Cliente de AnyConnect VPN (SSL) no IOS Router com exemplo de configuração CCP

Índice

Introdução

Este documento descreve como estabelecer um roteador do ® do Cisco IOS para executar o secure sockets layer (SSL) VPN em uma vara com o Cisco AnyConnect VPN Client que usa o Cisco Configuration Professional (CCP). Esta instalação aplica-se a um caso específico onde AnyConnect no roteador seja configurado com Split Tunneling, e permite o acesso seguro de cliente aos recursos corporativos e igualmente fornece o acesso inseguro ao Internet.

A tecnologia SSL VPN ou WebVPN é apoiada na maioria de plataformas de roteador tais como a geração 1 do roteador dos Serviços integrados (ISR), a geração 2 (consulte o Produtos ISR para a lista de Produtos ISR). Os clientes são recomendados consultar o guia do navegador da característica a fim obter uma lista completa das plataformas do IOS da Cisco que apoiam o cliente de AnyConnect VPN (SSL) (ou alguma outra tecnologia da característica para essa

matéria). Esta informação está disponível no navegador da característica.

O CCP é uma ferramenta de Gerenciamento de dispositivos com base em GUI que permita que você configure roteadores de acesso com base em IOS de Cisco. O CCP é instalado em um PC e simplifica o roteador, a Segurança, as comunicações unificadas, o Sem fio, o WAN, e configurações básicas LAN através dos assistentes com base em GUI, fáceis de usar.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Sistema operacional apropriado do cliente. Consulte os Release Note de AnyConnect para os sistemas operacionalsuportado.
- O navegador da Web com a versão JRE 1.4 do SOL ou mais atrasado ou um ActiveX controlou o navegador
- Privilégios administrativos locais no cliente
- Cisco IOS Router com Advanced Security image -12.4(20)T ou posterior
- Versão 1.3 ou mais recente do Cisco Configuration Professional

Se o Cisco Configuration Professional não é carregado já em seu computador, você pode obter uma cópia gratuita do software e instalar o arquivo do .exe (cisco-config-pro-k9-pkg-2_8-en.zip) do download do software. Para obter informações detalhadas sobre a instalação e a configuração do CCP, consulte o Guia de Início Rápido do Cisco Configuration Professional.

Componentes Utilizados

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

- Roteador da série CISCO2811 do Cisco IOS com versão de software 15.1(4)M8
- Versão 2.8 CCP
- Versão do cliente VPN de Cisco AnyConnect SSL para Windows 3.1.05160

As informações apresentadas 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Tarefas de Pré-configuração

1. Configurar o roteador para o CCP.

   O Roteadores com a licença apropriada do pacote da Segurança já tem o aplicativo CCP carregado no flash. Refira o guia de início rápido do Cisco Configuration Professional a fim obter e configurar o software.

2. Baixe uma cópia do arquivo .pkg de VPN do Anyconnect para seu PC de configuração.

Configurações

Nesta seção, você é presentado com as etapas necessárias a fim configurar as características descritas neste documento. Este exemplo de configuração usa o assistente CCP a fim permitir a operação do Anyconnect VPN no IOS Router.

Conclua estes passos para configurar o AnyConnect VPN no Cisco IOS Router:

1. Estabelecer o CCP e descobre o roteador do Cisco IOS.
2. Instale e permita o software de VPN de Anyconnect no roteador do Cisco IOS.
3. Configurar um contexto SSL VPN e o gateway de VPN SSL com o assistente CCP.
4. Configurar a base de dados de usuário para usuários de Anyconnect VPN.
5. Configurar o túnel completo de AnyConnect.

Cada um destas etapas é descrita com maiores detalhes nas próximas seções deste documento.

Passo 1: Estabelecer o CCP e descobre o roteador do Cisco IOS

1. Clique o **estado do roteador no** indicador CCP a fim ver a informação do dispositivo roteador.

2. O clique **configura** a fim começar a configuração.

Passo 2: Instale e permita o software de VPN de Anyconnect no IOS Router

Termine estas etapas a fim instalar e permitir o software de VPN de Anyconnect no IOS Router:

1. Abra o aplicativo CCP, navegue **para configurar o > segurança**, e clique então o **VPN**.
2. Expanda **SSLVPN** e escolha **Packages**.

