Responda às perguntas frequentes do AnyConnect - Túneis, DPDs e temporizador de inatividade

Contents

Introduction

Este documento descreve os túneis do Cisco AnyConnect Secure Mobility Client, o comportamento de reconexão e a Dead Peer Detection (DPD) e o temporizador de inatividade.

Informações de Apoio

Tipos de túneis

Há dois métodos usados para conectar uma sessão do AnyConnect:

- Pelo portal (sem cliente)
- Através do aplicativo independente

Com base na maneira como você se conecta, você cria três túneis diferentes (sessões) no Cisco Adaptive Security Appliance (ASA), cada um com uma finalidade específica:

1. Sem Cliente ou Túnel Pai: Esta é a sessão principal criada na negociação para configurar o token de sessão necessário caso uma reconexão seja necessária devido a problemas de conectividade de rede ou hibernação. Com base no mecanismo de conexão, o ASA lista a sessão como Sem cliente (Weblaunch via Portal) ou Pai (AnyConnect independente).

   Observação: o AnyConnect-Parent representa a sessão quando o cliente não está conectado ativamente. Efetivamente, ele funciona de forma semelhante a um cookie, pois é uma entrada de banco de dados no ASA que mapeia a conexão de um determinado cliente. Se o cliente dorme/hiberna, os túneis (protocolos IPsec/Internet Key Exchange (IKE)/Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS)) são desativados, mas o pai permanece até que o temporizador de ociosidade ou o tempo máximo de conexão entrem em vigor. Isso permite que o usuário se reconecte sem reautenticar.

2. Túnel SSL: a conexão SSL é estabelecida primeiro, e os dados são passados por essa conexão enquanto tentam estabelecer uma conexão DTLS. Uma vez estabelecida a conexão DTLS, o cliente envia os pacotes através da conexão DTLS em vez da conexão SSL. Por outro lado, os pacotes de controle sempre passam pela conexão SSL.

3. Túnel DTLS: quando o túnel DTLS é totalmente estabelecido, todos os dados se movem para o túnel DTLS e o túnel SSL é usado somente para tráfego ocasional do canal de controle. Se algo acontecer com o User Datagram Protocol (UDP), o túnel DTLS será desativado e todos os dados passarão pelo túnel SSL novamente.

Exemplo de saída do ASA

Aqui está um exemplo de saída dos dois métodos de conexão.

AnyConnect conectado via Web - Início:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

AnyConnect conectado por meio do aplicativo independente:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
```

```
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DPDs e temporizadores de inatividade

Quando uma sessão é considerada uma sessão inativa?

A sessão é considerada Inativa (e o temporizador começa a aumentar) somente quando o Túnel SSL não existe mais na sessão. Assim, cada sessão recebe um carimbo de data e hora com o tempo de descarte do túnel SSL.

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

Quando o ASA descarta o túnel SSL?

Há duas maneiras de desconectar um túnel SSL:

1. **DPD** - Os DPDs são usados pelo cliente para detectar uma falha na comunicação entre o cliente AnyConnect e o headend ASA. Os DPDs também são usados para limpar recursos no ASA. Isso garante que o headend não mantenha conexões no banco de dados se o endpoint não responder aos pings DPD. Se o ASA enviar um DPD ao endpoint e responder, nenhuma ação será tomada. Se o ponto final não estiver respondendo, após o número máximo de retransmissão (depende se IKEv1 ou IKEv2 for usado) o ASA desfaz o túnel no banco de dados de sessão e move a sessão para o modo "Aguardando para Retomar". Isso significa que o DPD do head-end foi iniciado e o head-end não se comunica mais com o cliente. Nessas situações, o ASA mantém o Túnel pai ativo para permitir que o usuário faça roaming das redes, entre em modo de espera e recupere a sessão. Essas sessões são contadas em relação às sessões conectadas ativamente e são limpas sob estas condições: User Idle-TimeoutO cliente retoma a sessão original e encerra a sessão corretamente Para configurar DPDs, use o comando **anyconnect dpd-interval** sob os atributos WebVPN nas configurações da política de grupo. Por padrão, o DPD é ativado e definido como 30 segundos para o ASA (gateway) e o cliente.

