AnyConnect: Configurar VPN SSL Básica para o Headend do Cisco IOS Router com CLI

Introduction

Contents

Este documento descreve a configuração básica de um Cisco IOS® Router como headend da VPN SSL (Secure Sockets Layer VPN) do AnyConnect.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS
- AnyConnect Secure Mobility Client
- Operação geral de SSL

Componentes Utilizados

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

- Roteador Cisco 892W executando 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.08009

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

Informações de Apoio

Informações de licenciamento para versões diferentes do IOS

- O conjunto de recursos securityk9 é necessário para usar os recursos de VPN SSL, independentemente da versão do Cisco IOS usada.
- Cisco IOS 12.x - o recurso SSL VPN é integrado em todas as imagens 12.x que começam com 12.4(6)T e que têm pelo menos uma licença de segurança (por exemplo, advsecurityk9, adventerprise9 e assim por diante).
- Cisco IOS 15.0 - versões anteriores exigem que um arquivo LIC seja instalado no roteador, o que permitirá conexões de 10, 25 ou 100 usuários. Licenças com direito de uso* foram implementadas em 15.0(1)M4
- Cisco IOS 15.1 - versões anteriores exigem que um arquivo LIC seja instalado no roteador, o que permitirá conexões de 10, 25 ou 100 usuários. Licenças com direito de uso* foram implementadas em 15.1(1)T2, 15.1(2)T2, 15.1(3)T e 15.1(4)M1
- Cisco IOS 15.2 - todas as versões 15.2 oferecem licenças de direito de uso* para SSLVPN
- O Cisco IOS 15.3 e mais avançado - as versões anteriores oferecem as licenças de direito de uso*. A partir do 15.3(3)M, o recurso SSLVPN estará disponível após você inicializar em um pacote de tecnologia securityk9

Para licenciamento RTU, uma licença de avaliação será ativada quando o primeiro recurso webvpn for configurado (ou seja, gateway webvpn GATEWAY1) e o Contrato de Licença de Usuário Final (EULA) tiver sido aceito. Após 60 dias, essa licença de avaliação se torna uma licença permanente. Essas licenças são baseadas em honra e exigem a compra de uma licença em papel para usar o recurso. Além disso, em vez de se limitar a um determinado número de usos, a RTU permite o número máximo de conexões simultâneas que a plataforma do roteador pode suportar simultaneamente.

Melhorias significativas de software

Esses IDs de bug resultaram em recursos ou correções significativos para o AnyConnect:

- CSCti89976: Suporte adicionado para AnyConnect 3.x ao IOS
- CSCtx38806: Correção para vulnerabilidade BEAST, Microsoft KB2585542

Configurar

Etapa 1. Confirmar se a licença está ativada

A primeira etapa quando o AnyConnect é configurado em um headend do IOS Router é confirmar se a licença foi instalada corretamente (se aplicável) e ativada. Consulte as informações de licenciamento na seção anterior para obter as especificações de licenciamento em versões diferentes. Depende da versão do código e da plataforma se o comando show license lista uma licença SSL_VPN ou securityk9. Independentemente da versão e da licença, o EULA precisará ser aceito e a licença será mostrada como Ativo.

Etapa 2. Fazer upload e instalar o pacote do AnyConnect Secure Mobility Client no roteador

Para carregar uma imagem do AnyConnect para a VPN, o headend tem duas finalidades. Em primeiro lugar, somente os sistemas operacionais com imagens do AnyConnect presentes no headend do AnyConnect poderão se conectar. Por exemplo, os clientes Windows exigem que um pacote Windows seja instalado no headend, os clientes Linux de 64 bits exigem um pacote Linux de 64 bits e assim por diante. Em segundo lugar, a imagem do AnyConnect instalada no headend será automaticamente empurrada para baixo para a máquina cliente na conexão. Os usuários que se conectarem pela primeira vez poderão fazer o download do cliente no portal da Web e os usuários que retornarem poderão fazer o upgrade, desde que o pacote do AnyConnect no headend seja mais recente do que o instalado em sua máquina cliente.

Os pacotes do AnyConnect podem ser obtidos através da seção AnyConnect Secure Mobility Client do site Cisco Software Downloads. Embora haja muitas opções disponíveis, os pacotes a serem instalados no headend serão rotulados com o sistema operacional e a implantação do Head-end (PKG). Os pacotes do AnyConnect estão disponíveis no momento para essas plataformas de sistema operacional: Windows, Mac OS X, Linux (32 bits) e Linux de 64 bits. Observe que, para Linux, há pacotes de 32 e 64 bits. Cada sistema operacional exige que o pacote apropriado seja instalado no headend para permitir conexões.

Depois que o pacote do AnyConnect tiver sido baixado, ele poderá ser carregado na memória flash do Roteador com o comando **copy** via TFTP, FTP, SCP ou algumas outras opções. Aqui está um exemplo:

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0):
!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]

37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

Depois de copiar a imagem do AnyConnect para a flash do Roteador, ela deve ser instalada através da linha de comando. Vários pacotes do AnyConnect podem ser instalados quando você especifica um número de sequência no final do comando de instalação; isso permitirá que o Roteador atue como headend para vários sistemas operacionais clientes. Ao instalar o pacote do AnyConnect, ele também o moverá para o **diretório flash:/webvpn/** se não tiver sido copiado lá

inicialmente.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1

SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

Nas versões do código que foram lançadas antes de 15.2(1)T, o comando para instalar o PKG é ligeiramente diferente.

