Configurar o encapsulamento de divisão dinâmica ASA/AnyConnect

Contents

Introdução

Este documento descreve como configurar o AnyConnect Secure Mobility Client para Dynamic Split Exclude Tunneling via ASDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do ASA.
- Conhecimento básico do Cisco Anyconnect Security Mobility Client.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

As informações 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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer

comando.

Informações de Apoio

O tunelamento dividido do Anyconnect permite que o Cisco AnyConnect Secure Mobility Client tenha acesso seguro aos recursos corporativos via IKEV2 ou Secure Sockets Layer (SSL).

Antes do AnyConnect versão 4.5, com base na política configurada no Adaptive Security Appliance (ASA), o comportamento do túnel dividido poderia ser Tunnel Specified, Tunnel All ou Exclude Specified.

Com o advento dos recursos de computador hospedados na nuvem, os serviços às vezes resolvem para um endereço IP diferente com base na localização do usuário ou na carga dos recursos hospedados na nuvem.

Como o Anyconnect Secure Mobility Client fornece separação de túneis para intervalo de sub-rede estática, host ou pool de IPV4 ou IPV6, torna-se difícil para os administradores de rede excluir domínios/FQDNs enquanto configuram o AnyConnect.

Por exemplo, um administrador de rede deseja excluir o domínio Cisco.com da configuração de túnel dividido, mas o mapeamento DNS para Cisco.com é alterado, já que ele é hospedado na nuvem.

Usando o encapsulamento Dynamic Split Exclude, o Anyconnect resolve dinamicamente o endereço IPv4/IPv6 do aplicativo hospedado e faz as alterações necessárias na tabela de roteamento e nos filtros para permitir que a conexão seja feita fora do túnel.

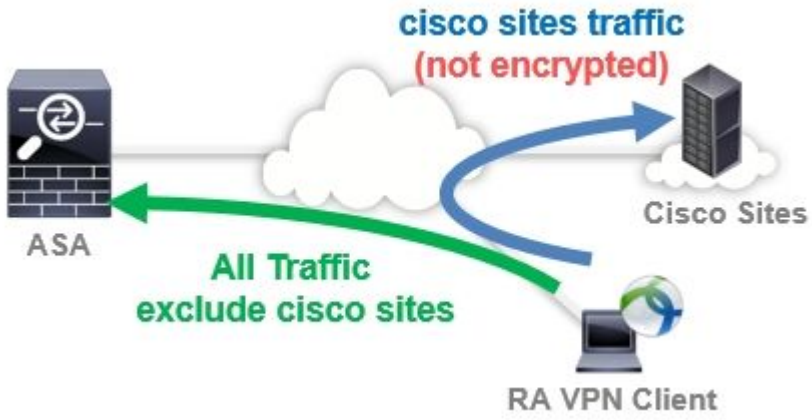
A partir do AnyConnect 4.5, o Dynamic Spit Tunneling pode ser usado onde o Anyconnect resolve dinamicamente o endereço IPv4/IPv6 do aplicativo hospedado e faz as alterações necessárias na tabela de roteamento e nos filtros para permitir que a conexão seja feita fora do túnel

Configuração

Esta seção descreve como configurar o Cisco AnyConnect Secure Mobility Client no ASA.