   Assegure-o que a licença de recurso SSL VPN está instalada no dispositivo, se não pôde obter o aviso mostrado na imagem anterior. Consulte o link da licença de recurso a fim ver a seção de informação de pedido.

3. No Cisco SSLVPN Client Software, clique em **Browse**.

   A caixa de diálogo seleta do lugar SVC aparece.

4. Especifique o lugar da imagem do Cisco AnyConnect VPN Client (escolha qualquer uma das duas opções disponíveis).

   Se a imagem do Cisco AnyConnect VPN Client está no flash de roteador, clique a caixa de diálogo do botão de rádio do **sistema de arquivos do roteador**, e o clique **consulta.**

   Se a imagem do Cisco AnyConnect VPN Client não está no flash de roteador, clique a caixa de diálogo do rádio do **meu computador**, e o clique **consulta**.

5. Selecione a imagem do cliente que você quer instalar e clicar a **APROVAÇÃO**.
6. Após você especificar o local da imagem do cliente, clique em **Install**.
7. O clique **sim** e clica então a **APROVAÇÃO**.
8. Uma vez que a imagem do cliente é instalada com sucesso, você recebe o mensagem de sucesso. **APROVAÇÃO do** clique a fim continuar.
9. Uma vez que instalado, veja os detalhes do pacote instalado sob a **Segurança > o VPN > o SSL VPN > pacotes**.

Passo 3: Configurar um contexto SSLVPN e o gateway SSLVPN com o assistente CCP

Termine estas etapas a fim configurar um contexto SSL VPN e o gateway de VPN SSL:

1. Vá para **Configure > Security > VPN** e clique em **SSL VPN**.

2. Clique o **gerente SSL VPN** e clique então a aba da **criação SSL VPN**.

3. Siga as alertas a fim permitir o Authentication, Authorization, and Accounting (AAA) se não é permitido já.

4. Verifique a **criação um** botão de rádio **novo SSL VPN** e clique então o **lançamento a tarefa selecionada**.

   A caixa de diálogo SSL VPN Wizard é aberta.

5. Clique em Next.

   Nota: Se o SSL VPN é configurado sob a relação através de que Cisco CP está invocado, pôde causar Cisco CP ao disconnet do roteador. Como uma prática melhor, você pode alcançar o roteador do Cisco IOS através do CCP da interface interna (neste exemplo, 10.106.44.141) ou de toda a outra relação, quando o SSL VPN for configurado sob o FastEthernet0/0 da interface externa (neste exemplo, 10.105.130.149).

6. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway de VPN novo SSL e dê entrada com um nome exclusivo para este contexto SSL VPN.

   Você pode criar contextos diferentes de VPN SSL para o mesmo endereço IP (gateway de VPN SSL), mas cada nome deve ser exclusivo. Este exemplo usa este endereço IP: **https://10.105.130.149/**

7. Clique **em seguida**, e continue à próxima seção.

Passo 4: Configurar o banco de dados de usuários para usuários do Anyconnect VPN

Para autenticação, você pode utilizar um servidor AAA, usuários locais ou ambos. Este exemplo

de configuração usa usuários local-criados para a autenticação.

Conclua estes passos para configurar o banco de dados de usuários para usuários do AnyConnect VPN:

1. Depois que você termina etapa 3, clique **localmente sobre este** botão de rádio do **roteador** situado na caixa de diálogo da autenticação de usuário do wizard VPN SSL.

   Esta caixa de diálogo permite que você adicione usuários ao banco de dados local.

2. Clique **adicionam** e incorporam a informação sobre o usuário.

3. Clique a **APROVAÇÃO** e adicionar usuários adicionais como necessário.

4. Depois que você adiciona os usuários necessários, clique **em seguida**, e continue à próxima seção.

Etapa 5. Configurar o túnel de Anyconnect

Termine estas etapas a fim configurar o túnel de Anyconnect e o pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT para os usuários:

1. Porque Anyconnect fornece o de acesso direto aos recursos do intranet corporativa, a lista URL não é precisada a fim configurar. Clique no **botão Next** localizado na caixa de diálogo Configure Intranet Websites.

2. Certifique-se de que a caixa de verificação **Enable Full Tunnel** esteja marcada.

3. Crie um pool de endereços IP que podem ser utilizados pelos clientes deste contexto de VPN SSL.

   O conjunto de endereço deve corresponder aos endereços disponíveis e ao roteável em seu intranet.

