AnyConnect: Configurar SSLVPN básico para o final do cabeçalho do IOS Router com o uso do CLI

Índice

Introdução

Este documento descreve a configuração básica de um roteador do Cisco IOS como um final do cabeçalho de AnyConnect SSLVPN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Sistema operacional inter-redes Cisco (IO)
- Cliente seguro da mobilidade de AnyConnect

- Operação geral do secure sockets layer (SSL)

Componentes Utilizados

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

- Cisco 892W Router que executa 15.3(3)M5
- Cliente seguro 3.1.08009 da mobilidade de AnyConnect

Informação licenciando para Versões do IOS diferentes

- O conjunto de recursos securityk9 é exigido para usar as características SSLVPN, apesar de que a Versão do IOS é usada.
- IO 12.x - a característica SSLVPN é integrada em todas as imagens 12.x que começam com 12.4(6)T que têm pelo menos uma licença da Segurança (IE. advsecurityk9, adventerprisek9, e assim por diante).
- IO 15.0 - as versões anterior exigem um arquivo LIC ser instaladas no roteador que permitirá o 10, 25, ou 100 conexões do usuário. Direito às licenças de Use* foram executados em 15.0(1)M4
- IO 15.1 - as versões anterior exigem um arquivo LIC ser instaladas no roteador que permitirá o 10, 25, ou 100 conexões do usuário. Direito às licenças de Use* foram executados em 15.1(1)T2, em 15.1(2)T2, em 15.1(3)T, e em 15.1(4)M1
- IO 15.2 - todas as 15.2 versões oferecem certo às licenças de Use* para SSLVPN
- IO 15.3 e além - as versões anterior oferecem certo às licenças de Use*. Começando em 15.3(3)M, a característica SSLVPN está disponível depois que você carreg em um tecnologia-pacote securityk9

Para RTU que licencia, uma licença de avaliação será permitida quando a primeira característica do webvpn é configurada (isto é, gateway GATEWAY1 do webvpn) e o contrato de licença do utilizador final (EULA) foi aceitado. Após 60 dias, esta licença de avaliação transforma-se uma licença permanente. Estas licenças são honra baseada e exigem uma licença de papel ser comprado a fim usar a característica. Adicionalmente, um pouco do que sendo limitado a um determinado número de usos, os RTU permitem o número máximo de conexões simultâneas que a plataforma de roteador pode apoiar simultaneamente.

Melhoras de software significativas

Estes erros ID conduziram às características ou aos reparos significativos para AnyConnect:

- CSCti89976: Apoio adicionado para AnyConnect 3.x aos IO
- CSCtx38806: Reparo para a vulnerabilidade do ANIMAL, Microsoft KB2585542

Configurar

Etapa 1. Confirme a licença é permitido

A primeira etapa quando AnyConnect é configurado em um final do cabeçalho do IOS Router é confirmar que a licença corretamente esteve instalada (se aplicável) e permitida. Refira a informação licenciando na seção anterior para os específicos licenciar em versões diferentes.

Depende da versão de código e da plataforma se a licença da mostra alista uma licença SSL_VPN ou securityk9. Apesar da versão e da licença, o EULA deverá ser aceitado e a licença mostrará como o Active.

Etapa 2. Transfira arquivos pela rede e instale o pacote seguro do cliente da mobilidade de AnyConnect no roteador

Para transferir arquivos pela rede uma imagem de AnyConnect aos saques do fim de cabeçalho de VPN duas finalidades. Em primeiro lugar, somente os sistemas operacionais que têm as imagens de AnyConnect atuais no final do cabeçalho de AnyConnect serão permitidos para conectar. Por exemplo, os clientes do Windows exigem um pacote de Windows ser instalados no final do cabeçalho, Linux que os clientes 64-bit exigem um pacote 64-bit de Linux, e assim por diante. Em segundo lugar, a imagem de AnyConnect instalada no final do cabeçalho será abaixada automaticamente para a máquina cliente em cima da conexão. Os usuários que conectam pela primeira vez poderão transferir o cliente do portal da web e os usuários que o retorno poderá promover, desde que o pacote de AnyConnect no final do cabeçalho é mais novo do que o que está instalado em sua máquina cliente.