Cuidado: Esteja ciente da ID de bug da Cisco CSCts66926 - O DPD não consegue encerrar o túnel DTLS após a perda da conexão do cliente.

2. **Idle-Timeout** - A segunda maneira pela qual o túnel SSL é desconectado é quando o Idle-Timeout para este túnel expira. Entretanto, lembre-se de que não é apenas o túnel SSL que deve ficar ocioso, mas também o túnel DTLS. A menos que a sessão DTLS expire, o Túnel SSL será retido no banco de dados.

Por que os keepalives precisam ser ativados se os DPDs já estão ativados?

Como explicado anteriormente, o DPD não elimina a própria sessão do AnyConnect. Ele simplesmente elimina o túnel nessa sessão para que o cliente possa restabelecer o túnel. Se o cliente não puder restabelecer o túnel, a sessão permanecerá até que o temporizador de ociosidade expire no ASA. Como os DPDs são ativados por padrão, os clientes podem geralmente ser desconectados devido ao fechamento de fluxos em uma direção com dispositivos NAT (Network Address Translation), Firewall e Proxy. A habilitação de keepalives em intervalos baixos, como 20 segundos, ajuda a evitar isso.

Os keepalives são ativados sob os atributos WebVPN de uma política de grupo específica com o comando **anyconnect ssl keepalive** comando. Por padrão, os temporizadores são definidos como 20 segundos.

Comportamento do AnyConnect Client em caso de reconexões

O AnyConnect tenta se reconectar se a conexão for interrompida. Isso não é configurável, automaticamente. Desde que a sessão VPN no ASA ainda seja válida e se o AnyConnect puder restabelecer a conexão física, a sessão VPN será retomada.

O recurso de reconexão continua até que o timeout da sessão ou o timeout de desconexão, que é na verdade o timeout de ociosidade, expire (ou 30 minutos se nenhum timeout for configurado). Quando elas expirarem, o cliente não poderá continuar porque as sessões VPN já foram descartadas no ASA. O cliente continua enquanto ele pensa que o ASA ainda tem a sessão VPN.

O AnyConnect se reconecta, independentemente de como a interface de rede muda. Não importa se o endereço IP da placa de rede (NIC) muda ou se a conectividade muda de uma NIC para outra NIC (sem fio para com fio ou vice-versa).

Ao considerar o processo de reconexão do AnyConnect, há três níveis de sessões que você deve lembrar. Além disso, o comportamento de reconexão de cada uma dessas sessões é livremente acoplado, no sentido de que qualquer uma delas pode ser restabelecida sem uma dependência dos elementos de sessão da camada anterior:

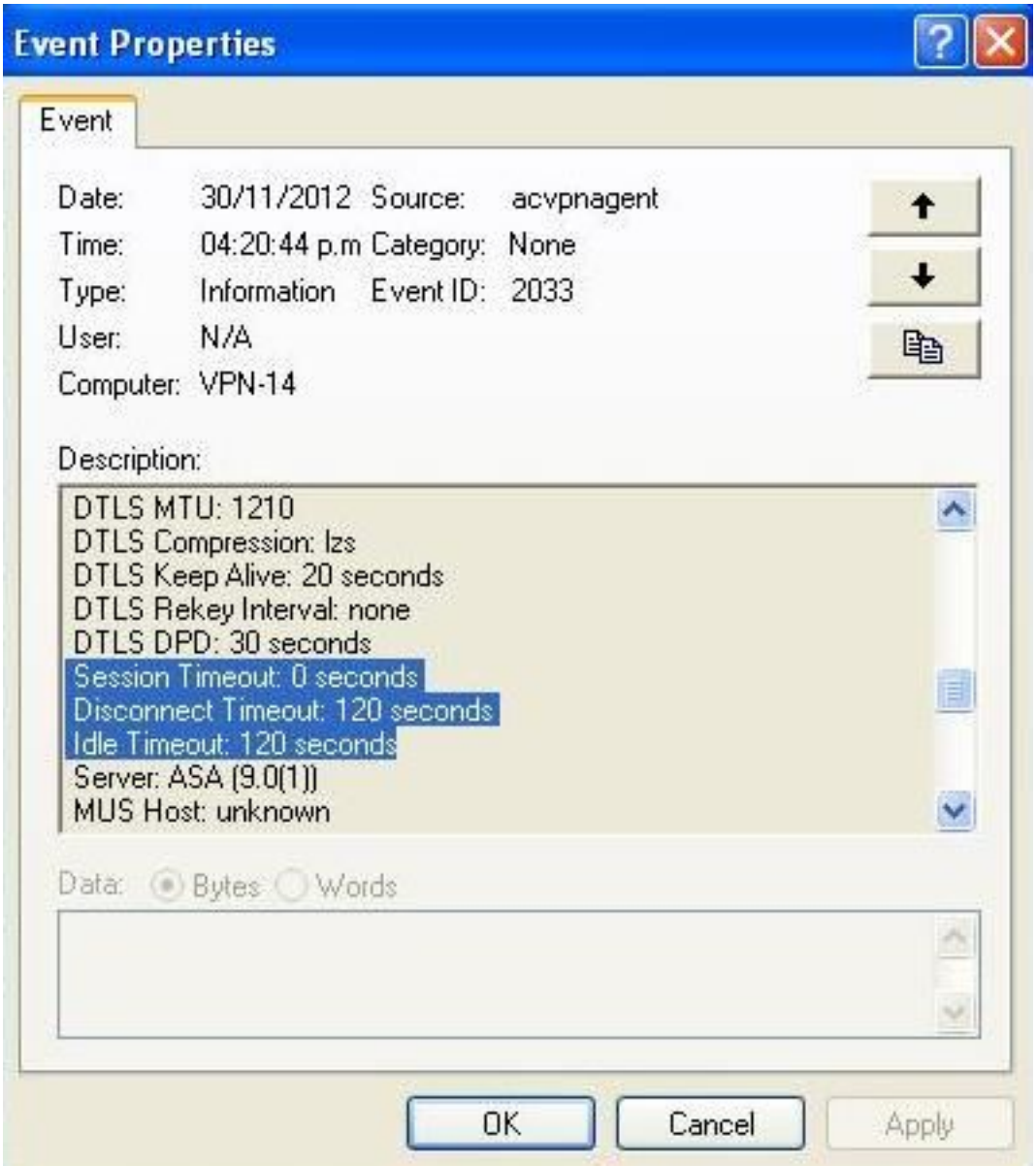
1. Reconexões TCP ou UDP [Camada OSI 3]
2. TLS, DTLS ou IPSec(IKE+ESP) [Camada 4 do modelo OSI] - Não há suporte para a retomada de TLS.
3. VPN [OSI layer 7] - O token de sessão VPN é usado como um token de autenticação para restabelecer a sessão VPN sobre um canal seguro quando há uma interrupção. É um mecanismo proprietário que é muito semelhante, conceitualmente, a como um token Kerberos ou um certificado de cliente é usado para autenticação. O token é exclusivo e gerado criptograficamente pelo head-end, que contém a ID da sessão mais um payload

aleatório gerado criptograficamente. Ele é passado para o cliente como parte do estabelecimento de VPN inicial depois que um canal seguro para o headend é estabelecido. Ele permanece válido durante o tempo de vida da sessão no head-end e é armazenado na memória do cliente, que é um processo privilegiado.
Dica: estas versões do ASA e mais recentes contêm um token de sessão criptográfica mais forte: 9.1(3) e 8.4(7.1)