4. Clique as elipses (**...**) ao lado do campo do pool do endereço IP de Um ou Mais Servidores Cisco ICM NT, e escolha **criam um IP pool novo**.

5. Na caixa de diálogo Add IP Local Pool, insira um nome para o pool (por exemplo, *novo*) e clique em **Add**.

6. Na caixa de diálogo do intervalo de endereço IP adicionar, incorpore a escala do conjunto de endereços para os clientes VPN de Anyconnect e clique a **APROVAÇÃO**.

   Nota: Antes da **versão 12.4(20)T**, o pool do endereço IP de Um ou Mais Servidores Cisco ICM NT deve estar em uma escala de uma relação conectada diretamente ao roteador. Se você quer usar uma escala diferente do pool, você pode criar um endereço de loopback associado com seu pool novo a fim satisfazer esta exigência.

7. Clique em **OK**.

8. Configure avançou opções do túnel, tais como o Split Tunneling, o DNS em divisão, os ajustes do proxy do navegador, e os server do Domain Name System (DNS) e do Windows Internet Name Service (VITÓRIAS).

   Nota: Cisco recomenda que você configura pelo menos o DNS e GANHA server.

   Termine estas etapas a fim configurar opções avançadas do túnel, tais como o Split Tunneling:

   Clique no botão **>Advanced Tunnel Options**.

   Clique o **DNS e GANHE server** aba e incorporem os endereços IP primários para o DNS e GANHE server.

   Clique a aba do **Split Tunneling** a fim configurar o Split Tunneling.

   A capacidade de transmitir tráfego protegido e não protegido na mesma interface é conhecida como tunelamento dividido. O tunelamento dividido exige que você especifique exatamente qual tráfego é protegido e qual é o destino desse tráfego. Assim, somente o tráfego especificado entra no túnel, enquanto que o resto é transmitido sem criptografia através da rede pública (Internet).

   No exemplo, o túnel em divisão é configurado a fim incluir o tráfego.

9. Após configurar as opções necessárias, clique **Next**. Escolha a opção de interface de túnel apropriada SSL VPN e clique-a **em seguida**.

10. Personalize a página do portal de VPN SSL ou selecione os valores padrão.

    A página de personalização do portal de VPN SSL permite que você personalize como a

página do portal de VPN SSL é mostrada para seus clientes.

11. Após personalizar a página do portal de VPN SSL, clique **Next**.
12. Clique em Finish.
13. O clique **entrega** a fim salvar sua configuração e clicar então a **APROVAÇÃO**.

    O wizard VPN SSL submete seus comandos ao roteador.

Basicamente estes são os comandos que são entregados do CCP ao roteador:

AAA commands:

```
aaa new-model
aaa authorization exec default local
aaa authentication login default local
line vty 0 4
login authentication default
authorization exec default
exit
```

Remaining commands:

```
aaa authentication login ciscocp_vpn_xauth_ml_1 local
ip local pool IP_Pool 192.168.1.10 192.168.1.15
interface Virtual-Template1
exit
default interface Virtual-Template1
interface Virtual-Template1
no shutdown
ip unnumbered FastEthernet0/0
exit
webvpn gateway gateway_1
ip address 10.105.130.149 port 443
http-redirect port 80
inservice
ssl trustpoint TP-self-signed-1878971148
exit
webvpn context Test
aaa authentication list ciscocp_vpn_xauth_ml_1
gateway gateway_1
virtual-template 1
max-users 1000
inservice
secondary-color white
title-color #FF9900
text-color black
policy group policy_1
```

```
svc split include 10.106.44.0 255.255.255.0
svc keep-client-installed
functions svc-enabled
svc address-pool IP_Pool netmask 255.255.255.255
svc default-domain cisco.com
svc dns-server primary 10.106.44.10
svc wins-server primary 10.106.44.12
exit
default-group-policy policy_1
exit
! IP address / user account command
username user1 privilege 1 secret 0 *********
```

Nota: Se você recebe um Mensagem de Erro, a licença SSL VPN pôde estar incorreta.

