AnyConnect FAQ: Os túneis, reconectam o comportamento, e o temporizador de inatividade

Índice

Introdução

Este documento descreve em detalhe alguns pontos importantes sobre os túneis do Cliente de mobilidade Cisco AnyConnect Secure (AnyConnect), o comportamento da reconexão e o Dead Peer Detection (DPD), e o temporizador de inatividade.

Informações de Apoio

Tipos de túneis

Há dois métodos usados a fim conectar uma sessão de AnyConnect:

- Através do portal (sem clientes)
- Através do aplicativo isolado

Baseado na maneira você conecta, você cria três túneis diferentes (sessões) no ASA, cada um com uma finalidade específica:

1. **Sem clientes ou Pai-túnel:** Esta é a sessão principal que é criada na negociação a fim estabelecer o token da sessão que é necessário caso que uma reconexão é necessário devido às questões de conectividade de rede ou à hibernação. Baseado no mecanismo de conexão, a ferramenta de segurança adaptável de Cisco (ASA) alista a sessão como os sem clientes (Weblaunch através do portal) ou o pai (AnyConnect autônomo).

   Note: O AnyConnect-pai representa a sessão quando o cliente não é conectado ativamente. Eficazmente, trabalha similar a um Cookie, que é uma entrada no base de dados no ASA esse traça à conexão de um cliente específico. Se o cliente fechou ou sonos, os túneis (IPsec/Internet Key Exchange (IKE)/protocolos Transport Layer Security do Transport Layer Security (TLS) /Datagram (DTL)) são rasgados para baixo, mas as sobras do pai até o tempo de conexão do temporizador de ociosidade ou do máximo tomam o efeito. Isto permite que o usuário reconecte sem reauthenticating.

2. **Secure sockets layer (SSL) - Túnel:** A conexão SSL é estabelecida primeiramente, e os dados estão passados sobre esta conexão quando tentarem estabelecer uma conexão DTL. Uma vez que a conexão DTL é estabelecida, o cliente envia os pacotes através da conexão DTL em vez através da conexão SSL. Os pacotes de controle, por outro lado, vão sempre sobre a conexão SSL.

3. **DTL-túnel:** Quando o DTL-túnel é estabelecido inteiramente, todos os dados se movem para o DTL-túnel, e o SSL-túnel é usado somente para o tráfego ocasional do canal de controle. Se algo acontece ao User Datagram Protocol (UDP), o DTL-túnel está rasgado para baixo e todos os dados passam através do SSL-túnel outra vez.

Exemplo de saída do ASA

Está aqui o exemplo de saída dos dois métodos de conexão.

AnyConnect conectou através do Web-lançamento:

```
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 conectou através do aplicativo isolado:

```
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
```

DPD e temporizadores de inatividade

Quando uma sessão é considerada uma sessão inativa?

A sessão estiver considerada inativa (e o temporizador começa a aumentar) somente quando o SSL-túnel não existe anymore na sessão. Assim, cada sessão tempo-é carimbada com o tempo de gota do SSL-túnel.

```
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 deixa cair o SSL-túnel?

Há duas maneiras que um SSL-túnel pode ser desligado:

1. **DPD** - Os DPD são usados pelo cliente a fim detectar uma falha nas comunicações entre o cliente de AnyConnect e a extremidade principal ASA. Os DPD são usados igualmente a fim limpar recursos no ASA. Isto assegura-se de que a extremidade principal não mantenha conexões no base de dados se o valor-limite é nonresponsive aos sibilos DPD. Se o ASA envia um DPD ao valor-limite e responde, nenhuma ação está tomada. Se o valor-limite não é responsivo, o ASA rasga para baixo o túnel no base de dados da sessão, e move a sessão em uma “espera para recomeçar” o modo. O que este os meios são que o DPD da extremidade principal começou, e a extremidade principal já não comunica-se com o cliente. Em tais situações, o ASA mantém o Pai-túnel a fim permitir que o usuário vagueie redes, vá dormir, e recupere a sessão. Estas sessões contam contra sessões ativo-conectadas e são

canceladas sob estas condições:
Quietude-intervalo do usuárioO cliente recomeça a sessão original e os logs para fora corretamente
A fim configurar DPD, use o comando do DPD-intervalo do anyconnect sob os atributos WebVPN nos ajustes da grupo-política. À revelia, o DPD é permitido e ajustado a 30 segundos para o ASA (gateway) e o cliente.