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

Etapa 3. Gerar um par de chaves RSA e certificado autoassinado

Ao configurar SSL ou qualquer recurso que implemente PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) e certificados digitais, um par de chaves Rivest-Shamir-Adleman (RSA) é necessário para a assinatura do certificado. Esse comando gerará um par de chaves RSA que será usado quando o certificado PKI autoassinado for gerado. Use um módulo de 2048 bits, não é um requisito, mas é recomendável usar o maior módulo disponível para maior segurança e compatibilidade com as máquinas cliente AnyConnect. Também é recomendável usar um rótulo de chave descritiva que será atribuído com o gerenciamento de chaves. A geração de chave pode ser confirmada com o comando **show crypto key mypubkey rsa**.

> **Note**: Como há muitos riscos de segurança associados a tornar as chaves RSA exportáveis, a prática recomendada é garantir que as chaves sejam configuradas para não serem exportáveis, o que é o padrão. Os riscos envolvidos quando você torna as chaves RSA exportáveis são discutidos neste documento: Implantação de chaves RSA em um PKI.

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048

The name for the keys will be: SSLVPN_KEYPAIR

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

show crypto key mypubkey rsa SSLVPN_KEYPAIR

% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAFA936 5C866DE8 5184D2D3
```

```
6D020301 0001
```

Depois que o par de chaves RSA tiver sido gerado com êxito, um ponto de confiança PKI deve ser configurado com as informações do roteador e o par de chaves RSA. O nome comum (CN) no nome do assunto deve ser configurado com o endereço IP ou o nome de domínio totalmente qualificado (FQDN) que os usuários usam para se conectar ao gateway do AnyConnect; neste exemplo, os clientes usam o FQDN de fdenofa-SSLVPN.cisco.com quando tentam se conectar. Embora não seja obrigatório, quando você digita corretamente no CN, ele ajuda a reduzir o número de erros de certificado solicitados no login.

> **Note**: Em vez de usar um certificado autoassinado gerado pelo roteador, é possível usar um certificado emitido por uma CA de terceiros. Isso pode ser feito por meio de alguns métodos diferentes conforme discutido neste documento: Configuring Certificate Enrollment for a PKI.

```
crypto pki trustpoint SSLVPN_CERT
 enrollment selfsigned
 subject-name CN=fdenofa-SSLVPN.cisco.com
 rsakeypair SSLVPN_KEYPAIR
```

Depois que o ponto de confiança tiver sido definido corretamente, o roteador deve gerar o certificado usando o comando **crypto pki enroll**. Com esse processo, é possível especificar alguns outros parâmetros, como o número de série e o endereço IP. No entanto, isso não é necessário. A geração de certificado pode ser confirmada com o comando **show crypto pki certificate**.

```
crypto pki enroll SSLVPN_CERT

% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
    end   date: 20:00:00 EDT Dec 31 2019
  Associated Trustpoints: SSLVPN_CERT
```

Etapa 4. Configurar contas de usuário de VPN local

Embora seja possível usar um servidor AAA (External Authentication, Authorization, and Accounting, Autenticação, Autorização e Contabilidade) externo, para este exemplo é usada a autenticação local. Esses comandos criarão um nome de usuário VPNUSER e também uma lista de autenticação AAA chamada SSLVPN_AAA.

```
aaa new-model
aaa authentication login SSLVPN_AAA local
username VPNUSER password TACO
```

Etapa 5. Definir pool de endereços e lista de acesso de túnel dividido a serem usados pelos clientes

Um pool de endereços IP local deve ser criado para que os adaptadores clientes AnyConnect obtenham um endereço IP. Certifique-se de configurar um pool grande o suficiente para suportar o número máximo de conexões simultâneas de cliente AnyConnect.

Por padrão, o AnyConnect operará no modo de túnel completo, o que significa que todo o tráfego gerado pela máquina cliente será enviado através do túnel. Como isso geralmente não é desejável, é possível configurar uma ACL (Access Control List, lista de controle de acesso) que define o tráfego que deve ou não ser enviado pelo túnel. Como em outras implementações de ACL, o deny implícito no final elimina a necessidade de uma negação explícita; portanto, é necessário configurar somente instruções permit para o tráfego que deve ser encapsulado.

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Etapa 6. Configurar a Virtual-Template Interface (VTI)

VTIs dinâmicos fornecer uma interface de Acesso Virtual separada sob demanda para cada sessão VPN que permita conectividade altamente segura e escalável para VPNs de acesso remoto. A tecnologia DVTI substitui os mapas de criptografia dinâmicos e o método dinâmico hub-and-spoke que ajuda a estabelecer túneis. Como os DVTIs funcionam como qualquer outra interface real, eles permitem uma implantação de Acesso Remoto mais complexa porque suportam QoS, firewall, atributos por usuário e outros serviços de segurança assim que o túnel está ativo.

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
 ip unnumbered Loopback0
```

Passo 7. Configurar o Gateway WebVPN

O WebVPN Gateway é o que define o endereço IP e a(s) porta(s) que serão usados pelo headend do AnyConnect, bem como o algoritmo de criptografia SSL e o certificado PKI que serão apresentados aos clientes. Por padrão, o Gateway suportará todos os possíveis algoritmos de criptografia, que variam dependendo da versão do Cisco IOS no roteador.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