Os pacotes de AnyConnect podem ser obtidos através da seção segura do cliente da mobilidade de AnyConnect do Web site das transferências de software Cisco. Quando houver muitas opções disponíveis, os pacotes que devem ser instalada no final do cabeçalho estarão etiquetados com o sistema operacional e o desenvolvimento da extremidade principal (PKG). Os pacotes de AnyConnect estão atualmente disponíveis para estas plataformas de sistema operacional: Windows, Mac OS X, Linux (de 32 bits), e Linux 64-bit. Note que para Linux, há ambos os 32 e pacotes 64-bit. Cada sistema operacional exige o pacote apropriado ser instalado no final do cabeçalho para que as conexões sejam permitidas.

Uma vez que o pacote de AnyConnect foi transferido, pode ser transferido arquivos pela rede ao flash do roteador com o **comando copy** através do TFTP, do FTP, do SCP, ou das 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 que você copia a imagem de AnyConnect ao flash do roteador, deve ser instalado através da linha de comando. Os pacotes múltiplos de AnyConnect podem ser instalados quando você especifica um número de sequência no fim do comando da instalação; isto permitirá o roteador atuar como o final do cabeçalho para sistemas operacionais do cliente múltiplo. Quando você instala o pacote de AnyConnect, igualmente movê-lo-á para o **flash: diretório /webvpn/** se não foi 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 de código que foram liberadas antes de 15.2(1)T, o comando instalar o PKG é levemente diferente.

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

Etapa 3. Permita o server HTTP no roteador

```
ip http server
ip http secure-server
```

Etapa 4. Gerencia o par de chave RSA e o certificado auto-assinado

Quando você configura o SSL ou a toda a característica que executar o Public Key Infrastructure (PKI) e os Certificados digitais, um keypair de Rivest-Shamir-Adleman (RSA) é exigido para a assinatura do certificado. O comando do seguimento gerará um par de chave RSA que seja usado então quando o certificado auto-assinado PKI é gerado. Quando você utiliza um módulo de 2048 bit, não é uma exigência, recomenda-se usar o módulo o maior disponível para a segurança avançada e a compatibilidade com as máquinas cliente de AnyConnect. Para usar uma etiqueta descritiva é recomendada igualmente porque permitirá a facilidade do gerenciamento chave. A geração chave pode ser confirmada com o **comando show crypto key mypubkey rsa**.

> Nota: Porque há muitos riscos de segurança associados com a fatura do RSA fecha exportable, a prática recomendada está se assegurar de que as chaves estejam configuradas para ser não exportable que é o padrão. Os riscos que são involvidos quando você faz o RSA fecham exportable são discutidos neste documento: Chaves de distribuição RSA dentro de 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 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 exportable.
Key Data&colon;
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
```

Uma vez que o par de chave RSA foi gerado com sucesso, um ponto confiável PKI deve ser configurado com informação e par de chave RSA do nosso roteador. O Common Name (CN) no Assunto-nome deve ser configurado com o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome de domínio qualificado completo (FQDN) que os usuários se usam para conectar ao gateway de AnyConnect; neste exemplo, os clientes usam o FQDN de fdenofa-SSLVPN.cisco.com quando tentam conectar. Quando não for imperativo, quando você entra corretamente no CN, ajuda a reduzir o número de erros do certificado que são alertados no início de uma sessão.

> Nota: Um pouco do que usando um certificado auto-assinado gerado pelo roteador, é possível usar um certificado emitido por CA da terceira. Isto pode ser feito através de alguns métodos diferentes como discutido neste documento: Configurando o certificado de registro para um PKI.

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

Depois que o ponto confiável foi definido corretamente, o roteador deve gerar o certificado usando o **pki cripto registra o** comando. Com este processo, é possível especificar alguns outros parâmetros tais como o número de série e o endereço IP de Um ou Mais Servidores Cisco ICM NT. Contudo, isto não é exigido. A geração do certificado pode ser confirmada com o comando **cripto dos Certificados do pki da mostra**.

```
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 5. Configurar contas de usuário locais VPN

Quando for possível usar uma autenticação externa, server da autorização, e da contabilidade (AAA), porque esta autenticação local do exemplo está usado. Estes comandos criarão um nome de usuário VPNUSER e igualmente criarão uma lista da autenticação de AAA nomeada SSLVPN_AAA.

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

Etapa 6. Defina a lista de acessos do conjunto de endereços e do túnel em divisão a ser usada por clientes

Um pool do endereço IP local deve ser criado para que os adaptadores cliente de AnyConnect obtenham um endereço IP de Um ou Mais Servidores Cisco ICM NT. Assegure-se de que você configure um grande bastante pool para apoiar o número máximo de conexões de cliente simultâneas de AnyConnect.