Caution: Esteja ciente da identificação de bug Cisco CSCts66926 - O DPD não termina DTL escava um túnel após conexão de cliente perdida.

2. **Quietude-intervalo** - A segunda maneira que o SSL-túnel está desligado é quando o Quietude-intervalo para este túnel expira. Contudo, recorde que é não somente o SSL-túnel que deve rodar em marcha lenta para fora, mas os DTL escavam um túnel também. A menos que o tempo de sessão DTL para fora, o SSL-túnel for retido no base de dados.

Por que o Keepalives precisa de ser permitido se os DPD são permitidos já?

Como explicado previamente, o DPD não mata a sessão própria de AnyConnect. Mata meramente o túnel dentro dessa sessão de modo que o cliente possa restabelecer o túnel. Se o cliente não pode restabelecer o túnel, a sessão permanece até que o temporizador de ociosidade expire no ASA. Desde que os DPD são permitidos à revelia, os clientes puderam frequentemente obter desligado devido aos fluxos que fecham-se em um sentido com os dispositivos do Network Address Translation (NAT), do Firewall e do proxy. Permitir o Keepalives em baixos intervalos, tais como 20 segundos, ajuda a impedir esta.

O Keepalives é permitido sob os atributos WebVPN de uma grupo-política particular com o comando keepalive SSL do anyconnect. À revelia, os temporizadores são ajustados a 20 segundos.

O comportamento do cliente de AnyConnect em caso de reconecta

AnyConnect tentará reconectar se a conexão é interrompida. Isto não é configurável, automaticamente. Enquanto a sessão de VPN no ASA é ainda válida e se AnyConnect pode restabelecer a conexão física, a sessão de VPN estará recomeçada.

A característica da reconexão continua até o timeout de sessão ou o intervalo da disconexão, que é realmente o idle timeout, expira (ou 30 minutos se nenhum intervalo é configurado). Uma vez que estes expiram, você não deve continuar porque o ASA terá deixado cair a sessão de VPN. O cliente continuará enquanto pensa que o ASA ainda tem a sessão de VPN.

AnyConnect reconectará não importa como a interface de rede muda. Não importa se o endereço IP de Um ou Mais Servidores Cisco ICM NT das mudanças do Network Interface Cards (NIC), ou se a Conectividade comuta de um NIC a um outro NIC (Sem fio ao prendido ou vice versa).

Quando você considera o processo da reconexão para AnyConnect, há três níveis das sessões que você deve recordar. Adicionalmente, o comportamento da reconexão de cada um destas sessões é acoplado frouxamente, que alguns delas podem ser restabelecidos sem uma dependência nos elementos da sessão da camada precedente:

1. O TCP ou o UDP reconectam [camada de osi 3]
2. TLS, DTL, ou IPsec (IKE+ESP) [a camada de osi 4] - ressunção TLS não é apoiada.
3. VPN [camada de osi 7] - O token da sessão de VPN está usado porque um token de autenticação a fim restabelecer a sessão de VPN sobre um canal fixado quando houver um rompimento. É um mecanismo proprietário que seja muito similar, conceptualmente, a como um token do Kerberos ou um certificado de cliente são usados para a autenticação. O token é original e gerado criptograficamente pela extremidade principal, que contém o ID de sessão mais um payload aleatório criptograficamente gerado. Está passado ao cliente como parte do estabelecimento inicial VPN depois que um canal seguro à extremidade principal é estabelecido. Permanece válido para a vida da sessão na extremidade principal, e é armazenado na memória do cliente, que é um processo privilegiado.
   Tip: Estas liberações ASA e contêm mais tarde um token criptograficamente mais forte da sessão: 9.1(3) e 8.4(7.1)

O processo real

Um temporizador do intervalo da disconexão é começado assim que a conexão de rede for interrompida. O cliente de AnyConnect continua a tentar reconectar enquanto este temporizador não expira. O intervalo da disconexão é ajustado ao mais baixo ajuste do Quietude-**intervalo da** política do grupo ou do **tempo de conexão máximo**.

O valor deste temporizador é considerado no visualizador de eventos para a sessão de AnyConnect na negociação:

Neste exemplo, a sessão deve desligar após dois minutos (120 segundos), que podem ser verificadas dentro a história da mensagem do AnyConnect:

> **Tip**: Para que o ASA responda a um cliente que esteja tentando reconectar, a sessão do Pai-túnel deve ainda existir no base de dados ASA. No caso do Failover, os DPD igualmente precisam de ser permitidos para que o comportamento da reconexão trabalhe.