Etapa 8. Configurar o contexto e a política de grupo do WebVPN

O contexto e a política de grupo do WebVPN definem alguns parâmetros adicionais que serão usados para a conexão do cliente AnyConnect. Para uma configuração básica do AnyConnect, o contexto serve simplesmente como um mecanismo usado para chamar a política de grupo padrão que será usada para o AnyConnect. No entanto, o Contexto pode ser usado para personalizar ainda mais a página inicial WebVPN e a operação WebVPN. No Grupo de políticas definido, a lista SSLVPN_AAA é configurada como a lista de autenticação AAA da qual os usuários são membros. O comando **function svc-enabled** é a parte da configuração que permite que os usuários se conectem ao AnyConnect SSL VPN Client em vez de apenas WebVPN através de um navegador. Por fim, os comandos SVC adicionais definem parâmetros que são relevantes somente para conexões SVC: **svc address-pool** diz ao Gateway para distribuir endereços no SSLVPN_POOL para os clientes, **svc split include** define a política de split tunnel por ACL 1 definida acima, e **svc dns-server** define o servidor DNS que será usado para a resolução de nomes de domínio. Com essa configuração, todas as consultas DNS serão enviadas ao servidor DNS especificado. O endereço que é recebido na resposta da consulta determinará se o tráfego é enviado pelo túnel.

```
webvpn context SSLVPN_CONTEXT
virtual-template 1
 aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY inservice
policy group SSLVPN_POLICY functions svc-enabled svc address-pool "SSLVPN_POOL" netmask
255.255.255.0 svc split include acl 1 svc dns-server primary 8.8.8.8
default-group-policy SSLVPN_POLICY
```

Etapa 9 (Opcional) Configurar um perfil de cliente

Ao contrário dos ASAs, o Cisco IOS não tem uma interface GUI integrada que possa auxiliar os administradores na criação do perfil do cliente. O perfil do cliente AnyConnect precisa ser criado/editado separadamente com o Editor de perfis independente.

> **Tip**: Procure anyconnect-profileeditor-win-3.1.03103-k9.exe.

Siga estes passos para que o Roteador implante o perfil:

- Faça o upload para a Flash do IOS com o uso de ftp/tftp.
- Use este comando para identificar o perfil que acabou de ser carregado:

```
crypto vpn annyconnect profile SSLVPN_PROFILE flash:test-profile.xml
```

> **Tip**: Em versões do Cisco IOS anteriores a 15.2(1)T, este comando precisa ser usado: **webvpn import svc profile <profile_name> flash:<profile.xml>**