À revelia, AnyConnect operar-se-á no modo de túnel completo que significa que todo o tráfego gerado pela máquina cliente estará enviado através do túnel. Porque isto não é tipicamente desejável, é possível configurar um Access Control List (ACL) que define então o tráfego que deve ou não deve ser enviado através do túnel. Como com outras aplicações ACL, o implícitos negam na extremidade eliminam a necessidade para um explícito negam; consequentemente, é somente necessário configurar indicações da licença para o tráfego que deve ser escavado um túnel.

```
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 7. Configurar a interface de molde virtual (VTI)

VTIs dinâmico forneça uma interface de acesso virtual separada por encomenda para cada sessão de VPN que permite altamente seguro e a conectividade escalável para acessos remoto VPN. A tecnologia DVTI substitui os mapas cripto dinâmico e o método dinâmico do Hub-and-Spoke que as ajudas estabelecem túneis. Porque função de DVTIs como alguma outra interface real que permitirem um desenvolvimento remoto mais complexo de Accesss porque apoiam QoS, Firewall, por usuário attribtues e outros Serviços de segurança assim que o túnel for ativo.

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

Etapa 8. Configurar o gateway WebVPN

O gateway WebVPN é o que define o endereço IP de Um ou Mais Servidores Cisco ICM NT e as portas que serão usados pelo final do cabeçalho de AnyConnect, assim como o algoritmo de criptografia SSL e o certificado PKI que será apresentado aos clientes. À revelia, o gateway apoiará todos os algoritmos de criptografia possíveis, que variam segundo a Versão do IOS no roteador.

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

Etapa 9. Configurar o contexto WebVPN e a política do grupo

A política do contexto e do grupo WebVPN define alguns parâmetros adicionais que serão usados para a conexão de cliente de AnyConnect. Para uma configuração básica de AnyConnect, o contexto serve simplesmente como um mecanismo usado para chamar a política do grupo padrão que será usada para AnyConnect. Contudo, o contexto pode ser usado para personalizar mais a página do respingo WebVPN e a operação WebVPN. No grupo de política definida, a lista SSLVPN_AAA é configurada como a lista da autenticação de AAA de que os usuários são um membro. O comando SVC-**permitido funções** é a parte de configuração que permite que os usuários conectem com o **cliente VPN de** AnyConnect **SSL** um pouco do que apenas o WebVPN através de um navegador. Ultimamente, os comandos svc adicionais definem os parâmetros que são relevantes somente às conexões SVC: **o pool de endereços svc** diz o gateway aos endereços do comunicado no ACPool aos clientes, a **separação svc inclui** define a política do túnel em divisão por ACL 1 definida acima, e o dns-**server svc** define o servidor DNS qual será usado para a definição do Domain Name. Com esta configuração, todas as perguntas DNS serão enviadas ao servidor DNS especificado. O endereço que é recebido na resposta da pergunta ditará mesmo se o tráfego está enviado através do túnel.

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Etapa 10 (opcional). Configurar um perfil do cliente

Ao contrário nos ASA, o Cisco IOS não tem uma interface GUI incorporado que possa ajudar a admins em criar o perfil do cliente. O perfil do cliente de AnyConnect precisa de ser criado separadamente/editado com o editor autônomo do perfil.

> Dica: Procure anyconnect-profileeditor-win-3.1.03103-k9.exe

Siga estas etapas para mandar o roteador distribuir o perfil:

1. Transfira-o arquivos pela rede ao ftp de utilização instantâneo IO/tftp
2. Use este comando identificar o perfil que foi transferido arquivos pela rede apenas:

1.
```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```
Dica: Nas Versões do IOS mais velhas do que 15.2(1)T, este comando precisa de ser usado:

flash do <profile_name> do perfil svc da importação do webvpn: <profile.xml>

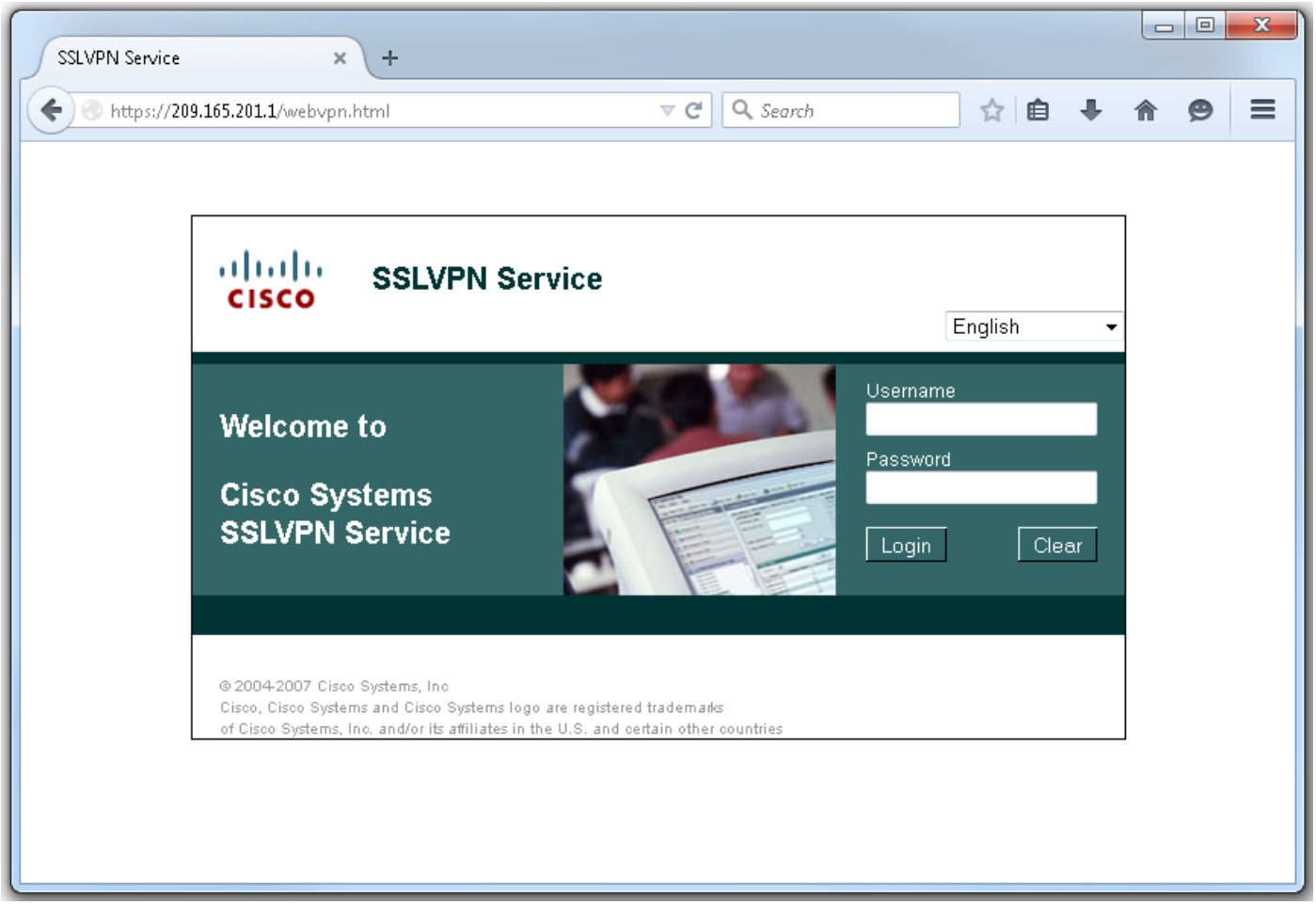
3. Sob o contexto, use este comando ligar o perfil a esse contexto:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