Como é visível dos mensagens anteriores, a reconexão falhada. Contudo, se a reconexão é bem sucedida, é aqui o que acontece:

1. O Pai-túnel permanece o mesmo; isto não é renegociado porque este túnel mantém o token da sessão que é exigido para a sessão a fim reconectar.
2. As sessões novas SSL e DTL são geradas, e as portas de origem diferentes são usadas na reconexão.
3. Todos os valores de idle timeout são restaurados.
4. O timeout por inatividade é restaurado.

> **Caution**: Esteja ciente da identificação de bug Cisco CSCtg33110. O base de dados da sessão de VPN não atualiza o endereço IP público no base de dados da sessão ASA quando AnyConnect reconecta.

Nesta situação onde as tentativas de reconectar a falha, você encontram esta mensagem:

> **Note**: Esta requisição de aprimoramento foi arquivada a fim fazer este mais granulado: Identificação de bug Cisco CSCsl52873 - O ASA não tem um intervalo desligado

configurável para AnyConnect.

O comportamento do cliente de AnyConnect em caso do sistema suspende

Há uma característica vagueando que permita que AnyConnect reconecte depois que um sono PC. O cliente continua a tentar até a quietude ou os timeouts de sessão expiram e o cliente não rasga imediatamente para baixo o túnel quando o sistema entra em hiberna/apoio. Para os clientes que não querem esta característica, ajuste o timeout de sessão a um valor baixo a fim impedir o sono/resumo reconecta.

> **Note**: Depois que o reparo da identificação de bug Cisco CSCso17627 (versão 2.3(111)+), um botão de controle foi introduzido a fim desabilitar este reconecte na característica do resumo.

O comportamento da Auto-reconexão para AnyConnect pode ser controlado com o perfil de AnyConnect XML com este ajuste:

```
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
```

Com esta mudança, AnyConnect tentará reconectar quando o computador é trazido para trás do sono. Os padrões da preferência de AutoReconnectBehavior a DisconnectOnSuspend. Este comportamento é diferente daquele da versão cliente 2.2 de AnyConnect. Para reconecte após o resumo, o administrador de rede deve ajustar ReconnectAfterResume no perfil ou fazer usuário das preferências de AutoReconnect e de AutoReconnectBehavior verificável no perfil para permitir que os usuários ajustem-no.

Perguntas mais freqüentes

Q1. Anyconnect DPD não tem um intervalo mas nenhuma nova tentativa - quantos

pacotes tem que faltar antes que marque a extremidade remota como inoperante?

R. Tem que faltar três novas tentativas/quatro pacotes.

Q2. É o processamento DPD diferente para AnyConnect com IKEv2?

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

Q3. Há uma outra finalidade para o Pai-túnel de AnyConnect?

A. Além do que ser um mapeamento no ASA, o túnel do pai é usado a fim empurrar upgrades da imagem de AnyConnect do ASA para o cliente, porque o cliente não é conectado ativamente durante o processo de upgrade.

Q4. Pode você filtrar e terminar apenas sessões inativas?

R. Você pode filtrar sessões inativas com o comando **inativo do filtro do anyconnect da mostra VPN-sessiondb**. Contudo, não há nenhum comando terminar apenas sessões inativas. Em lugar de, você precisa de terminar sessões específicas ou de terminar todas as sessões pelo usuário (deslocamento predeterminado - nome), o protocolo, ou o grupo de túneis. Uma requisição de aprimoramento, a identificação de bug Cisco CSCuh55707, foi arquivada a fim adicionar a opção para terminar apenas as sessões inativas.

Q5. Que acontece ao Pai-túnel quando o Quietude-intervalo dos túneis DTL ou TLS expira?

R. A “quietude” ao temporizador esquerdo da sessão do AnyConnect-pai é restaurada depois que o SSL-túnel ou o DTL-túnel são rasgados para baixo. Isto permite que o “quietude-intervalo” atue como “desligou” o intervalo. Este transforma-se eficazmente o momento permissível para que o cliente reconecte. Se o cliente não reconecta dentro do temporizador, a seguir o Pai-túnel estará terminado.

Q6. Que são o ponto de manter a sessão uma vez que os temporizadores DPD desligaram a sessão e porque o ASA não liberam o endereço IP de Um ou Mais Servidores Cisco ICM NT?