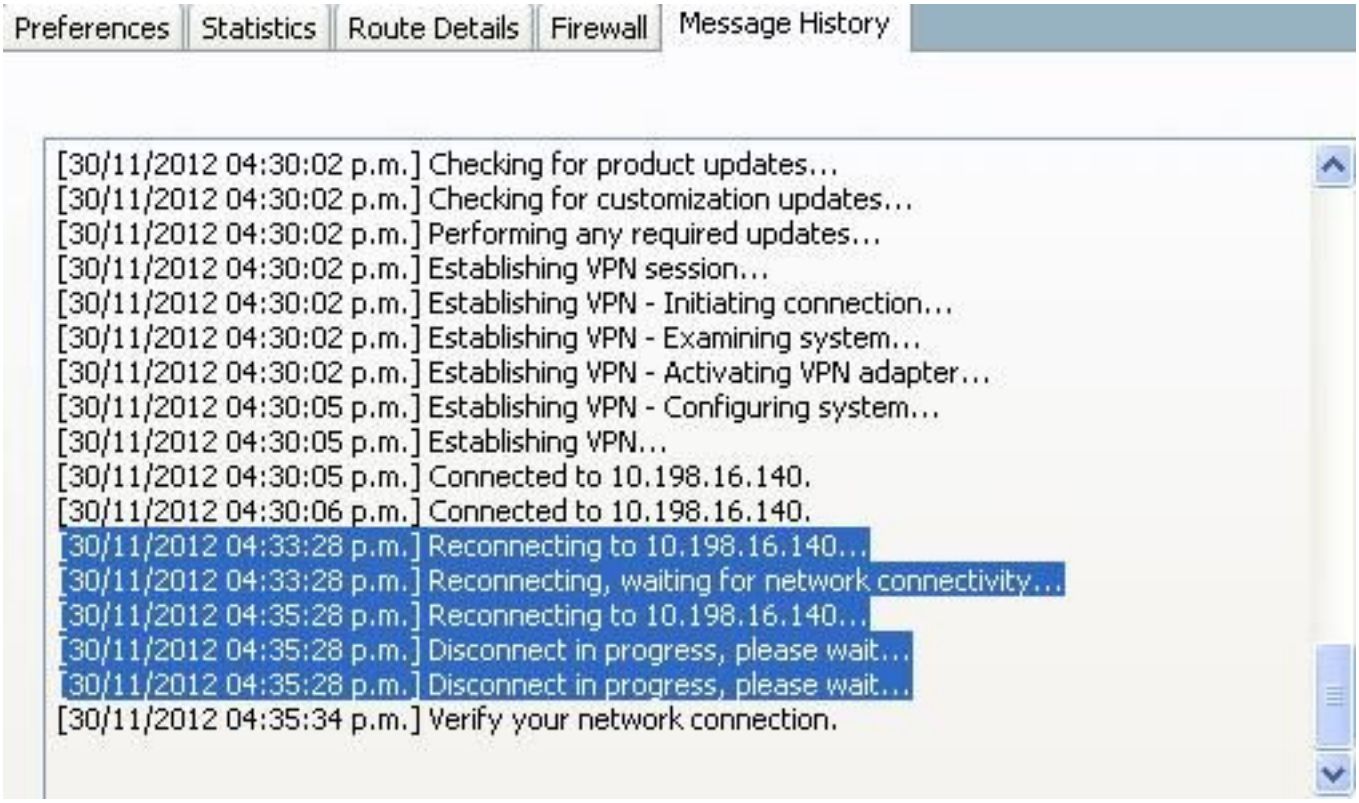
O processo real

Um temporizador de tempo limite de desconexão é iniciado assim que a conexão de rede é interrompida. O cliente AnyConnect continua tentando se reconectar, contanto que esse temporizador não expire. O Tempo Limite de Desconexão está definido com a configuração mais baixa do **Tempo Limite Ocioso da** Política de Grupo ou do **Tempo Máximo de Conexão**.