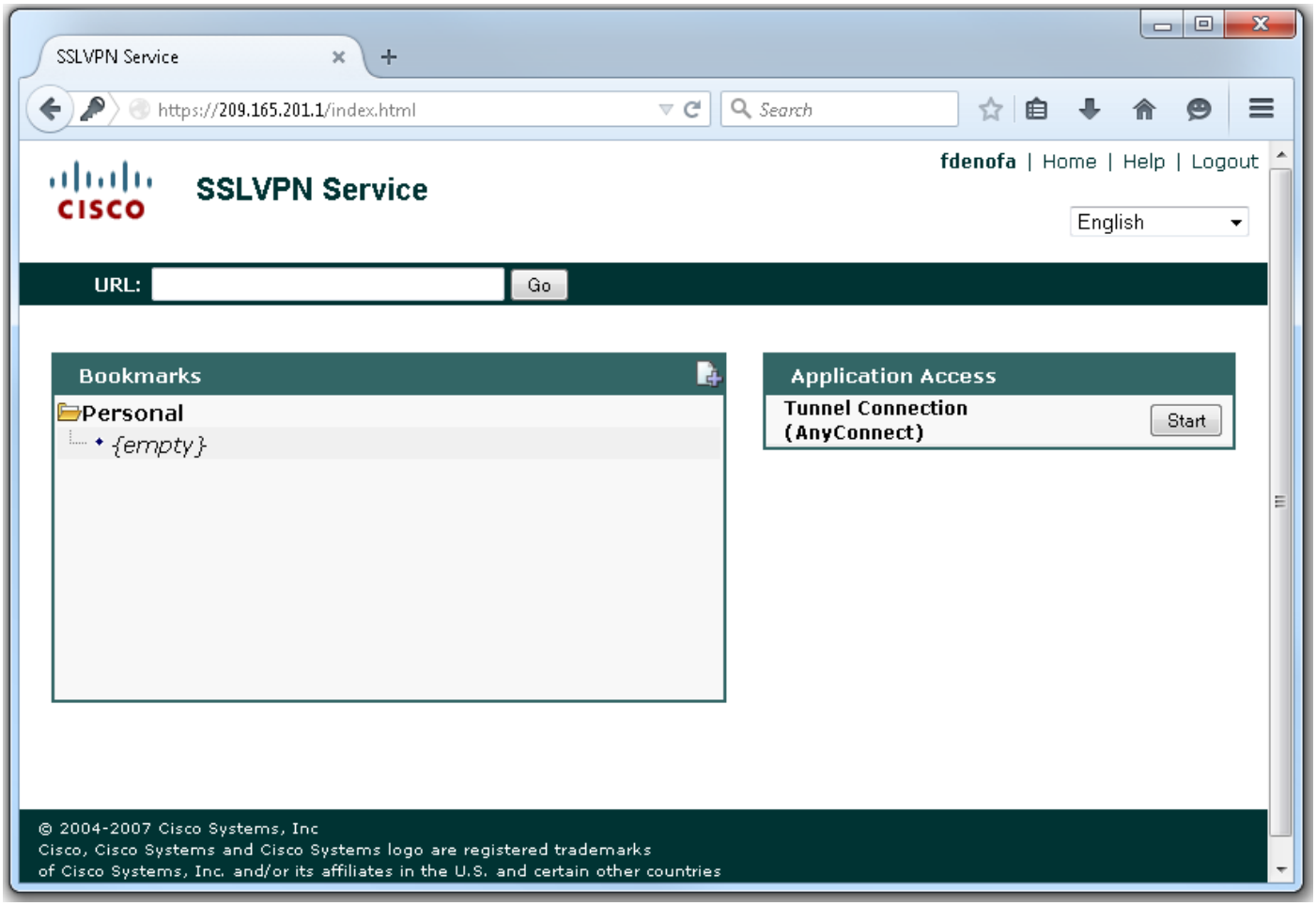
Verificar

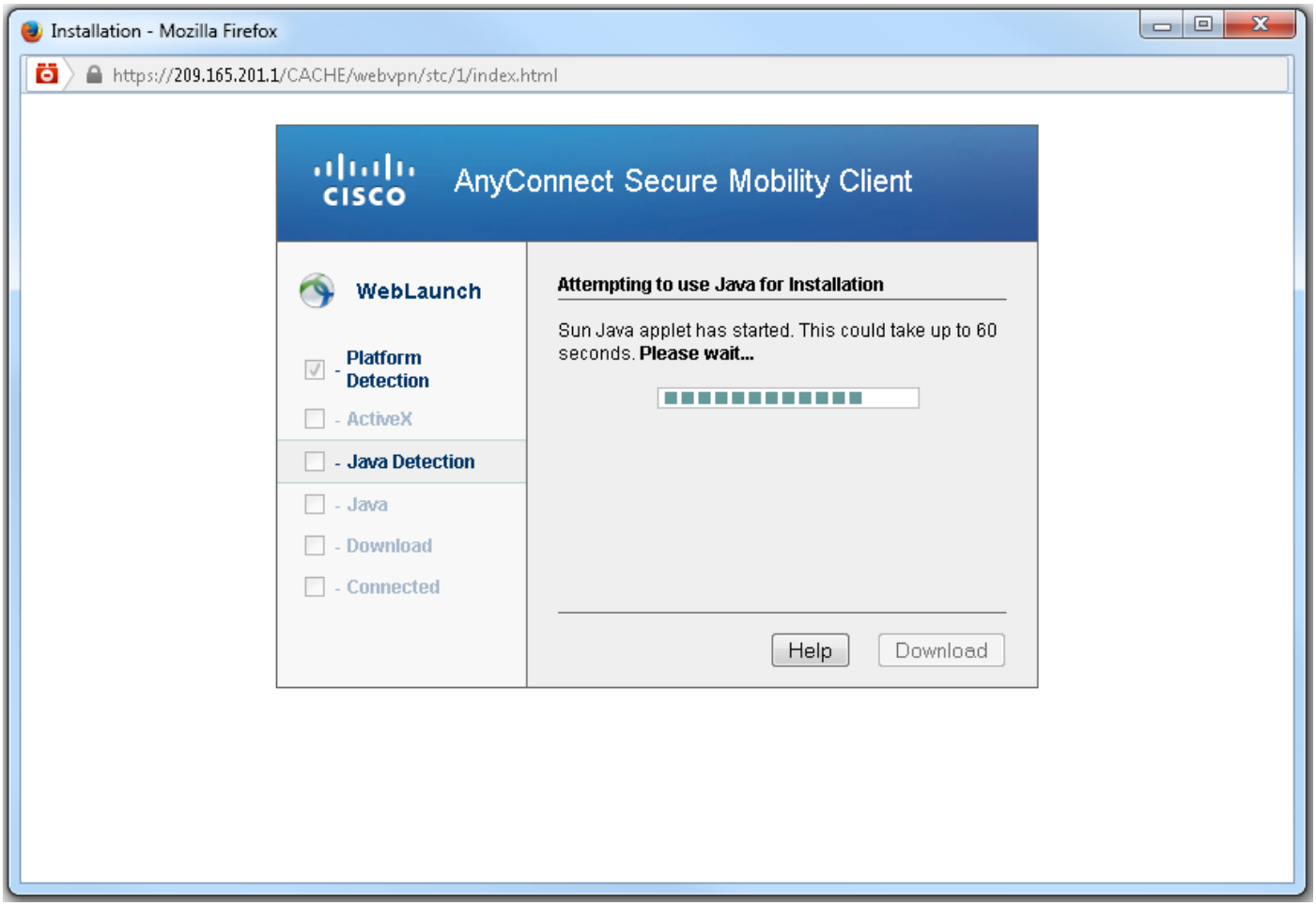
Uma vez que a configuração está completa, quando você alcança o endereço de gateway e o move através do navegador, retornará à página do respingo WebVPN.



Depois que você entra, o Home Page WebVPN está indicado. De aqui, **conexão de túnel do** clique **(AnyConnect).** Quando o internet explorer é usado, ActiveX está utilizado para abaixar e instalar o cliente de AnyConnect. Se não é detectado, as Javas estarão usadas pelo contrário.