R. A extremidade principal não tem nenhum conhecimento do estado de cliente. Neste caso, as esperas ASA para que o cliente reconecte esperançosamente até o tempo de sessão para fora em cima do temporizador de ociosidade. O DPD não mata uma sessão de AnyConnect; mata meramente o túnel (dentro dessa sessão) de modo que o cliente possa restabelecer o túnel. Se o cliente não restabelece um túnel, a sessão permanece até que o temporizador de ociosidade expire.

Se o interesse é sobre as sessões que estão sendo usadas acima, ajuste simultâneo-inícios de uma sessão a um valor baixo tal como um. Com este ajuste, usuários que têm uma sessão no

base de dados da sessão ter sua sessão prévia suprimida quando entrarem outra vez.

Q7. Que é o comportamento se o ASA falha sobre de ativo ao apoio?

R. Inicialmente, quando a sessão é estabelecida, os três túneis (pai, SSL, e DTL) replicated à unidade em standby; uma vez que o ASA falha sobre, os DTL e as sessões TLS estão restabelecidos porque não são sincronizados à unidade em standby, mas todos os dados correm através dos túneis devem trabalhar sem rompimento depois que a sessão de AnyConnect é restabelecida.

As sessões SSL/DTLS não são stateful, assim que o estado e o número de sequência SSL não são mantidos e podem bastante taxar. Assim, aquelas sessões precisam de ser restabelecidas a partir do zero, que é feito com a sessão do pai e o token da sessão.

> **Tip**: No caso de um evento do Failover, as sessões de cliente VPN SSL não estão transferidas ao dispositivo à espera se o Keepalives é desabilitado.

Q8. Por que há dois intervalos diferentes, o idle timeout e o intervalo desligado, se são ambo o mesmo valor?

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

- Idle timeout - O idle timeout está para quando nenhum dados é passado sobre uma conexão.
- Intervalo desligado - O intervalo desligado está para quando você dá acima a sessão de VPN porque a conexão esteve perdida e não pode ser restabelecida.

O intervalo desligado foi executado nunca no ASA. Em lugar de, o ASA envia o valor de idle timeout para a quietude e intervalos desligado ao cliente.

O cliente não usa o idle timeout, porque o ASA segura o idle timeout. O cliente usa o valor de timeout desligado, que é o mesmo que o valor de idle timeout, a fim saber quando dar acima reconecta tentativas desde que o ASA terá deixado cair a sessão.

Quando conectado não ativamente ao cliente, o ASA intervalo a sessão através do idle timeout. A razão principal não executar o intervalo desligado no ASA era evitar a adição de um outro temporizador para cada sessão de VPN e o aumento nas despesas gerais no ASA (embora o mesmo temporizador poderia ser usado em ambos os exemplos, apenas com valores de timeout diferentes, desde que os dois casos são mutuamente exclusivos).

O único de valor acrescentado com o intervalo desligado é permitir que um administrador especifique um intervalo diferente para quando o cliente não é conectado ativamente contra a quietude. Como notável mais cedo, a identificação de bug Cisco CSCsl52873 foi arquivada para esta.

Q9. Que acontece quando a máquina cliente é suspendida?

A. À revelia, AnyConnect tenta restabelecer uma conexão de VPN quando você perde a Conectividade. Não tenta restabelecer uma conexão de VPN depois que um sistema recomeça à

revelia. Refira o cliente que de AnyConnect o comportamento em caso do sistema suspende para detalhes.

Q10. Quando uma reconexão acontece, o adaptador virtual de AnyConnect bate ou faz a alteração de tabela de roteamento de todo?

R. Um túnel-nível reconecta não fará tampouco. Esta é uma reconexão apenas no SSL ou nos DTL. Estes vão aproximadamente 30 segundos antes que deem acima. Se os DTL falham, está deixada cair apenas. Se o SSL falha, causa um sessão-nível reconecta. Um sessão-nível reconecta refará completamente o roteamento. Se o endereço de cliente atribuído na reconexão, ou nenhuns outros parâmetros de configuração que impactam o adaptador virtual (VA), não mudaram, a seguir o VA não está desabilitado. Quando for improvável ter toda a mudança nos parâmetros de configuração recebidos do ASA, é possível que uma mudança na interface física usada para a conexão de VPN (por exemplo, se você retira e vai do prendido a WiFi) poderia conduzir a um valor diferente da unidade de transmissão máxima (MTU) para a conexão de VPN. O valor MTU impacta o VA, e uma mudança a ela faz com que o VA seja desabilitado e re-permitido então.

