificados do VPN 5000 Concentrator para VPN Clients

Siga estas etapas.

1. Se você não tiver um servidor de hora, você deve definir a data e a hora usando o comando **sys clock**.

```
RTP-5008# sys clock 12/14/00 12:15
```

Para verificar se a data e a hora foram definidas corretamente, execute o comando **sys date**.

2. Ative o recurso de gerador de certificados do VPN Concentrator.

```
RTP-5008# configure certificates

[ Certificates ]# certificategenerator=on

*[ Certificates ]# validityperiod=365
```

3. Crie o certificado raiz.

```
*RTP-5008# certificate generate root 512 locality rtp state nc
country us organization "cisco" commonname "cisco" days 365
```

4. Crie o certificado do servidor.

```
*RTP-5008# certificate generate server 512 locality rtp state nc
country us organization "cisco" commonname "cisco" days 365
```

5. Verifique o certificado.

```
*RTP-5008# certificate verify
```

6. Exiba o certificado no formato Privacy Enhanced Mail (PEM) e copie o certificado para um editor de texto para exportação para o cliente. Certifique-se de incluir a linha inicial, a linha final e o retorno do carro após a linha final.

```
*RTP-5008# show certificate pem root

-----BEGIN PKCS7-----

MIAGCSqGSIb3DQEHAqCAMIIBmAIBATEAMIAGAQAAAKCCAYYwggGCMIIBLKADAgEC

AgRAP0AJMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBAcTA3J0cDELMAkGA1UECBMC

bmMxCzAJBgNVBAYTAnVzMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY2lzY28o

HhcNMDAwNzE0MDYzOTIzWhcNMDEwNzE0MDYzOTIzWjBIMQwwCgYDVQQHEwNydHAx

CzAJBgNVBAgTAm5jMQswCQYDVQQGEwJ1czEOMAwGA1UEChMFY2lzY28xDjAMBgNV

BAMTBWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAML/buEqz3PnWQ5M6Seq

gE9uf7sZNUbHKZCp+GP9EpRkFuaYCD9vYZ3+MRTphiY55tDRmxTEglvK6l8sYIKd

XDcCAwEAATANBgkqhkiG9w0BAQQFAANBABuRHckNTXEAXSwyj7c5bEnAMCvI4Whd

ZRzVST5/QVRPjcaLXb0QJP47CzNecONfmM0bZ3n2nxBnbNDimJQbCgwxAAAAAAA=

-----END PKCS7-----
```

7. Abra o VPN Client para configurá-lo para autenticação de certificado.
8. Na guia Configuração do VPN Client, selecione **Adicionar**.
9. Selecione **Certificate** para o Login Method e insira o nome de logon e o endereço do servidor VPN principal (ou nome de domínio totalmente qualificado). Adicione uma entrada de servidor VPN secundário, se necessário.
10. Selecione **OK** para fechar a janela Propriedades de login.
11. Vá para **Certificados > Importar**, navegue até o local onde o certificado está localizado e selecione o arquivo do certificado.
12. Com o certificado listado no campo Certificados raiz, clique na guia Configuração do VPN Client.

13. Selecione o botão **Connect** para iniciar uma conexão VPN.

Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- Cisco VPN 5000 Client
- IPSec (IP Security Protocol)
- Suporte Técnico - Cisco Systems