O valor desse temporizador é visto no Visualizador de Eventos para a sessão do AnyConnect na negociação:



Neste exemplo, a sessão se desconecta após dois minutos (120 segundos), que podem ser verificados no Histórico de mensagens do AnyConnect:



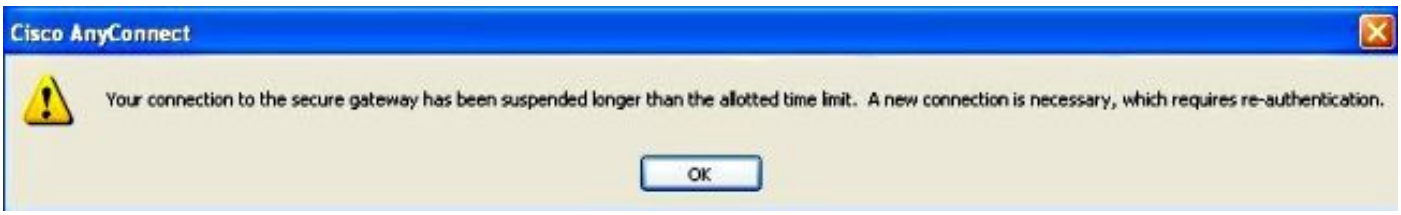
Dica: para que o ASA responda a um cliente que tenta se reconectar, a sessão Parent-Tunnel ainda deve existir no banco de dados do ASA. No caso de failover, os DPDs também precisam ser ativados para que o comportamento de reconexão funcione.

Como é visível nas mensagens anteriores, a reconexão falhou. No entanto, se a reconexão for bem-sucedida, isto é o que acontece:

1. O túnel pai permanece o mesmo; isso não é renegociado porque esse túnel mantém o token de sessão necessário para a sessão se reconectar.
2. Novas sessões SSL e DTLS são geradas, e diferentes portas de origem são usadas na reconexão.
3. Todos os valores de Idle-Timeout são restaurados.
4. O tempo limite de inatividade é restaurado.

Cuidado: esteja ciente da ID de bug Cisco CSCtg33110. O banco de dados da sessão VPN não atualiza o endereço IP público no banco de dados da sessão ASA quando o AnyConnect se reconecta.

Nessa situação em que as tentativas de reconexão falham, você encontra esta mensagem:



Observação: esta solicitação de aprimoramento foi preenchida para tornar isso mais granular: ID do Cisco bug CSCsl52873 - O ASA não tem um tempo limite desconectado configurável para o AnyConnect.

Comportamento do AnyConnect Client em caso de suspensão do sistema

Há um recurso de roaming que permite que o AnyConnect se reconecte após a suspensão do PC. O cliente continua tentando até que os tempos limite de sessão ou ociosos expirem e o cliente não desmonte imediatamente o túnel quando o sistema entra em hibernação/standby. Para usuários que não desejam esse recurso, defina o tempo limite da sessão como um valor baixo para impedir reconexões de suspensão/retomada.

> **Observação**: após a correção do bug da Cisco ID CSCso17627 (Versão 2.3(111)+), um botão de controle foi introduzido para desabilitar esse recurso de reconexão ao retomar.