Q11. Faz? O automóvel reconecta? forneça a Persistência de sessão? Em caso afirmativo, há alguma funcionalidade extra adicionada no cliente de AnyConnect?

A. AnyConnect não fornece nenhuma “mágica extra” para acomodar a Persistência de sessão para aplicativos. Mas a conectividade de VPN está restaurada automaticamente shortly after a conectividade de rede ao gateway seguro recomeça, desde que os idle e session timeout configurados no ASA não expiraram. E ao contrário do cliente de IPSec, o automáticos reconectam resultados no mesmo endereço IP cliente. Quando AnyConnect tentar reconectar, o adaptador virtual de AnyConnect permanece permitido e no estado conectado, assim que o endereço IP cliente permanece presente e permitido no PC cliente o tempo inteiro, que dá a persistência do endereço IP cliente. Os aplicativos do PC cliente, contudo, provavelmente ainda perceberão a perda de conectividade a seus server na rede de empreendimento se tomar demasiado por muito tempo para que a conectividade de VPN seja restaurada.

Q12. Esta característica trabalha em todas as variações de Microsoft Windows (vista de 32 bits & 64-bit, XP). Como sobre Macintosh? Trabalha no OS X 10.4?

R. Esta característica trabalha no Mac e no Linux. Houve umas edições com Mac e Linux, mas as melhorias recentes foram feitas, particularmente para o Mac. Linux ainda exige algum suporte adicional (CSCsr16670, CSCsm69213), mas a funcionalidade básica está lá também. A propósito de Linux, AnyConnect não reconhecerá que uma suspensão/resumo (sono/vigília) ocorreu. Isto tem basicamente dois impactos:

- O perfil/configuração de preferências de AutoReconnectBehavior não pode ser apoiado em Linux sem suspende/apoio do resumo, assim que uma reconexão ocorrerá sempre depois que suspenda/resumo.
- Em Microsoft Windows e em Macintosh, reconecta são executados imediatamente na sessão em nível após o resumo, que permite um interruptor mais rápido a uma interface física diferente. Em Linux, porque AnyConnect é completamente inconsciente da suspensão/resumo, reconecta ocorrerá no túnel-nível primeiramente (SSL e DTL) e isto pôde

significar que reconecta a tomada levemente mais por muito tempo. Mas reconecta ainda ocorrerá em Linux.

Q13. Há alguma limitação à característica em termos da Conectividade (prendida, Wi-fi, 3G e assim por diante)? Apoia a transição de um modo a outro (do Wi-fi a 3G, a 3G ao prendido, e assim por diante)?

A. AnyConnect não é amarrado a uma interface física particular para a vida da conexão de VPN. Se a interface física usada para a conexão de VPN está perdida ou se reconecte as tentativas sobre ela excedem um determinado ponto inicial da falha, a seguir AnyConnect já não usará essa relação e para tentar alcançar o gateway seguro com o que relações estão disponíveis até a quietude ou os temporizadores de sessão expire. Note que uma mudança na interface física poderia conduzir a um valor diferente MTU para o VA, que fará com que o VA tenha que ser desabilitado e re-permitido, mas ainda com o mesmo endereço IP cliente.

Se há algum rompimento de rede (relação para baixo, redes mudadas, relações mudadas), AnyConnect tentará reconectar; nenhuma reautenticação é precisada sobre de reconectar. Isto aplica-se mesmo a um interruptor das interfaces física:

Exemplo:

```
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
```

Q14. Como a operação do resumo é autenticada?

R. Em um resumo, você submete novamente o token autenticado que permanecerá para a vida da sessão, e a sessão é restabelecida então.

Q15. A autorização LDAP é executada igualmente em cima reconecta ou somente a autenticação?

R. Isto é executado somente na conexão inicial.

Q16. O pre-início de uma sessão e/ou a corrida hostscan em cima recomeçam?

R. Não, estes executados na conexão inicial somente. Qualquer outra coisa semelhante slated para a característica periódica futura da avaliação da postura.

Q17. No que diz respeito ao Balanceamento de carga VPN (LB) e ao resumo da conexão, o cliente conectará para trás diretamente ao membro de grânulos que foi conectado a antes?

R: Sim, isto está correto desde que você não faz re-resolução o hostname através do DNS para re-estblishment de uma sessão existente.

Informações Relacionadas

- Referência ASA DPD: Identificação de bug Cisco CSCsr63074 - DPD não enviado quando o par for inoperante & túnel não inativo em s2s com 7.2.4
- Suporte Técnico e Documentação - Cisco Systems