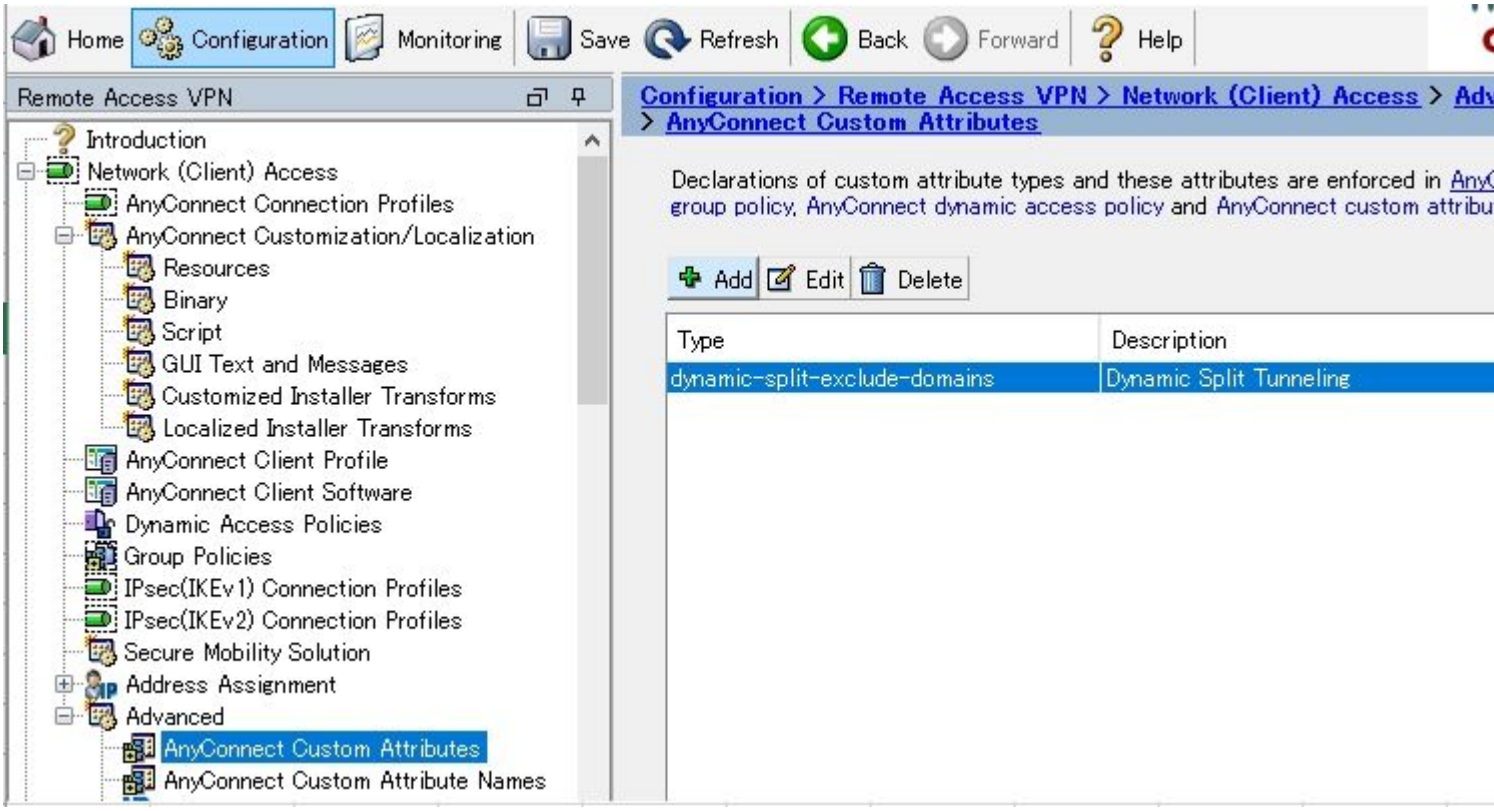
Diagrama de Rede

Esta imagem mostra a topologia usada para os exemplos deste documento.



Etapa 1. Crie atributos personalizados do AnyConnect.