Termine estas etapas a fim corrigir uma edição da licença:

1. Vá para **Configure > Security > VPN** e clique em **SSL VPN**.
2. Clique o **gerente SSL VPN** e clique então a aba da **edição SSL VPN no** lado direito.
3. Destaque seu contexto recém-criado e clique o **botão Edit**.
4. No campo do Maximum Number of users, insira o número correto de usuários para sua licença.
5. Clique em **OK** e, em seguida, em **Deliver**.

   Os comandos são escritos ao arquivo de configuração.

Configuração de CLI

O CCP cria estas configurações da linha de comando:

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
```

```
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
redundancy
!
```

```
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
  functions svc-enabled
```

```
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...

Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

Estabelecimento da conexão do AnyConnect VPN Client

Termine estas etapas a fim estabelecer uma conexão de VPN de AnyConnect com o roteador.

> Nota: Adicionar um roteador à lista de sites confiável no internet explorer. Para obter mais informações, consulte Adição de um Security Appliance/Roteador à Lista de Sites Confiáveis (IE).

1. Incorpore a URL ou o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do roteador WebVPN a seu navegador da Web no formato como mostrado.

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
```

```
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
redundancy
!
!
!
!
!
!
!
```

```
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
  functions svc-enabled
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
```

```
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...

Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

OU

```
Router#show running-config
Building configuration...

Current configuration : 3590 bytes
!
! Last configuration change at 06:30:34 UTC Sat Nov 29 2014
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
```

```
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1878971148
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1878971148
 revocation-check none
 rsakeypair TP-self-signed-1878971148
!
!
crypto pki certificate chain TP-self-signed-1878971148
 certificate self-signed 01
 3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31383738 39373131 3438301E 170D3134 31313239 30353537
 32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 38373839
 37313134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100C77D F135BBCA 8A84DE7D A3330085 3694EC3B 9BAE2F94 AF19CAEC 89A4AA6A
 DC098301 AC996CA7 BE1C6AB2 BF4745F4 911E9812 97BC1A1F 15D1AFD0 384878C6
 8781D8A7 3BFCFCFF 5626EF1A BCF73C78 B07E4587 710B6F18 B4E0017F 807606EA
 03E398B0 A2DE06B6 2D39B122 32D82E1B 7AE55554 63D8BDD6 222CF884 C9D5570D
 74BD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
 551D2304 18301680 1455F1A2 00753895 04EB04BE 13273EEF D48D86C6 84301D06
 03551D0E 04160414 55F1A200 75389504 EB04BE13 273EEFD4 8D86C684 300D0609
 2A864886 F70D0101 05050003 81810013 B72A05AE E7816FB7 377FC3B3 8EE7D2AC
 9211B78D 8B6A604A DA7D571F 6E083B78 279F0EB1 95B5ADC8 79572616 53B52B90
 1BF1A39B 46F8C88C 3335F498 E2CF5ABC 5D942A23 7DE35239 04D509EF 88E60201
 8B111BD6 FE82E159 67E05A62 03BFBCA6 E99EA1CE DA52F66A 8CE502C1 B9FAA488
 8A5B022A 3003F718 E8E1C6CC 2EB03C
       quit
!
!
license udi pid CISCO2811 sn FHK1404F3X2
username username privilege 15 secret 5 $1$hPnV$zwQ6MMwLA7HUC/NJRCMyt1
username user1 secret 5 $1$X3Vu$h5/xHipon7Fym16G2SCrz1
!
redundancy
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
!
ip local pool IP_Pool 192.168.1.10 192.168.1.15
ip forward-protocol nd
ip http server
ip http authentication local
```

```
ip http secure-server
!
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.105.130.149 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-1878971148
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-3.1.05160-k9.pkg sequence 1
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
  functions svc-enabled
  svc address-pool "IP_Pool" netmask 255.255.255.255
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc split include 10.106.44.0 255.255.255.0
  svc dns-server primary 10.106.44.10
  svc wins-server primary 10.106.44.12
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 inservice
!
end

Router#sh run int Virtual-Access2
Building configuration...

Current configuration : 104 bytes
!
interface Virtual-Access2
 description ***Internally created by SSLVPN context Test***
 mtu 1406
end
```

2. Insira seu nome de usuário e a senha.

3. Clique o **começo** a fim iniciar a conexão de túnel de Anyconnect VPN.

   Esta janela é mostrada antes da conexão VPN SSL ser estabelecida.