3. Sob o contexto, use este comando para vincular o perfil a esse contexto:

```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

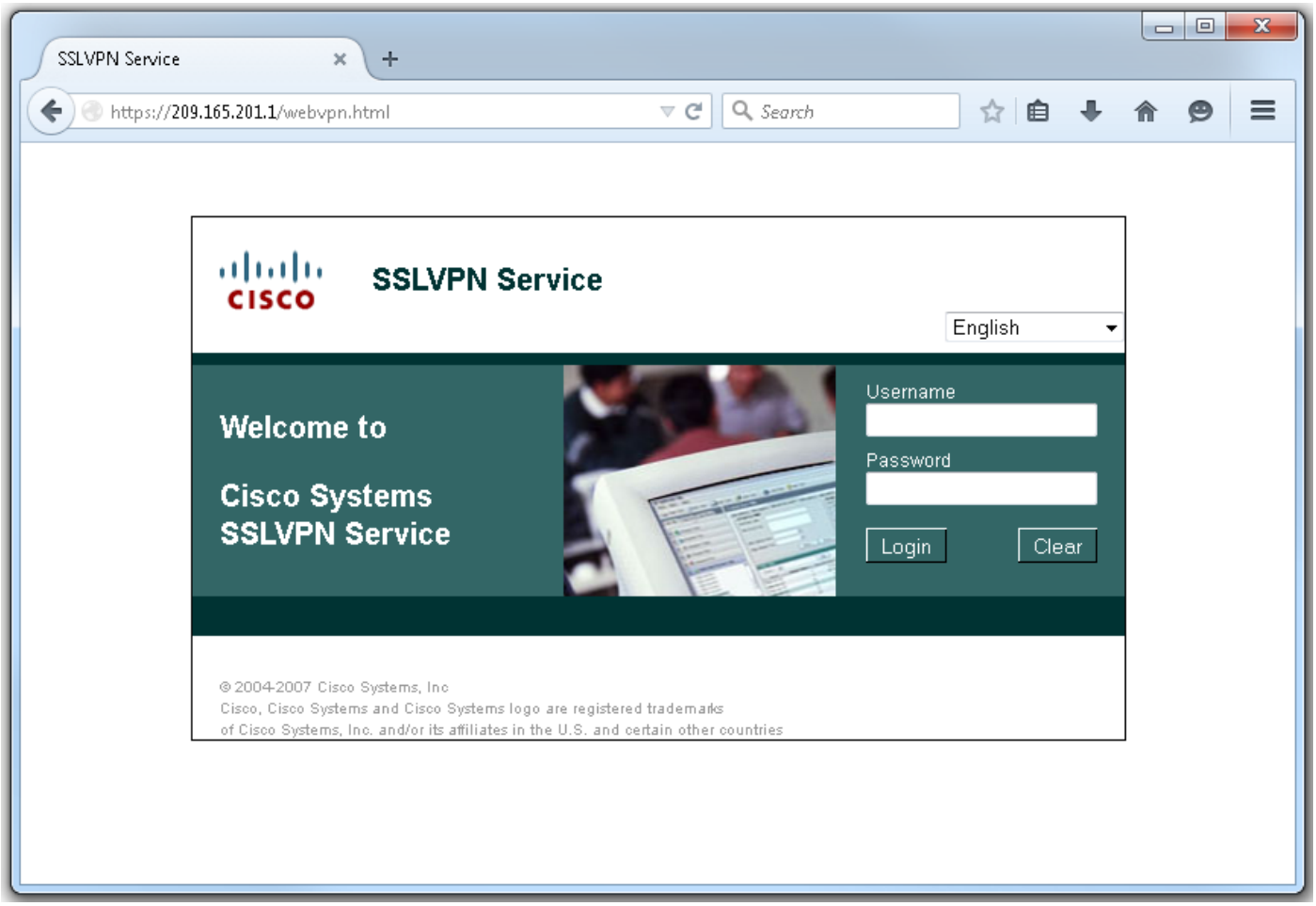
> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais

informações sobre os comandos usados nesta seção.

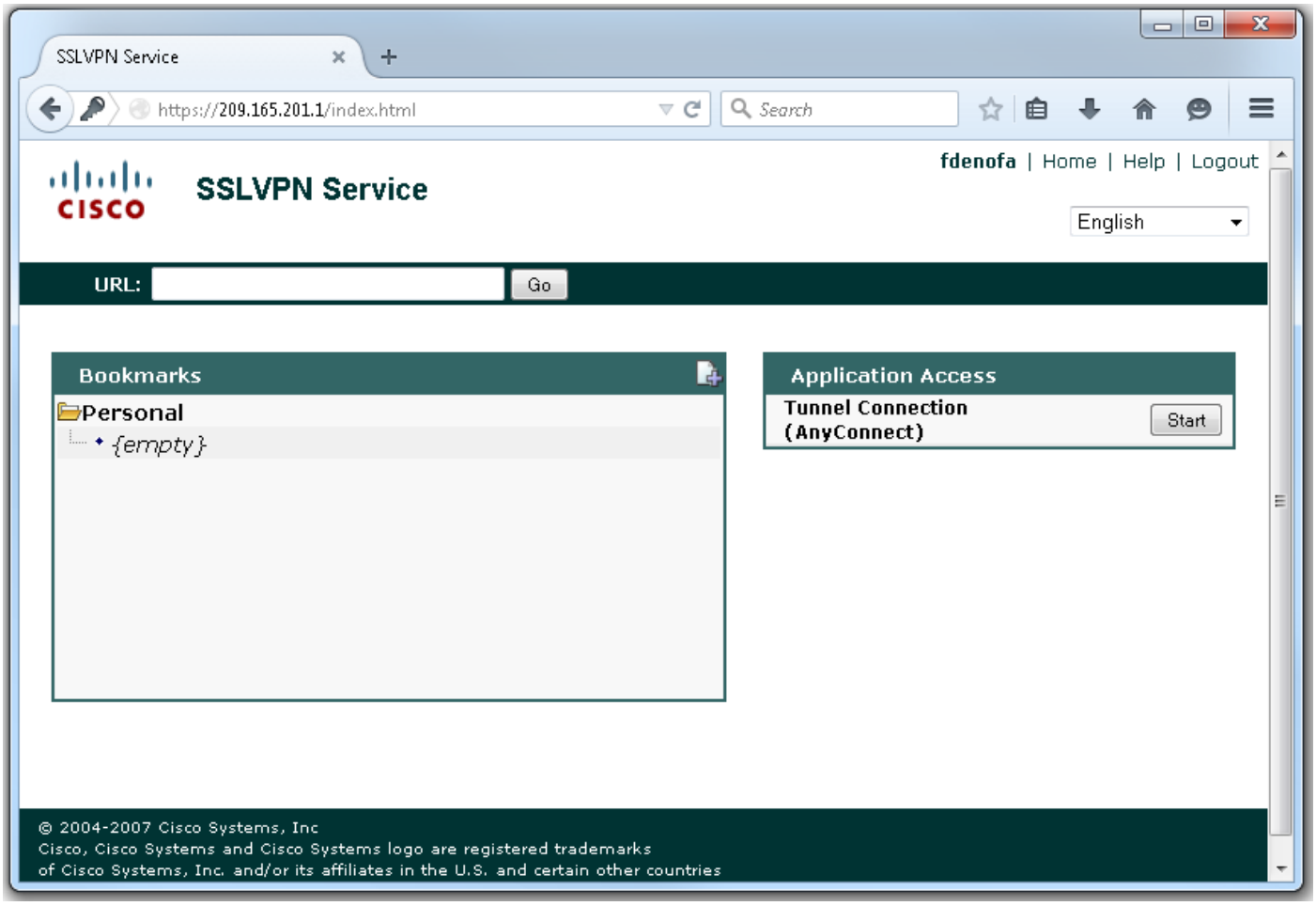
Verificar

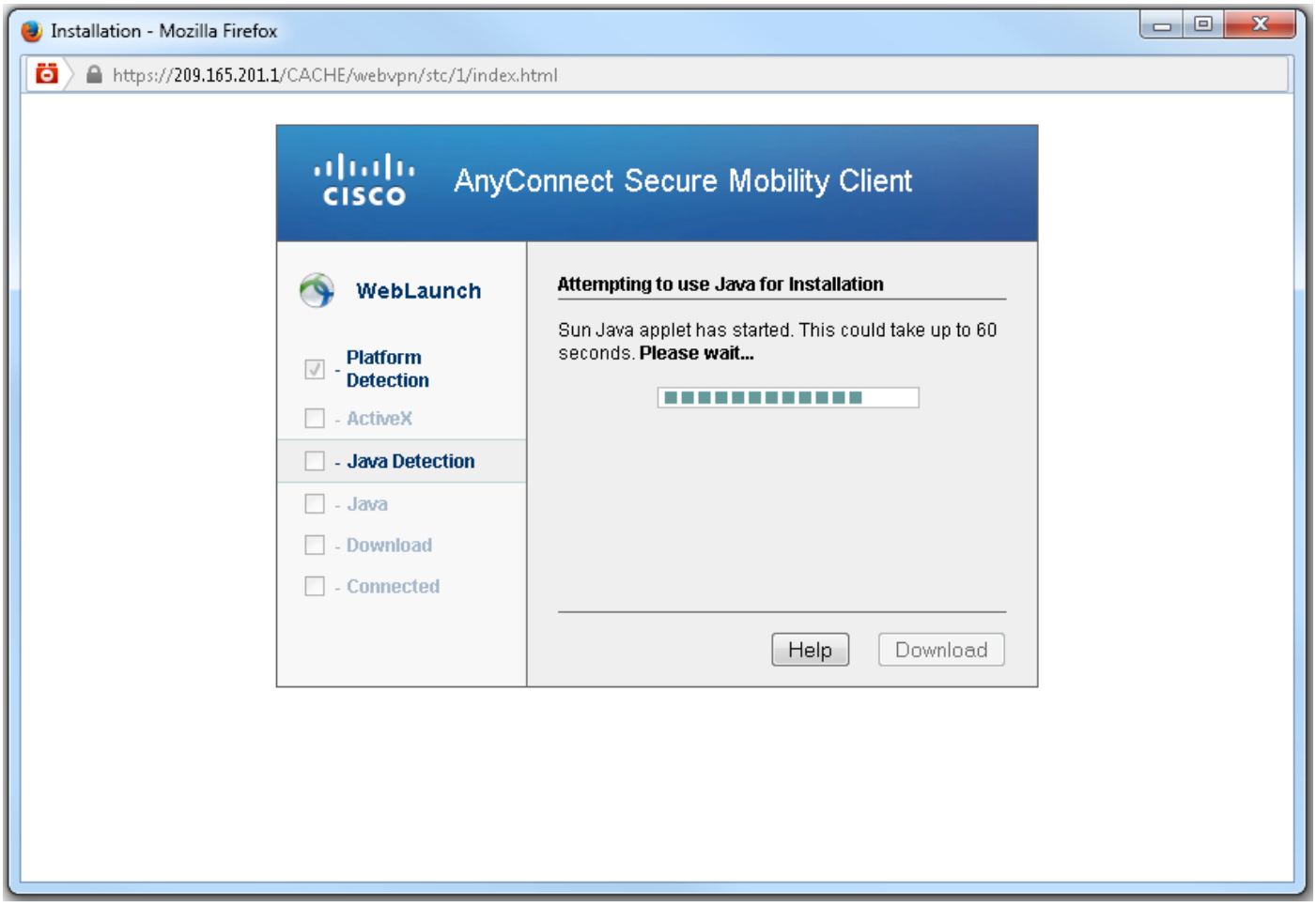
Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando a configuração estiver concluída, quando você acessar o endereço e a porta do Gateway pelo navegador, ela retornará à página inicial da WebVPN.



Após o login, a página inicial do WebVPN é exibida. A partir daqui, clique em **Conexão de túnel (AnyConnect).