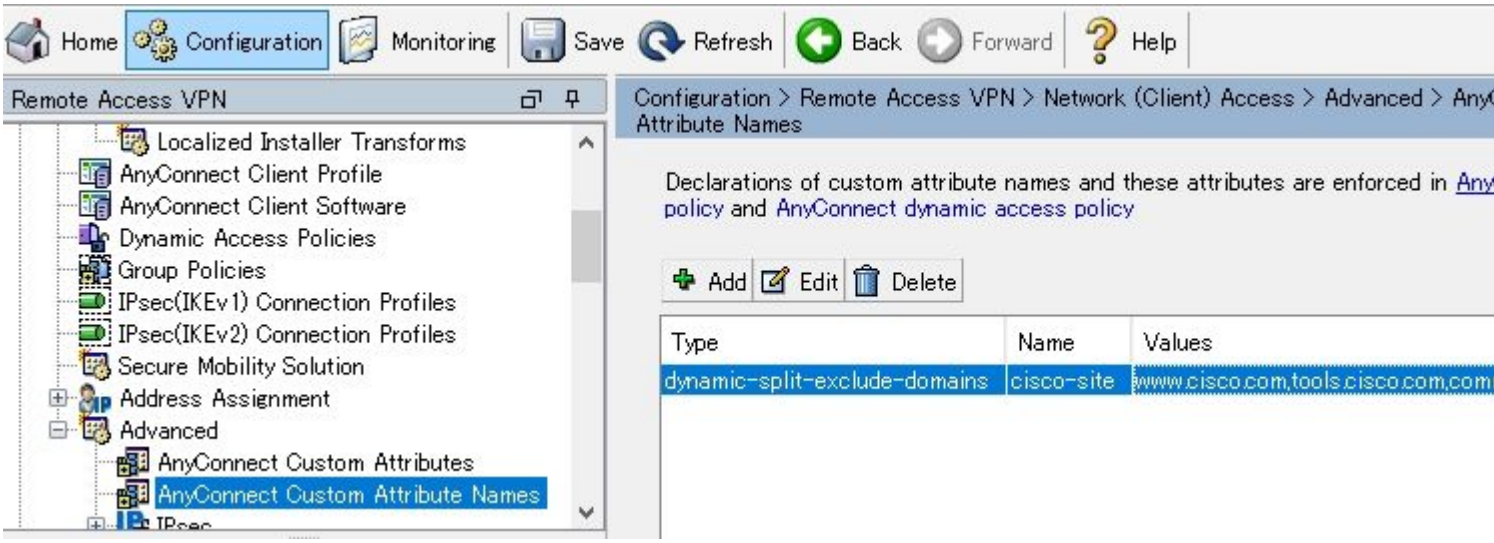
Navegue até **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.** clique em **Add** e definir **dynamic-split-exclude-domains** atributo e descrição opcional, como mostrado na imagem:



Etapa 2. Criar nome personalizado do AnyConnect e configurar valores.

Navegue até **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** clique em **Add** e defina a **dynamic-split-exclude-domains** atributo criado anteriormente a partir de Tipo, um nome arbitrário e Valores, como mostrado na imagem:

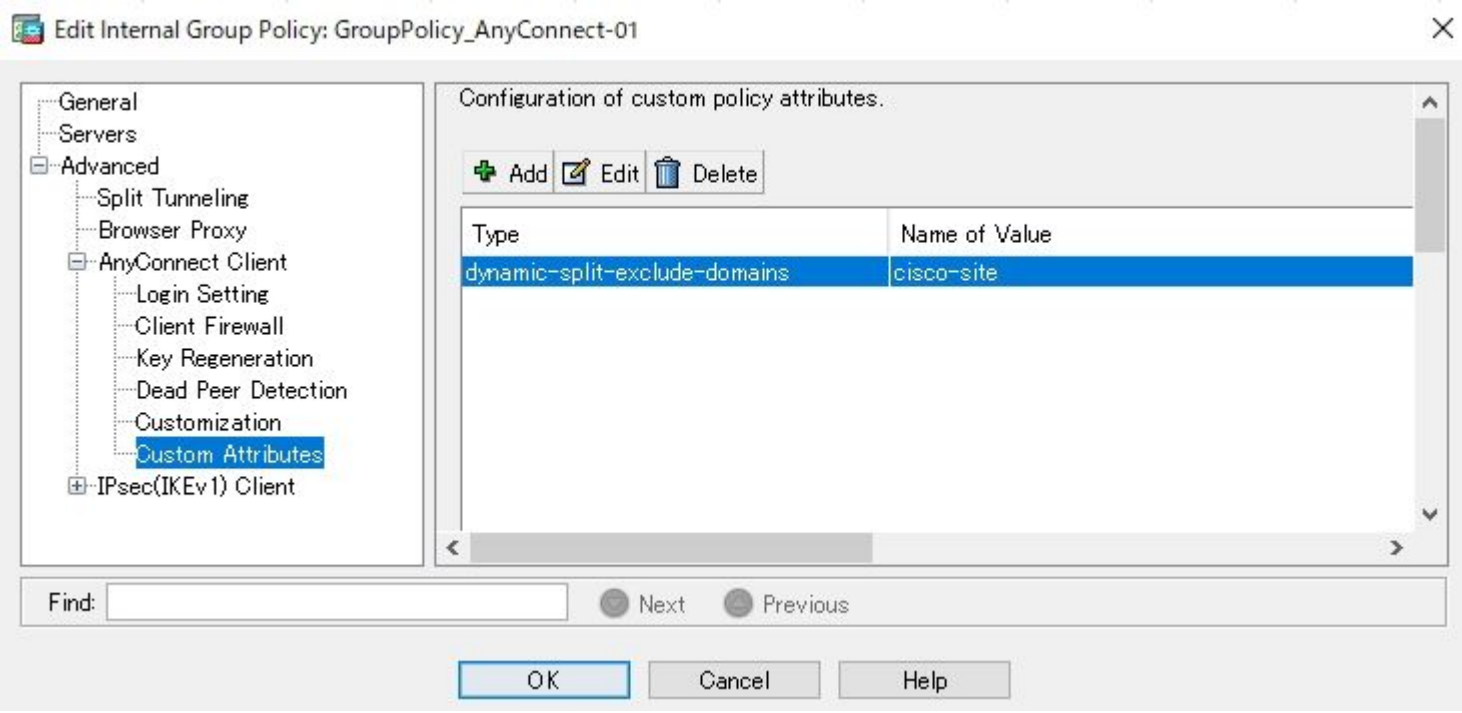
Tome cuidado para não inserir um espaço em Nome. (Exemplo: Possível "cisco-site" Impossível "cisco site") Quando vários domínios ou FQDNs em Valores são registrados, separe-os com uma vírgula (,).



Etapa 3. Adicione o Tipo e o Nome à Política de Grupo.

Navegue até **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** e selecione uma diretiva de

grupo. Em seguida, navegue até **Advanced> AnyConnect Client> Custom Attributes** e adicionar o **Type** e **Name,**conforme mostrado na imagem:



Exemplo de configuração de CLI

Esta seção fornece a configuração CLI do Dynamic Split Tunneling para fins de referência.

<#root>

```
ASAv10# show run
  --- snip ---
```

webvpn

```
 enable outside
```

anyconnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling

```
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.7.04056-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
```

anyconnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.

```
group-policy GroupPolicy_AnyConnect-01 internal
```

group-policy GroupPolicy_AnyConnect-01 attributes

```
wins-server none
dns-server value 10.0.0.0
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
split-tunnel-network-list value SplitACL
default-domain value cisco.com
```