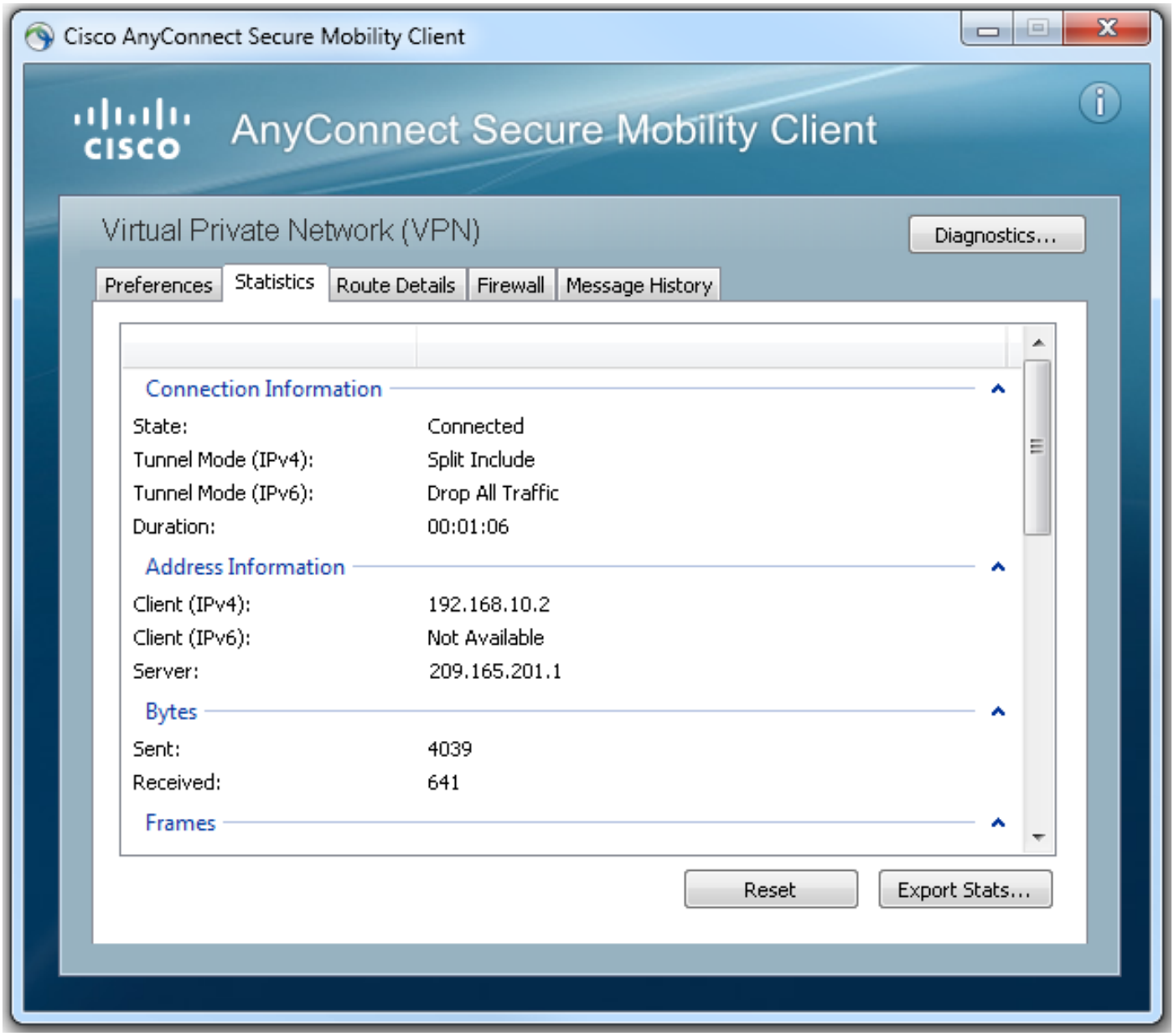
Todos navegadores restantes usam Javas imediatamente.

