# Corrigir interrupções no fluxo de tráfego causadas por reconexões do AnyConnect

## Contents



## Introdução

Este documento descreve o que acontece quando um cliente AnyConnect se reconecta ao Adaptive Security Appliance (ASA) em exatamente um minuto.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

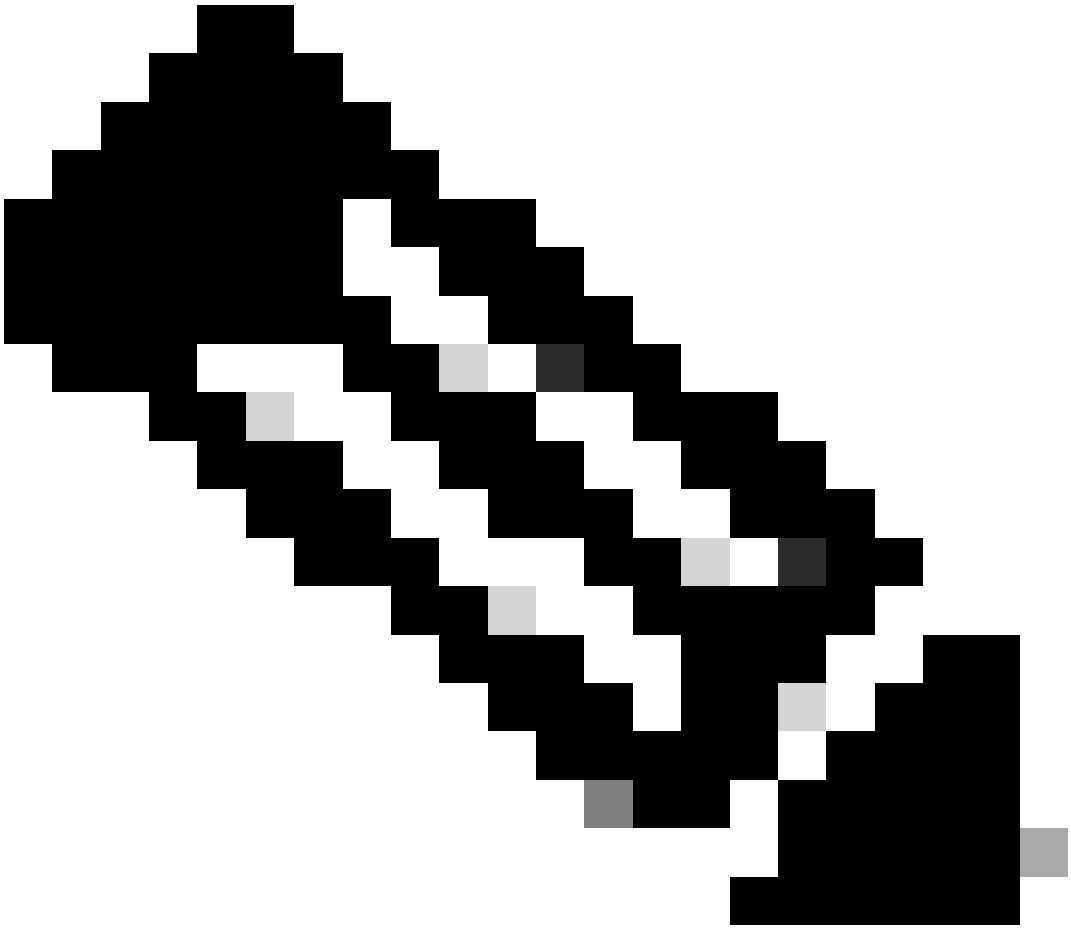
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Produtos Relacionados

Estes produtos foram afetados por este problema:

- ASA versão 9.17
- AnyConnect Client versão 4.10

## Informações de Apoio

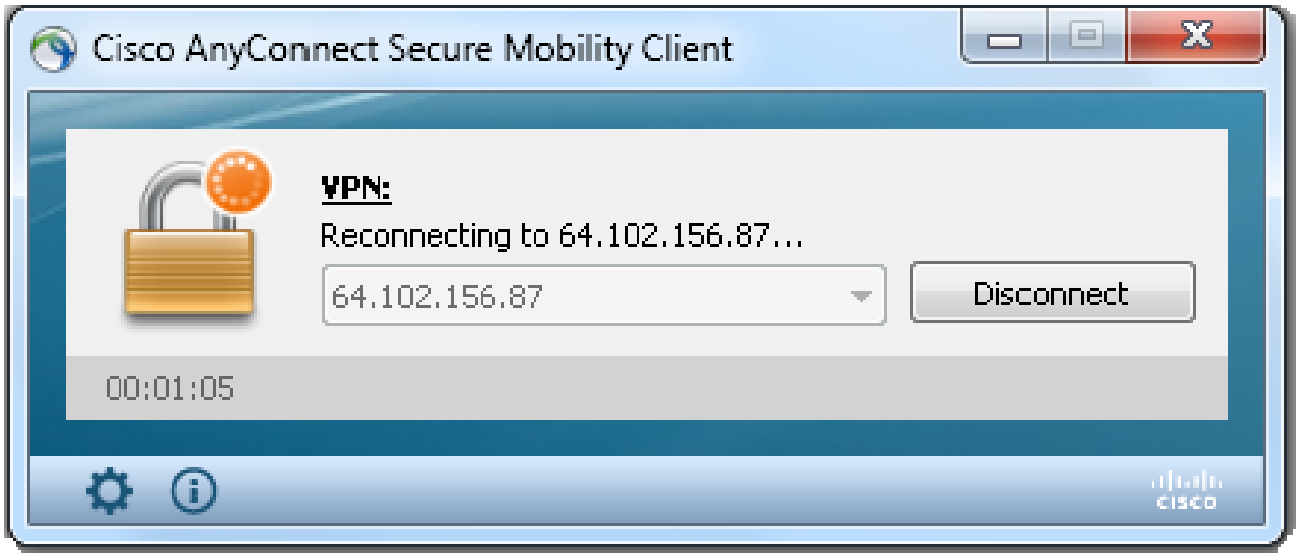


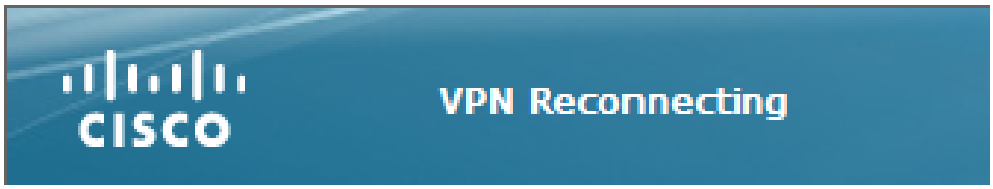
> Observação: o AnyConnect foi renomeado para Cisco Secure Client. Nada mais mudou, apenas o nome e o processo de instalação é o mesmo.

Se o cliente AnyConnect se reconectar ao Adaptive Security Appliance (ASA) em exatamente um minuto, os usuários não poderão receber tráfego pelo túnel Transport Layer Security (TLS) até que o AnyConnect se reconecte. Isso depende de alguns outros fatores discutidos neste documento.

## Sintomas

Neste exemplo, o cliente AnyConnect é mostrado quando se reconecta ao ASA.




Este syslog é visto no ASA:

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

# Descrição do problema

Esses registros do Diagnostics and Reporting Tool (DART) são exibidos com este problema:

<#root>

```
****************************************
```

Date : 11/16/2022
Time : 01:28:50
Type : Warning
Source : acvpnagent

Description : Reconfigure reason code 16:

**New MTU configuration.**

```
****************************************

Date        : 11/16/2022
Time        : 01:28:50
Type        : Information
```

```
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

****************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Warning
Source      : acvpnagent

Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.

****************************************
```

Causas

A causa desse problema é a falha na criação de um túnel DTLS (Datagram Transport Layer Security). Isso pode ocorrer por duas razões:

- O DTLS está bloqueado em algum lugar no caminho.
- Uso de uma porta DTLS não padrão.

O DTLS está bloqueado em algum lugar no caminho

A partir do ASA versão 9.x e do AnyConnect versão 4.x, uma otimização foi introduzida na forma de Unidades de Transição Máxima (MTUs - Maximum Transition Units) distintas que são negociadas para TLS/DTLS entre o cliente/ASA. Anteriormente, o cliente derivou uma estimativa aproximada de MTU que cobria TLS/DTLS e era obviamente inferior ao ideal. Agora, o ASA calcula a sobrecarga de encapsulamento para TLS/DTLS e deriva os valores de MTU de acordo.