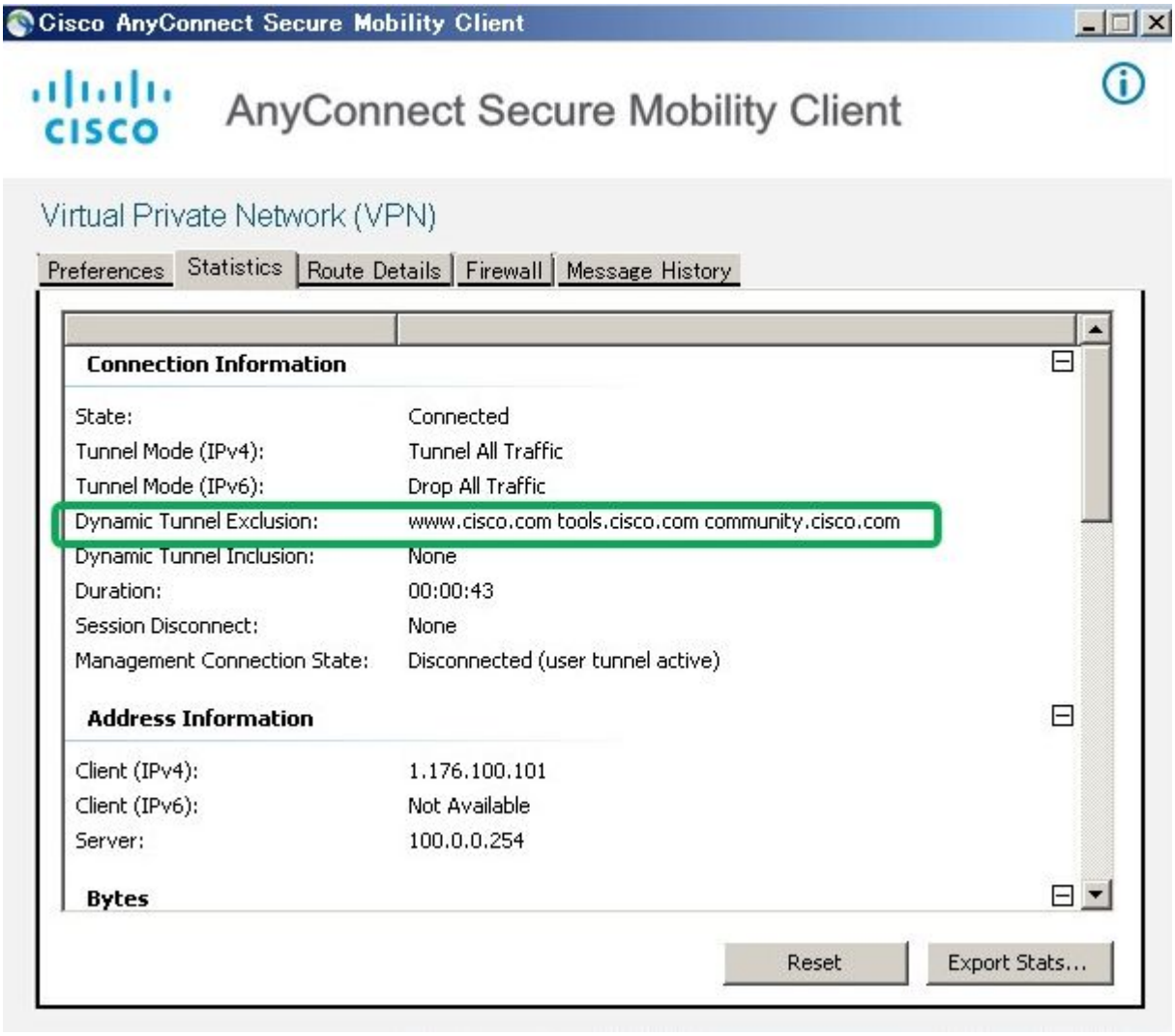
anyconnect-custom dynamic-split-exclude-domains value cisco-site