** Quando o Internet Explorer é usado, o AtiveX é utilizado para descarregar e instalar o cliente AnyConnect. Se não for detectado, o Java será usado. Todos os outros navegadores usam Java imediatamente.

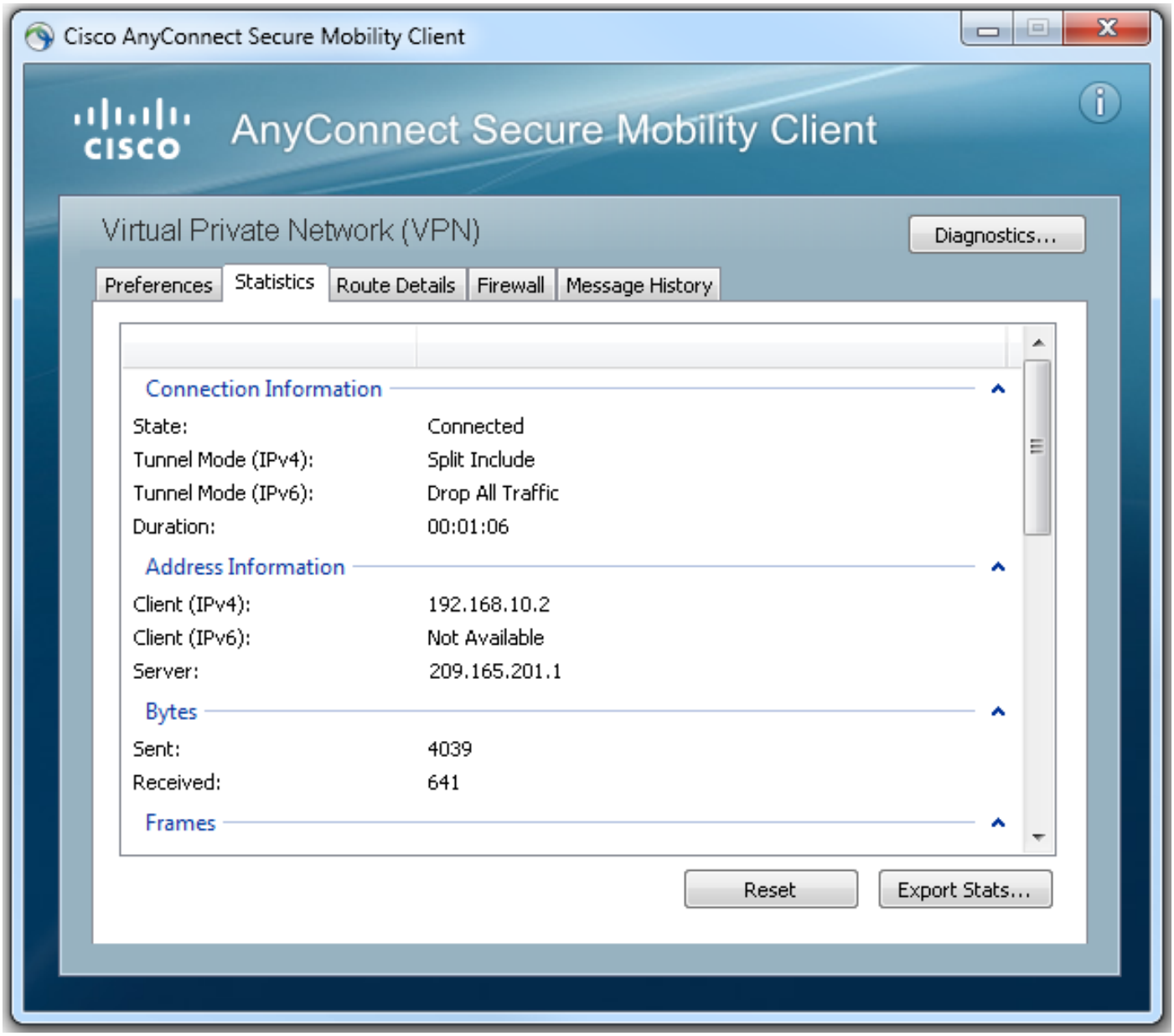


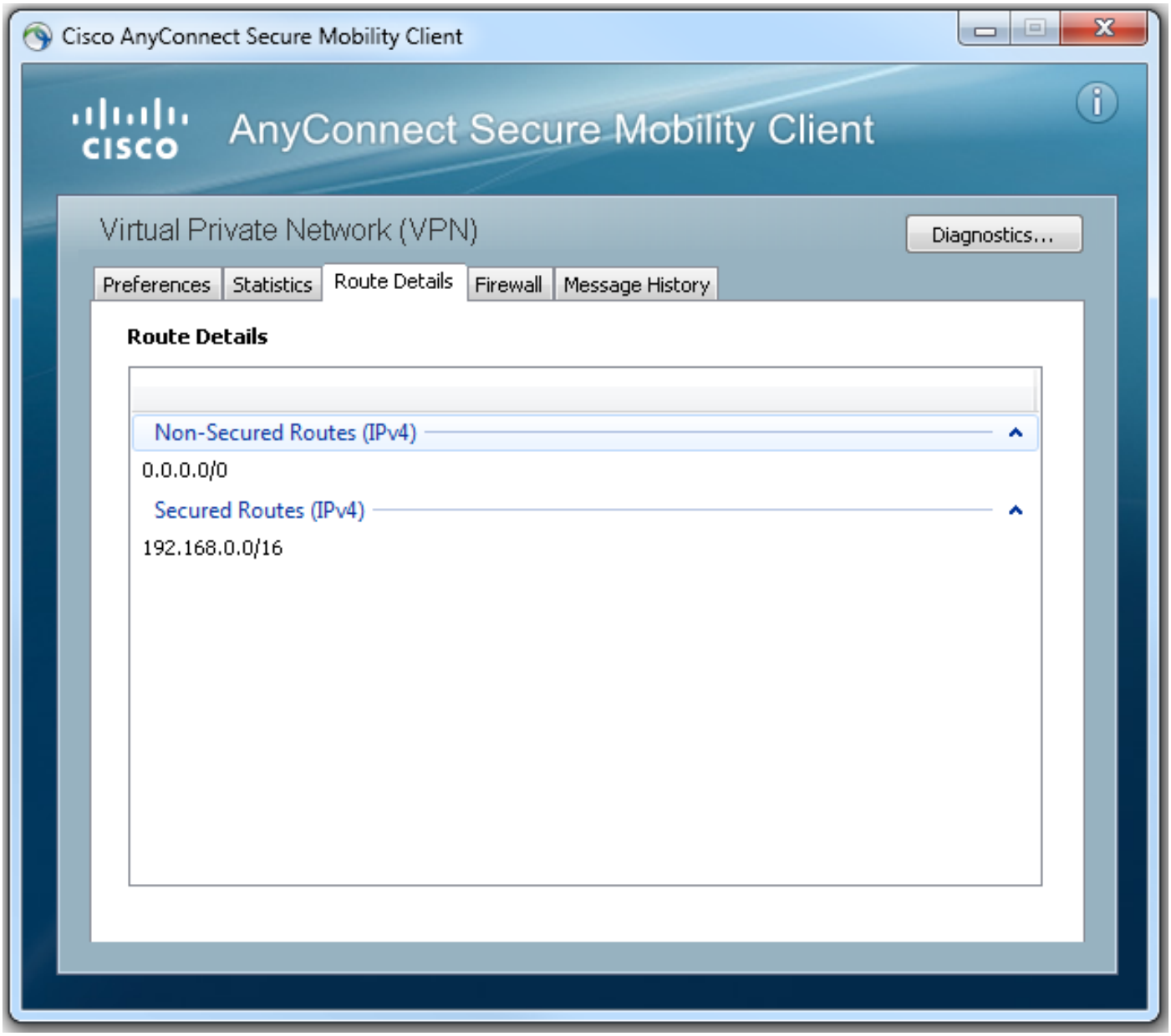


Quando a instalação for concluída, o AnyConnect tentará automaticamente se conectar ao Gateway WebVPN. Como um certificado autoassinado está sendo usado para que o Gateway se

identifique, vários avisos de certificado serão exibidos durante a tentativa de conexão. Eles são esperados e devem ser aceitos para que a conexão continue. Para evitar estes avisos de certificado, o certificado autoassinado que é apresentado tem de ser instalado no arquivo de certificados fidedignos da máquina cliente ou, se estiver a ser utilizado um certificado de terceiros, o certificado de Autoridade de Certificação tem de estar no arquivo de certificados fidedignos.

Quando a conexão concluir a negociação, clique no ícone **da engrenagem** na parte inferior esquerda do AnyConnect, ele exibirá algumas informações avançadas sobre a conexão. Nesta página, é possível visualizar algumas estatísticas de conexão e detalhes de rota obtidos da ACL de túnel dividido na configuração de Política de Grupo.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Include
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:06
Address Information
Client (IPv4): 192.168.10.2
Client (IPv6): Not Available
Server: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



Este é o resultado final da configuração atual das etapas de configuração:

```
crypto pki trustpoint SSLVPN_TP_SELFSIGNED
 enrollment selfsigned
 serial-number
 subject-name cn=892_SELF_SIGNED_CERT
 revocation-check none
 rsakeypair SELF_SIGNED_RSA
!
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
crypto vpn anyconnect profile SSLVPN_PROFILE flash:test-profile.xml ! access-list 1 permit
192.168.0.0 0.0.255.255 ! ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10 ! webvpn gateway
SSLVPN_GATEWAY ip address 209.165.201.1 port 443 ssl trustpoint SSLVPN_TP_SELFSIGNED inservice !
webvpn context SSLVPN_CONTEXT virtual-template 1
aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY
! ssl authenticate verify all inservice ! policy group SSLVPN_POLICY functions svc-enabled svc
address-pool "SSLVPN_POOL" netmask 255.255.255.0 svc split include acl 1 svc dns-server primary
8.8.8.8
svc profile SSLVPN_PROFILE default-group-policy SSLVPN_POLICY
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Há alguns componentes comuns a serem verificados ao solucionar problemas de conexão do AnyConnect:

- Como o cliente deve apresentar um certificado, é necessário que o certificado especificado no Gateway WebVPN seja válido. Para emitir um **certificado show crypto pki** mostrará informações referentes a todos os certificados no roteador.
- Sempre que uma alteração é feita na configuração do WebVPN, é uma prática recomendada emitir um no inservice e inservice no Gateway e no Context. Isso garante que as alterações entrem em vigor corretamente.
- Como mencionado anteriormente, é necessário ter um PKG do AnyConnect para cada sistema operacional cliente que se conectará a este Gateway. Por exemplo, os clientes Windows requerem um PKG Windows, os clientes Linux de 32 bits requerem um PKG Linux de 32 bits e assim por diante.
- Quando você considera o cliente AnyConnect e o WebVPN baseado em navegador para utilizar SSL, para poder acessar a página inicial WebVPN geralmente indica que o AnyConnect será capaz de se conectar (suponha que a configuração pertinente do AnyConnect esteja correta).