O comportamento de Reconexão automática para o AnyConnect pode ser controlado por meio do perfil XML do AnyConnect com esta configuração:

```
      <AutoReconnect UserControllable="true">true
<AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Com essa alteração, o AnyConnect tenta se reconectar quando o computador volta da espera. A preferência AutoReconnectBehavior assume como padrão DisconnectOnSuspend. Esse comportamento é diferente do AnyConnect Client Release 2.2. Para reconectar após retomar, o administrador de rede deve definir ReconnectAfterResume no perfil ou tornar as preferências AutoReconnect e AutoReconnectBehavior controláveis pelo usuário no perfil para permitir que os usuários as definam.

Perguntas mais freqüentes

Q1. O AnyConnect DPD tem um intervalo, mas nenhuma nova tentativa - quantos pacotes ele precisa perder antes de marcar a extremidade remota como inoperante?

A. Do ponto de vista do cliente, os DPDs apenas removem um túnel durante a fase de estabelecimento do túnel. Se o cliente encontrar três novas tentativas (envia quatro pacotes) durante o estágio de estabelecimento do túnel e não receber uma resposta do servidor VPN primário, ele voltará a usar um dos servidores de backup se estiver configurado. No entanto, uma vez que o túnel tenha sido estabelecido, os DPDs perdidos não têm nenhum impacto sobre o túnel da perspectiva dos clientes. O impacto real dos DPDs é no servidor VPN, conforme explicado na seção DPDs e Temporizadores de inatividade.

Q2. O processamento de DPD é diferente para o AnyConnect com IKEv2?

R. Sim, o IKEv2 tem um número fixo de novas tentativas - seis novas tentativas/sete pacotes.

Q3. Há outra finalidade para o túnel principal do AnyConnect?

A. Além de ser um mapeamento no ASA, o túnel pai é usado para enviar atualizações de imagem do AnyConnect do ASA para o cliente, pois o cliente não está conectado ativamente durante o

processo de atualização.

Q4. Você pode filtrar e fazer logoff apenas de sessões inativas?

R. Você pode filtrar sessões inativas com o comando **show vpn-sessiondb anyconnect filter inative**. No entanto, não há nenhum comando para fazer logoff apenas de sessões inativas. Em vez disso, você precisa fazer logoff de sessões específicas ou de todas as sessões por usuário (index - name), protocolo ou grupo de túneis. Uma solicitação de aprimoramento, ID do Cisco Bug CSCuh5707 , foi preenchida para adicionar a opção de fazer logoff apenas das sessões inativas.

P5. O que acontece com o túnel pai quando o tempo limite de ociosidade dos túneis DTLS ou TLS expira?

R. O temporizador "Idle TO Left" da sessão AnyConnect-Parent é redefinido após o encerramento do túnel SSL ou do túnel DTLS. Isso permite que o "timeout de ociosidade" atue como um timeout "desconectado". Esse efetivamente se torna o tempo permitido para o cliente se reconectar. Se o cliente não se reconectar dentro do temporizador, o Túnel pai será encerrado.

P6. Por que manter a sessão depois que os temporizadores de DPD desconectaram a sessão e por que o ASA não libera o endereço IP?

R. O headend não tem conhecimento do estado do cliente. Nesse caso, o ASA espera que o cliente se reconecte até que a sessão expire no temporizador de ociosidade. O DPD não elimina uma sessão do AnyConnect; ele simplesmente elimina o túnel (dentro dessa sessão) para que o cliente possa restabelecer o túnel. Se o cliente não restabelecer um túnel, a sessão permanecerá até que o temporizador de ociosidade expire.

Se a preocupação for com as sessões que estão esgotadas, defina os logons simultâneos com um valor baixo, como um. Com essa configuração, os usuários que têm uma sessão no banco de dados de sessão têm sua sessão anterior excluída quando efetuam logon novamente.

P7. Qual é o comportamento se o ASA falhar de Ativo para Standby?

R. Inicialmente, quando a sessão é estabelecida, os três túneis (pai, SSL e DTLS) são replicados para a unidade em standby; quando o ASA falha, as sessões DTLS e TLS são restabelecidas, pois não são sincronizadas com a unidade em standby, mas qualquer fluxo de dados através dos túneis deve funcionar sem interrupção após a sessão do AnyConnect ser restabelecida.