Limitações

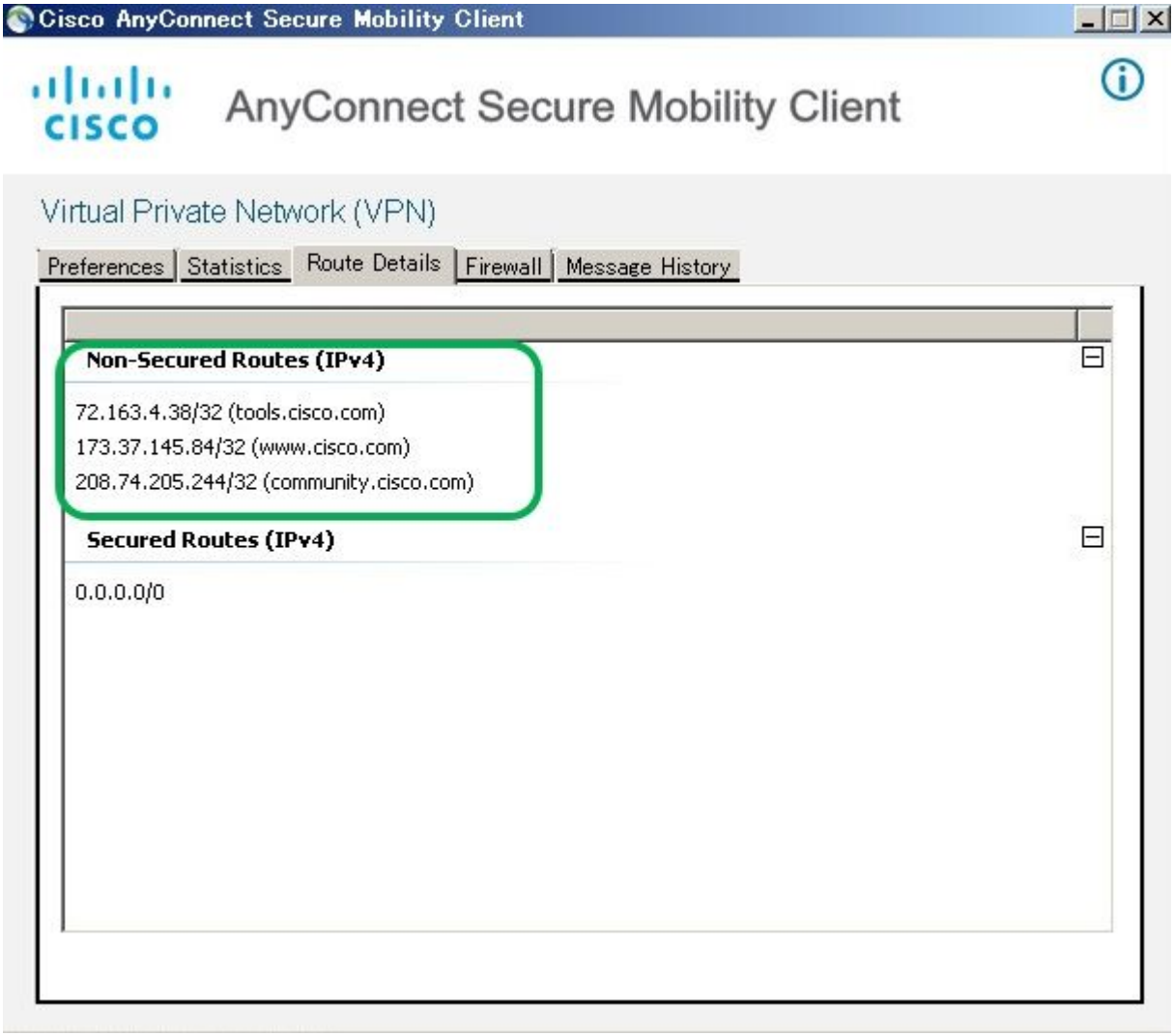
- O ASA versão 9.0 ou posterior é necessário para usar os atributos personalizados do Dynamic Split Tunneling.
- Não há suporte para curinga no campo Valores.
- O Dynamic Split Tunneling não é suportado em dispositivos iOS (Apple) (Solicitação de Aprimoramento: '[ID de bug Cisco CSCvr54798]').