Enquanto o DTLS estiver habilitado, o cliente aplicará o MTU do DTLS (neste caso, 1418) no adaptador VPN (que é habilitado antes do túnel DTLS ser estabelecido e é necessário para a aplicação de rotas/filtros), para garantir o desempenho ideal. Se o túnel DTLS não puder ser estabelecido ou for descartado em algum momento, o cliente efetuará o failover para TLS e ajustará a MTU no adaptador virtual (VA) para o valor de MTU de TLS (isso requer uma reconexão em nível de sessão).

Resolução

Para eliminar essa transição visível de **DTLS > TLS**, o administrador pode configurar um grupo de túneis separado para acesso TLS apenas para usuários que tenham problemas com o estabelecimento do túnel DTLS (como devido a restrições de firewall).

- A melhor opção é definir o valor de MTU do AnyConnect para ser inferior ao MTU do TLS, que é negociado em seguida.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect mtu 1300
```

Isso faz com que os valores de MTU de TLS e DTLS sejam iguais. As reconexões não são vistas nesse caso.

- A segunda opção é permitir a fragmentação.

```
group-policy ac_users_group attributes
 webvpn
  anyconnect ssl df-bit-ignore enable
```

Com a fragmentação, pacotes grandes (cujo tamanho excede o valor de MTU) podem ser fragmentados e enviados através do túnel TLS.

- A terceira opção é definir o Tamanho Máximo de Segmento (MSS) como 1460 mostrado aqui:

```
sysopt conn tcpmss 1460
```

Nesse caso, o MTU de TLS pode ser 1427 (RC4/SHA1), que é maior que o MTU de DTLS 1418 (AES/SHA1/LZS). Isso resolve o problema com o TCP do ASA para o cliente AnyConnect (graças ao MSS), mas o grande tráfego UDP do ASA para o cliente AnyConnect pode sofrer com isso, pois pode ser descartado pelo cliente AnyConnect devido ao menor MTU 1418 do cliente AnyConnect. Se sysopt conn tcpmss for modificado, isso pode afetar outros recursos, como túneis VPN IPSec LAN a LAN (L2L).

Reconectar Fluxo de Trabalho

Suponha que essas cifras estejam configuradas:

ssl cipher tlsv1.2 custom AES256-SHA256 AES128-SHA256 DHE-RSA-AES256-SHA256

Esta sequência de eventos ocorre neste caso:

- O AnyConnect estabelece um túnel pai e um túnel de dados TLS com AES256-SHA256 como a criptografia SSL.
- O DTLS está bloqueado no caminho e um túnel DTLS não pode ser estabelecido.
- O ASA anuncia parâmetros para o AnyConnect, que inclui valores de MTU TLS e DTLS, que são dois valores separados.
- O MTU de DTLS é 1418 por padrão.
- A MTU de TLS é calculada a partir do valor de sysopt conn tcpmss (o padrão é 1380). É assim que a MTU de TLS é derivada (conforme visto na saída do comando debug webvpn anyconnect):

1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347

- O AnyConnect ativa o adaptador de VPN e atribui MTU de DTLS a ele, na expectativa de que ele possa se conectar via DTLS.
- O cliente AnyConnect agora está conectado e o usuário vai para um site específico.
- O navegador envia TCP SYN e define MSS = 1418-40 = 1378 nele.
- O servidor HTTP no interior do ASA envia pacotes de tamanho 1418.
- O ASA não pode colocá-los no túnel e não pode fragmentá-los, pois eles têm o conjunto de bits Não Fragmentar (DF).
- O ASA imprime e descarta pacotes com a razão de descarte mp-svc-no-fragment-ASP.

%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347)

- Ao mesmo tempo, o ASA envia o Destino ICMP Inalcançável, Fragmentação Necessária, ao remetente:

```
%ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- Se o Internet Control Message Protocol (ICMP) for permitido, o remetente retransmitirá os pacotes descartados e tudo começará a funcionar. Se o ICMP estiver bloqueado, o tráfego será bloqueado no ASA.

- Após várias retransmissões, ele entende que o túnel DTLS não pode ser estabelecido e precisa reatribuir um novo valor de MTU ao adaptador VPN.

- A finalidade dessa reconexão é atribuir uma nova MTU.

Para obter mais informações sobre o comportamento e os temporizadores de reconexão, consulte Perguntas frequentes do AnyConnect: túneis, comportamento de reconexão e temporizador de inatividade

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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.