As sessões SSL/DTLS não têm informações de estado, portanto, o estado e o número de sequência SSL não são mantidos e podem ser bastante onerosos. Assim, essas sessões precisam ser restabelecidas do zero, o que é feito com a sessão Pai e o token de sessão.

> **Dica**: no caso de um evento de failover, as sessões de cliente VPN SSL não são transportadas para o dispositivo em standby se as manutenções de atividade estiverem desativadas.

P8. Por que existem dois timeouts diferentes, o timeout ocioso e o timeout desconectado, se ambos têm o mesmo valor?

A. Quando os protocolos foram desenvolvidos, dois intervalos diferentes foram fornecidos para:

- Tempo limite ocioso - O tempo limite ocioso é para quando nenhum dado é passado por uma conexão.
- Tempo limite desconectado - O tempo limite desconectado é para quando você desistir da sessão VPN porque a conexão foi perdida e não pode ser restabelecida.

O tempo limite desconectado nunca foi implementado no ASA. Em vez disso, o ASA envia o valor de timeout ocioso para os timeouts ocioso e desconectado ao cliente.

O cliente não usa o timeout de ociosidade, pois o ASA trata o timeout de ociosidade. O cliente usa o valor de timeout desconectado, que é o mesmo que o valor de timeout ocioso, para saber quando desistir de tentativas de reconexão, já que o ASA descartou a sessão.

Embora não esteja conectado ativamente ao cliente, o ASA expira a sessão por meio do timeout de ociosidade. O principal motivo para não implementar o timeout desconectado no ASA foi evitar a adição de outro temporizador para cada sessão VPN e o aumento da sobrecarga no ASA (embora o mesmo temporizador possa ser usado em ambas as instâncias, apenas com valores de timeout diferentes, já que os dois casos são mutuamente exclusivos).

O único valor agregado com o tempo limite desconectado é permitir que um administrador especifique um tempo limite diferente para quando o cliente não estiver conectado ativamente versus ocioso. Como observado anteriormente, o bug da Cisco ID CSCsl52873 foi preenchido para isso.

P9. O que acontece quando a máquina do cliente é suspensa?

R. Por padrão, o AnyConnect tenta restabelecer uma conexão VPN quando você perde a conectividade. Por padrão, não tenta restabelecer uma conexão VPN após a retomada de um sistema. Consulte Comportamento do AnyConnect Client em caso de suspensão do sistema para obter detalhes.

P10. Quando ocorre uma reconexão, o AnyConnect Virtual Adapter oscila ou a tabela de roteamento muda?

A. Uma reconexão em nível de túnel também não funciona. Esta é uma reconexão apenas em SSL ou DTLS. Isso acontece cerca de 30 segundos antes de eles desistirem. Se o DTLS falhar, ele será simplesmente descartado. Se o SSL falhar, ele causará uma reconexão em nível de sessão. Uma reconexão em nível de sessão refaz completamente o roteamento. Se o endereço do cliente atribuído na reconexão, ou qualquer outro parâmetro de configuração que impacte o Adaptador virtual (VA), não tiver sido alterado, o VA não será desabilitado. Embora seja improvável que haja qualquer alteração nos parâmetros de configuração recebidos do ASA, é possível que uma alteração na interface física usada para a conexão VPN (por exemplo, se você desencaixar e passar de cabeada para WiFi) possa resultar em um valor de Unidade Máxima de Transmissão (MTU) diferente para a conexão VPN. O valor de MTU afeta o VA, e uma alteração nele faz com que o VA seja desabilitado e, em seguida, reabilitado.

P11. A "Reconexão automática" fornece persistência de sessão? Em caso afirmativo, há alguma funcionalidade extra adicionada ao AnyConnect Client?

A. O AnyConnect não oferece nenhuma "mágica" extra para acomodar a persistência da sessão