   Nota: O software de ActiveX deve ser instalado em seu computador antes que você transfira o Anyconnect VPN.

4. Assim que a conexão for estabelecida com êxito, clique na guia **Statistics**.

   A guia Statistics exibe informações sobre a conexão SSL.

   As estatísticas detalham a informação estatística detalhada indicadores da conexão da caixa de diálogo, que inclui o estado de túnel e o modo, a duração da conexão, o número de bytes e moldam-na enviado e recebido, informação de endereço, informação do transporte, e o estado da avaliação da postura do Cisco Secure Desktop. O botão Reset nesta guia redefine as estatísticas da transmissão. O botão **Stats da exportação** permite que você exporte as estatísticas atual, a relação, e a tabela de roteamento para um arquivo de texto. O AnyConnect Client pergunta a você um nome e local para o arquivo de texto. O nome padrão é *A* **nyConnect-ExportedStats.txt** e o local padrão está no desktop.

5. Verifique os detalhes da rota (baseados na configuração do túnel em divisão) sob a aba dos **detalhes da rota**.

6. Na caixa de diálogo do Cisco AnyConnect VPN Client, clique **aproximadamente a** aba a fim indicar a informação de versão do Cisco AnyConnect VPN Client.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Comandos

> Nota: A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos no CLI a fim mostrar estatísticas e a outra informação. Para obter informações detalhadas sobre os **comandos show**, consulte Verificação da Configuração do WebVPN.

mostre o contexto todo da sessão do webvnp

```
Router#show webvpn session context all
WebVPN context name: Test
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.106.42.10               1         00:01:22  00:00:01
```

mostre o teste do contexto do usuário1 do usuário da sessão do webvpn

```
Router#show webvpn session user user1 context Test detail
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.05160

Username          : user1                 Num Connection : 1
Public IP         : 10.106.42.10          VRF Name       : None
Context           : Test                  Policy Group   : policy_1
Last-Used         : 00:00:00              Created        : *06:33:24.505 UTC Sat
Nov 29 2014
Session Timeout   : Disabled              Idle Timeout   : 2100
DNS primary serve : 10.106.44.10          WINS primary s : 10.106.44.12
DPD GW Timeout    : 300                   DPD CL Timeout : 300
Address Pool      : IP_Pool               MTU Size       : 1199
Rekey Time        : 3600                  Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.1.10          Netmask        : 255.255.255.255
Rx IP Packets     : 0                     Tx IP Packets  : 617
CSTP Started      : 00:01:22              Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                     Virtual Access : 2
Msie-ProxyServer  : None                  Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 10.106.44.0 255.255.255.0
Client Ports      : 60304

Detail Session Statistics for User:: user1
---------------------------------

CSTP Statistics::
Rx CSTP Frames    : 618               Tx CSTP Frames   : 0
Rx CSTP Bytes     : 46113             Tx CSTP Bytes    : 0
Rx CSTP Data Fr   : 617               Tx CSTP Data Fr  : 0
Rx CSTP CNTL Fr   : 1                 Tx CSTP CNTL Fr  : 0
Rx CSTP DPD Req   : 0                 Tx CSTP DPD Req  : 0
Rx CSTP DPD Res   : 0                 Tx CSTP DPD Res  : 0
Rx Addr Renew Req : 0                 Tx Address Renew : 0
Rx CDTP Frames    : 0                 Tx CDTP Frames   : 0
Rx CDTP Bytes     : 0                 Tx CDTP Bytes    : 0
Rx CDTP Data Fr   : 0                 Tx CDTP Data Fr  : 0
```

```
Rx CDTP CNTL Fr   : 0                Tx CDTP CNTL Fr  : 0
Rx CDTP DPD Req   : 0                Tx CSTP DPD Req  : 0
Rx CDTP DPD Res   : 0                Tx CDTP DPD Res  : 0
Rx IP Packets     : 0                Tx IP Packets    : 617
Rx IP Bytes       : 0                Tx IP Bytes      : 41122

CEF Statistics::
Rx CSTP Data Fr   : 0                Tx CSTP Data Fr  : 0
Rx CSTP Bytes     : 0                Tx CSTP Bytes    : 0
```