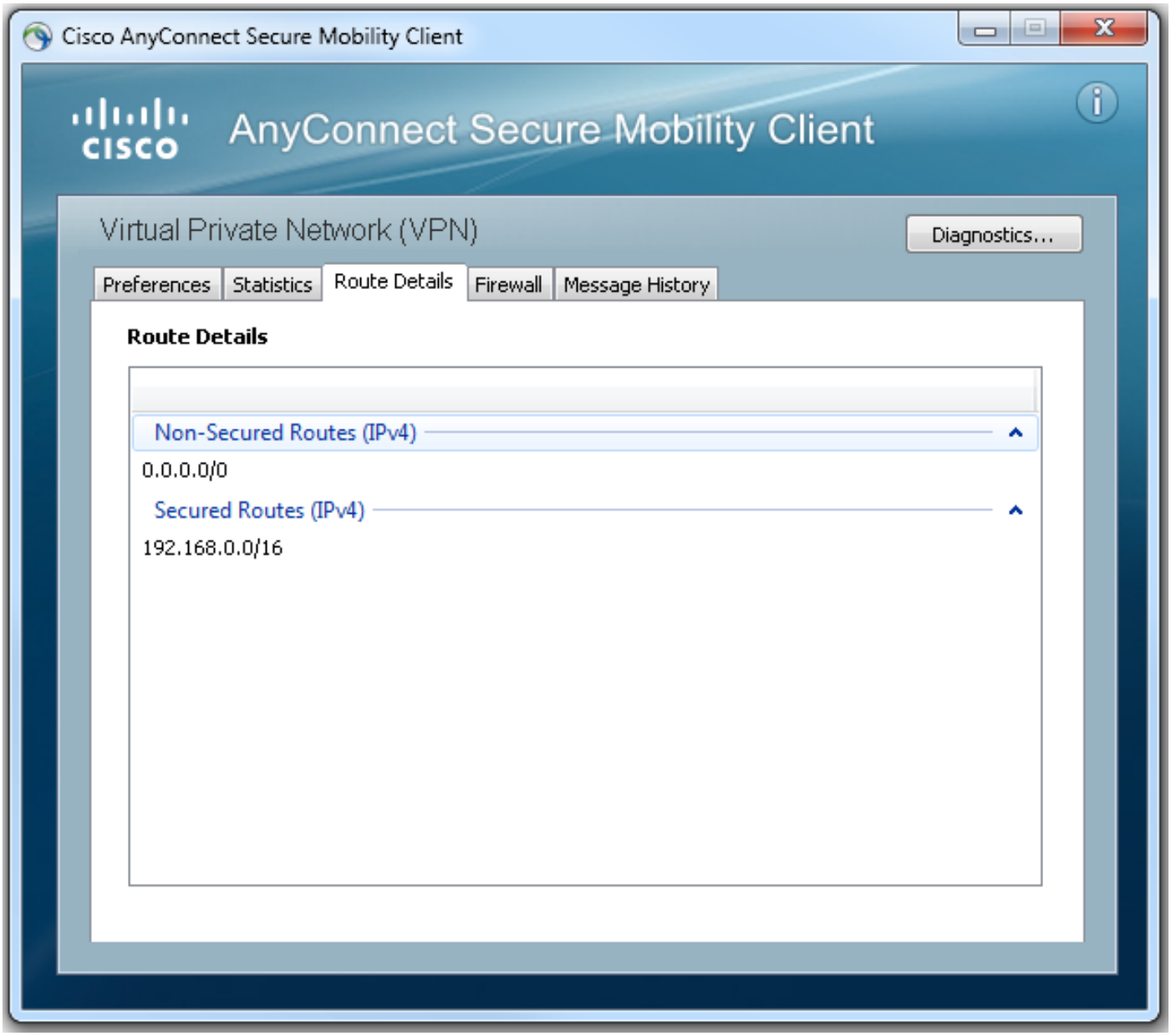




Uma vez que a instalação é terminada, AnyConnect tentará automaticamente conectar ao gateway WebVPN. Porque um certificado auto-assinado está sendo usado para que o gateway se identifique, os avisos dos certificados múltiplos aparecerão durante a tentativa de conexão. Estes são esperados e devem ser aceitados para que a conexão continue. Para evitar estes avisos do certificado, o certificado auto-assinado que está sendo apresentado deve ser instalado na loja do certificado confiável da máquina cliente, ou se um certificado da terceira está sendo usado então o certificado do Certificate Authority deve estar na loja do certificado confiável.

Quando a conexão termina a negociação, clique sobre o ícone da **engrenagem na** esquerda mais baixa de AnyConnect indicará alguma informação avançada sobre a conexão. Nesta página é possível ver alguma estatística de conexão e distribuir os detalhes alcançados do túnel em divisão ACL na configuração das normas do 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...



Está aqui o resultado final da executar-configuração das etapas de configuração:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Troubleshooting

Há alguns componentes comuns a verificar quando você pesquisa defeitos questões de conexão de AnyConnect:

- Como o cliente deve apresentar um certificado, é uma exigência que o certificado especifique no gateway WebVPN seja válido. Para emitir um **certificado cripto do pki da mostra** mostrará

a informação que se refere todos os Certificados no roteador.

- Sempre que uma mudança é feita à configuração WebVPN, é um melhor prática emitir um não em serviço e em serviço no gateway e no contexto. Isto assegurar-se-á de que as mudanças tomem o efeito corretamente.
- Como mencionado mais cedo, é uma exigência ter um AnyConnect PKG para cada sistema operacional do cliente que conectará a este gateway. Por exemplo, os clientes do Windows exigem Windows PKG, Linux que os clientes de 32 bits exigem Linux PKG de 32 bits, e assim por diante.
- Quando você considera o cliente de AnyConnect e o WebVPN com base em navegador utiliza o SSL, poder alcançar a página do respingo WebVPN indica geralmente que AnyConnect poderá conectar (supõe que a configuração pertinente de AnyConnect está correta).

O Cisco IOS oferece algum vário debuga as opções do webvpn que podem ser usadas para pesquisar defeitos conexões de falha. Esta é a saída gerada de debuga o webvpn aaa, debuga o túnel do wevpn, e mostra a sessão do webvpn em cima de uma tentativa da conexão bem sucedida:

```
webvpn context SSL_Context
 gateway SSLVPN_Gateway
 inservice
 policy group SSL_Policy
  aaa authentication list SSLVPN_AAA
  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
virtual-template 1
default-group-policy SSL_Policy
```

Informações Relacionadas

- Guia de configuração de VPN SSL, Cisco IOS Release 15M&T
- Cliente de AnyConnect VPN (SSL) no IOS Router com exemplo de configuração CCP