O Cisco IOS oferece várias opções de debug webvpn que podem ser usadas para solucionar problemas de conexões com falha. Esta é a saída gerada a partir de debug webvpn aaa, debug wevpn tunnel e show webvpn session em uma tentativa bem-sucedida de conexão:

```
fdenofa-892#show debugging


WebVPN Subsystem:
  WebVPN AAA debugging is on
  WebVPN tunnel debugging is on
  WebVPN Tunnel Events debugging is on
  WebVPN Tunnel Errors debugging is on


*May 26 20:11:06.381: WV-AAA: Nas Port ID set to 64.102.157.2.
*May 26 20:11:06.381: WV-AAA: AAA authentication request sent for user: "VPNUSER"AAA returned
status: 2 for session 37
*May 26 20:11:06.381: WV-AAA: AAA Authentication Passed!
*May 26 20:11:06.381: WV-AAA: User "VPNUSER" has logged in from "64.102.157.2" to gateway
"SSLVPN_GATEWAY"
             context "SSLVPN_CONTEXT"
*May 26 20:11:12.265:
*May 26 20:11:12.265:
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] CSTP Version recd , using 1
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Allocating IP 192.168.10.9 from address-pool
SSLVPN_POOL
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Using new allocated IP 192.168.10.9 255.255.255.0
*May 26 20:11:12.265:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:12.265: HTTP/1.1 200 OK
*May 26 20:11:12.265: Server: Cisco IOS SSLVPN
```

```
*May 26 20:11:12.265: X-CSTP-Version: 1
*May 26 20:11:12.265: X-CSTP-Address: 192.168.10.9
*May 26 20:11:12.269: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:12.269: X-CSTP-Keep: false
*May 26 20:11:12.269: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:12.269: X-CSTP-Lease-Duration: 43200
*May 26 20:11:12.269: X-CSTP-MTU: 1280
*May 26 20:11:12.269: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:12.269: X-CSTP-DPD: 300
*May 26 20:11:12.269: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Session-Timeout: 0
*May 26 20:11:12.269: X-CSTP-Keepalive: 30
*May 26 20:11:12.269: X-DTLS-Session-ID:
85939A3FE33ABAE5F02F8594D56DEDE389F6FB3C9EEC4D211EB71C0820DF8DC8
*May 26 20:11:12.269: X-DTLS-Port: 443
*May 26 20:11:12.269: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:12.269: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:12.269: X-DTLS-DPD: 300
*May 26 20:11:12.269: X-DTLS-KeepAlive: 30
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269: [WV-TUNL-EVT]:[8A3AE410] For User VPNUSER, DPD timer started for 300
seconds
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd a Req Cntl Frame (User
VPNUSER, IP 192.168.10.9)
Severity ERROR, Type CLOSE_ERROR
Text: reinitiate tunnel to negotiate a different MTU
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd Close Error Frame
*May 26 20:11:14.105:
*May 26 20:11:14.105:
*May 26 20:11:14.105: [WV-TUNL-EVT]:[8A3AE690] CSTP Version recd , using 1
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Tunnel Client reconnecting removing existing tunl
ctx
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE410] Closing Tunnel Context 0x8A3AE410 for Session
0x8A3C2EF8 and User VPNUSER
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Reusing IP 192.168.10.9 255.255.255.0
*May 26 20:11:14.109:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:14.109: HTTP/1.1 200 OK
*May 26 20:11:14.109: Server: Cisco IOS SSLVPN
*May 26 20:11:14.109: X-CSTP-Version: 1
*May 26 20:11:14.109: X-CSTP-Address: 192.168.10.9
*May 26 20:11:14.109: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:14.109: X-CSTP-Keep: false
*May 26 20:11:14.109: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:14.113: X-CSTP-Lease-Duration: 43200
*May 26 20:11:14.113: X-CSTP-MTU: 1199
*May 26 20:11:14.113: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:14.113: X-CSTP-DPD: 300
*May 26 20:11:14.113: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Session-Timeout: 0
*May 26 20:11:14.113: X-CSTP-Keepalive: 30
*May 26 20:11:14.113: X-DTLS-Session-ID:
22E54D9F1F6344BCB5BB30BC8BB3737907795E6F3C3665CDD294CBBA1DA4D0CF
*May 26 20:11:14.113: X-DTLS-Port: 443
*May 26 20:11:14.113: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:14.113: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:14.113: X-DTLS-DPD: 300
*May 26 20:11:14.113: X-DTLS-KeepAlive: 30
```

```
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113: [WV-TUNL-EVT]:[8A3AE690] For User VPNUSER, DPD timer started for 300
seconds
```

```
fdenofa-892#show webvpn session user VPNUSER context SSLVPN_CONTEXT

Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.08009

Username          : VPNUSER              Num Connection : 5
Public IP         : 64.102.157.2         VRF Name       : None
Context           : SSLVPN_CONTEXT       Policy Group   : SSLVPN_POLICY
Last-Used         : 00:00:00             Created        : *16:11:06.381 EDT Tue May 26 2015
Session Timeout   : Disabled             Idle Timeout   : 2100
DNS primary serve : 8.8.8.8
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSLVPN_POOL          MTU Size       : 1199
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.10.9         Netmask        : 255.255.255.0
Rx IP Packets     : 0                    Tx IP Packets  : 42
CSTP Started      : 00:00:13             Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                    Virtual Access : 2
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : ACL 1
Client Ports      : 17462 17463 17464 17465 17471
```

Informações Relacionadas

- Guia de configuração de VPN SSL, Cisco IOS versão 15M&T
- Exemplo de configuração do AnyConnect VPN (SSL) Client no IOS Router com CCP
- Suporte Técnico e Documentação - Cisco Systems