mostre o stats do webvpn

```
Router#show webvpn stats
User session statistics:
   Active user sessions     : 1          AAA pending reqs         : 0
   Peak user sessions       : 1          Peak time                : 00:02:29
   Active user TCP conns    : 1          Terminated user sessions : 0
   Session alloc failures   : 0          Authentication failures  : 0
   VPN session timeout      : 0          VPN idle timeout         : 0
   User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 57         Server process rcvd pkts : 0
   Client process sent pkts : 8134       Server process sent pkts : 0
   Client CEF received pkts : 664        Server CEF received pkts : 0
   Client CEF rcv punt pkts : 29         Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 0          Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 0          Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0          SSLVPN eng  bufs inuse   : 0
   Active server TCP conns  : 0

Mangling statistics:
   Relative urls            : 0          Absolute urls            : 0
   Non-http(s) absolute urls: 0          Non-standard path urls   : 0
   Interesting tags         : 0          Uninteresting tags       : 0
   Interesting attributes   : 0          Uninteresting attributes : 0
   Embedded script statement: 0          Embedded style statement : 0
   Inline scripts           : 0          Inline styles            : 0
   HTML comments            : 0          HTTP/1.0 requests        : 0
   HTTP/1.1 requests        : 3          Unknown HTTP version     : 0
   GET requests             : 3          POST requests            : 0
   CONNECT requests         : 0          Other request methods    : 0
   Through requests         : 0          Gateway requests         : 3
   Pipelined requests       : 0          Req with header size >1K : 0
   Processed req hdr bytes  : 844        Processed req body bytes : 0
   HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
   HTML responses           : 0          CSS responses            : 0
   XML responses            : 0          JS responses             : 0
   Other content type resp  : 0          Chunked encoding resp    : 0
   Resp with encoded content: 0          Resp with content length : 0
   Close after response     : 0          Resp with header size >1K: 0
   Processed resp hdr size  : 0          Processed resp body bytes: 0
   Backend https response   : 0          Chunked encoding requests: 0

HTTP Authentication stats :
   Successful NTLM Auth     : 0          Failed NTLM Auth         : 0
   Successful Basic Auth    : 0          Failed Basic Auth        : 0
   Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
   NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
   Oversize NTLM Type3 cred : 0          Internal Error           : 0
   Num 401 responses        : 0          Num non-401 responses    : 0
   Num Basic forms served   : 0          Num NTLM forms served    : 0
```

```
   Num Basic Auth sent      : 0          Num NTLM Auth sent       : 0

CIFS statistics:
 SMB related Per Context:
   TCP VC's                 : 0          UDP VC's                 : 0
   Active VC's              : 0          Active Contexts          : 0
   Aborted Conns            : 0
 NetBIOS related Per Context:
   Name Queries             : 0          Name Replies             : 0
   NB DGM Requests          : 0          NB DGM Replies           : 0
   NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
 SMB related Global:
   Sessions in use          : 0          Mbufs in use             : 0
   Mbuf Chains in use       : 0          Active VC's              : 0
   Active Contexts          : 0          Browse Errors            : 0
   Empty Browser List       : 0          NetServEnum Errors       : 0
   Empty Server List        : 0          NBNS Config Errors       : 0
   NetShareEnum Errors      : 0
 HTTP related Per Context:
   Requests                 : 0          Request Bytes RX         : 0
   Request Packets RX       : 0          Response Bytes TX        : 0
   Response Packets TX      : 0          Active Connections       : 0
   Active CIFS context      : 0          Requests Dropped         : 0
 HTTP related Global:
   Server User data         : 0          CIFS User data           : 0
   Net Handles              : 0          Active CIFS context      : 0
   Authentication Fails     : 0          Operations Aborted       : 0
   Timers Expired           : 0          Pending Close            : 0
   Net Handles Pending SMB  : 0          File Open Fails          : 0
   Browse Network Ops       : 0          Browse Network Fails     : 0
   Browse Domain Ops        : 0          Browse Domain Fails      : 0
   Browse Server Ops        : 0          Browse Server Fails      : 0
   Browse Share Ops         : 0          Browse Share Fails       : 0
   Browse Dir Ops           : 0          Browse Network Fails     : 0
   File Read Ops            : 0          File Read Fails          : 0