para aplicativos. Mas a conectividade VPN é restaurada automaticamente logo após a conectividade de rede ao gateway seguro ser retomada, desde que os tempos limite de ociosidade e de sessão configurados no ASA não tenham expirado. E, ao contrário do cliente IPsec, a reconexão automática resulta no mesmo endereço IP do cliente. Enquanto o AnyConnect tenta se reconectar, o AnyConnect Virtual Adapter permanece habilitado e no estado conectado, de modo que o endereço IP do cliente permaneça presente e habilitado no PC cliente o tempo todo, o que dá persistência ao endereço IP do cliente. Os aplicativos de PC cliente, no entanto, ainda percebem a perda de conectividade com seus servidores na rede corporativa se levar muito tempo para que a conectividade VPN seja restaurada.

P12. Esse recurso funciona em todas as variantes do Microsoft Windows (Vista 32 bits e 64 bits, XP). E o Macintosh? Ele funciona no OS X 10.4?

A. Esse recurso funciona no Mac e no Linux. Houve problemas com o Mac e o Linux, mas melhorias recentes foram feitas, particularmente para o Mac. O Linux ainda requer algum suporte adicional (bug da Cisco ID CSCsr1670, bug da Cisco ID CSCsm69213), mas a funcionalidade básica também está lá. Com relação ao Linux, o AnyConnect não reconhece que ocorreu uma suspensão/retomada (repouso/despertar). Isso basicamente tem dois impactos:

- A configuração de perfil/preferência AutoReconnectBehavior não pode ser suportada no Linux sem suporte para suspender/retomar, portanto uma reconexão sempre ocorre após suspender/retomar.
- No Microsoft Windows e Macintosh, as reconexões são executadas imediatamente no nível de sessão após a retomada, o que permite um switch mais rápido para uma interface física diferente. No Linux, como o AnyConnect desconhece completamente a suspensão/retomada, as reconexões ocorrem primeiro no nível do túnel (SSL e DTLS) e isso pode significar que as reconexões demoram um pouco mais. Mas as reconexões ainda ocorrem no Linux.

P13. Há alguma limitação para o recurso em termos de conectividade (com fio, wi-fi, 3G e assim por diante)? Ele oferece suporte à transição de um modo para outro (de Wi-Fi para 3G, 3G para com fio, etc.)?

A. O AnyConnect não está ligado a uma interface física específica durante a vida útil da conexão VPN. Se a interface física usada para a conexão VPN for perdida ou se as tentativas de reconexão excederem um determinado limite de falha, o AnyConnect não usará mais essa interface e tentará acessar o gateway seguro com quaisquer interfaces que estejam disponíveis até que os temporizadores de ociosidade ou de sessão expirem. Observe que uma alteração na interface física pode resultar em um valor de MTU diferente para o VA, o que faz com que o VA tenha que ser desabilitado e reabilitado, mas ainda com o mesmo endereço IP do cliente.

Se houver qualquer interrupção de rede (interface inoperante, redes alteradas, interfaces alteradas), o AnyConnect tenta se reconectar; não é necessária uma nova autenticação na reconexão. Isso se aplica até mesmo a um switch de interfaces físicas:

Exemplo:

```
1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in
30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs
```

P14. Como a operação de retomada é autenticada?

A. Em um currículo, você reenvia o token autenticado que permanece para o tempo de vida da sessão, e a sessão é restabelecida.

P15. A autorização LDAP também é executada na reconexão ou somente na autenticação?

A. Isso só é executado na conexão inicial.

P16. O pré-login e/ou a verificação de host é executada após a retomada?

A. Não, eles são executados somente na conexão inicial. Algo assim seria programado para o futuro recurso de Avaliação Periódica de Postura.

P17. Com relação ao Balanceamento de Carga (LB - Load Balancing) da VPN e ao reinício da conexão, o cliente se conecta de volta diretamente ao membro do cluster ao qual estava conectado antes?

R: Sim, isso está correto, já que você não resolve novamente o nome do host via DNS para restabelecer uma sessão atual.

Informações Relacionadas

- Referência do ASA DPD: ID de bug da Cisco CSCsr63074 - DPD não enviado quando o peer está inativo e o túnel não está ocioso em s2s com 7.2.4
- Suporte Técnico e Documentação - Cisco Systems

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.