Verificar

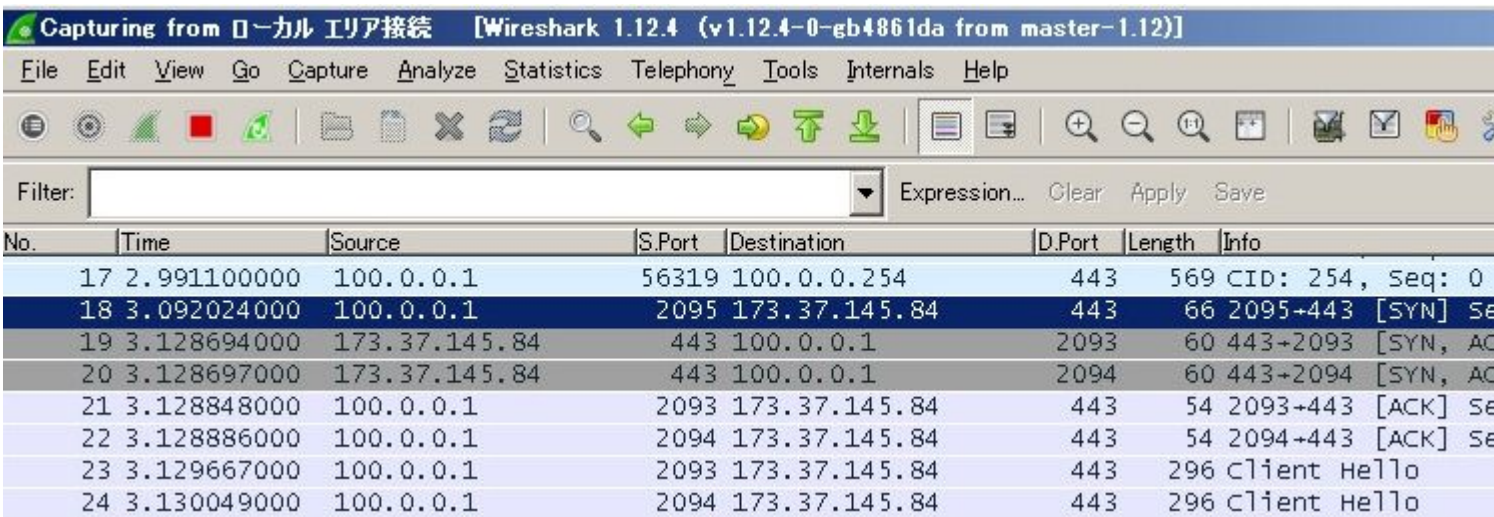
Para verificar se os switches **Dynamic Tunnel Exclusions,** Lançamento **AnyConnect** no cliente, clique em **Advanced Window** > **Statistics,** como mostra a imagem:



Você também pode navegar para **Advanced Window** > **Route Details** na qual você pode verificar **Dynamic Tunnel Exclusions** estão listados em **Non-Secured Routes,** conforme mostrado na imagem.



Neste exemplo, você configurou www.cisco.com em **Dynamic Tunnel Exclusion list** e a captura do Wireshark coletada na interface física do cliente AnyConnect confirma que o tráfego para www.cisco.com (198.51.100.0) não é criptografado pelo DTLS.



Troubleshooting

Caso o curinga seja usado no campo Valores

Se um curinga estiver configurado no campo Valores, por exemplo, ***.cisco.com** estiver configurado em Valores, a sessão do AnyConnect será desconectada, como mostrado nos logs:

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01>
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Firs
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Clie
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebV
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session d
```

> **Observação**: como alternativa, você pode usar o domínio **cisco.com** em Valores para permitir FQDNs como **www.cisco.com** e tools.cisco.com.

Caso as rotas não seguras não sejam vistas na guia Route Details (Detalhes da rota)

O cliente AnyConnect aprende e adiciona automaticamente o endereço IP e o FQDN na guia Detalhes da rota, quando o cliente inicia o tráfego para os destinos excluídos.

Para verificar se os usuários do AnyConnect estão atribuídos à política de grupo do Anyconnect correta, você pode executar o comando '**show vpn-sessiondb anyconnect filter name**
'

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                  Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373                Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
```

```
Security Grp : none
```

Solução de problemas gerais

Você pode usar o AnyConnect Diagnostics and Reporting Tool (DART) para coletar os dados que são úteis para solucionar problemas de instalação e conexão do AnyConnect. O assistente do DART é usado no computador que executa o AnyConnect. O DART reúne os registros, o status e as informações de diagnóstico para a análise do Cisco Technical Assistance Center (TAC) e não exige os privilégios de administrador para ser executado no computador cliente.

Informações Relacionadas

- **Guia do administrador do Cisco AnyConnect Secure Mobility Client, versão 4.7 - Sobre o Dynamic Split Tunneling**
- **ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.13 - Configure Dynamic Split Tunneling**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.