   File Write Ops           : 0          File Write Fails         : 0
   Folder Create Ops        : 0          Folder Create Fails      : 0
   File Delete Ops          : 0          File Delete Fails        : 0
   File Rename Ops          : 0          File Rename Fails        : 0
   URL List Access OK       : 0          URL List Access Fails    : 0

Socket statistics:
   Sockets in use           : 1          Sock Usr Blocks in use   : 1
   Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
   Select timers in use     : 1          Sock Select Timeouts     : 0
   Sock Tx Blocked          : 150        Sock Tx Unblocked        : 150
   Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
   Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
   Sock Premature Close     : 0          Sock Pipe Errors         : 13
   Sock Select Timeout Errs : 0

Smart Tunnel statistics:
 Client                               Server
   proc pkts                : 0          proc pkts                : 0
   proc bytes               : 0          proc bytes               : 0
   cef  pkts                : 0          cef  pkts                : 0
   cef  bytes               : 0          cef  bytes               : 0

Port Forward statistics:
 Client                               Server
   proc pkts                : 0          proc pkts                : 0
   proc bytes               : 0          proc bytes               : 0
   cef pkts                 : 0          cef pkts                 : 0
   cef bytes                : 0          cef bytes                : 0
```

```
WEBVPN Citrix statistics:

             Server                   Client
 Packets in  : 0                       0
 Packets out : 0                       0
 Bytes in    : 0                       0
 Bytes out   : 0                       0

ACL statistics:
   Permit web request       : 0          Deny web request         : 0
   Permit cifs request      : 0          Deny cifs request        : 0
   Permit without ACL       : 0          Deny without match ACL   : 0
   Permit with match ACL    : 0          Deny with match ACL      : 0

Single Sign On statistics:
   Auth Requests            : 0          Pending Auth Requests    : 0
   Successful Requests      : 0          Failed Requests          : 0
   Retranmissions           : 0          DNS Errors               : 0
   Connection Errors        : 0          Request Timeouts         : 0
   Unknown Responses        : 0

URL-rewrite splitter statistics:
   Direct access request    : 0          Redirect request         : 0
   Internal request         : 0

Tunnel Statistics:
   Active connections       : 1
   Peak connections         : 1          Peak time                : 00:01:44
   Connect succeed          : 2          Connect failed           : 0
   Reconnect succeed        : 1          Reconnect failed         : 0
   DPD timeout              : 0
 Client
   in  CSTP frames          : 671        in  CSTP control         : 1
   in  CSTP data            : 670        in  CSTP bytes           : 50002
   out CSTP frames          : 0          out CSTP control         : 0
   out CSTP data            : 0          out CSTP bytes           : 0
   in  CDTP frames          : 0          in  CDTP control         : 0
   in  CDTP data            : 0          in  CDTP bytes           : 0
   out CDTP frames          : 0          out CDTP control         : 0
   out CDTP data            : 0          out CDTP bytes           : 0
   cef in  CSTP data frames : 0          cef in  CSTP data bytes  : 0
   cef out CSTP data frames : 0          cef out CSTP data bytes  : 0
   cef in  CDTP data frames : 0          cef in  CDTP data bytes  : 0
   cef out CDTP data frames : 0          cef out CDTP data bytes  : 0
 Server
   In  IP pkts              : 0          In  IP bytes             : 0
   Out IP pkts              : 670        Out IP bytes             : 44587
```

No CCP, escolha o **> segurança > o status VPN > o SSL VPN da monitoração (todos os contextos)** a fim ver as listas de usuários atuais SSL VPN no roteador.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Comandos para Troubleshooting

Vários **comandos clear** estão associados ao WebVPN. Para obter informações detalhadas sobre os comandos show, consulte Verificação da Configuração do WebVPN.

Vários **comandos debug** estão associados ao WebVPN. Para obter informações detalhadas sobre estes comandos, consulte Uso de Comandos de Depuração do WebVPN.

> Nota: O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

Informações Relacionadas

- Cisco IOS SSLVPN
- Perguntas frequentes sobre AnyConnect VPN Client
- Guia do administrador do Cisco AnyConnect VPN Client
- SSL VPN - WebVPN
- Exemplo de Configuração de VPN SSL Sem Clientes (WebVPN) no Cisco IOS com SDM
- Exemplo de Configuração de VPN SSL com Thin-Client (WebVPN) no Cisco IOS com SDM
- Guia de Implantação de WebVPN e Convergência DMVPN
- Suporte Técnico e Documentação - Cisco Systems