Answer AnyConnect FAQ - 터널, DPD 및 비활성 타이머

목차

소개

이 문서에서는 Cisco AnyConnect Secure Mobility Client 터널, 재연결 동작 및 DPD(Dead Peer Detection), 비활성 타이머에 대해 설명합니다.

배경 정보

터널 유형

AnyConnect 세션을 연결하는 데 사용되는 두 가지 방법이 있습니다.

- 포털을 통해(클라이언트리스)
- 독립형 애플리케이션을 통해

연결 방법에 따라 Cisco ASA(Adaptive Security Appliance)에서 각각 특정 목적을 가진 세 개의 서로 다른 터널(세션)을 생성합니다.

1. 클라이언트리스 또는 상위 터널: 네트워크 연결 문제 또는 최대 절전 모드로 인해 다시 연결해야 하는 경우 필요한 세션 토큰을 설정하기 위해 협상에 생성되는 기본 세션입니다. 연결 메커니즘에 따라 ASA는 세션을 클라이언트리스(포털을 통한 Weblaunch) 또는 상위(독립형 AnyConnect)로 나열합니다.

   참고: AnyConnect-Parent는 클라이언트가 능동적으로 연결되지 않은 세션을 나타냅니다. 사실상 특정 클라이언트의 연결에 매핑되는 ASA의 데이터베이스 항목이라는 점에서 쿠키와 유사하게 작동합니다. 클라이언트가 절전/절전 모드로 전환되면 터널(IPsec/IKE(Internet Key Exchange)/TLS(Transport Layer Security)/DTLS(Datagram Transport Layer Security) 프로토콜)이 해제되지만 유휴 타이머 또는 최대 연결 시간이 적용될 때까지 상위 항목은 유지됩니다. 이를 통해 사용자는 재인증 없이 다시 연결할 수 있습니다.

2. SSL(Secure Sockets Layer)-Tunnel: SSL 연결이 먼저 설정되고, DTLS 연결을 설정하는 동안 데이터가 이 연결을 통해 전달됩니다. DTLS 연결이 설정되면 클라이언트는 SSL 연결이 아닌 DTLS 연결을 통해 패킷을 전송합니다. 반면 제어 패킷은 항상 SSL 연결을 통해 전달됩니다.

3. DTLS-Tunnel(DTLS 터널): DTLS 터널이 완전히 설정되면 모든 데이터가 DTLS 터널로 이동하며 SSL 터널은 가끔 제어 채널 트래픽에만 사용됩니다. UDP(User Datagram Protocol)에 문제가 발생하면 DTLS 터널이 해제되고 모든 데이터가 SSL 터널을 다시 통과합니다.

ASA의 샘플 출력

다음은 두 가지 연결 방법의 샘플 출력입니다.

웹 런칭을 통해 연결된 AnyConnect:

```
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
```

독립형 애플리케이션을 통해 연결된 AnyConnect:

```
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 및 비활성 타이머

세션이 비활성 세션으로 간주되는 경우는 언제입니까?

SSL-Tunnel이 세션에 더 이상 존재하지 않는 경우에만 세션이 비활성(타이머가 증가하기 시작)으로 간주됩니다. 따라서 각 세션은 SSL-Tunnel 삭제 시간으로 타임스탬프가 찍힙니다.

```
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
```

ASA에서 SSL 터널을 삭제하는 시점은 언제입니까?

SSL-Tunnel의 연결을 끊는 방법에는 두 가지가 있습니다.

1. **DPD** - DPD는 AnyConnect 클라이언트와 ASA 헤드엔드 간의 통신 실패를 탐지하기 위해 클라이언트에서 사용합니다. DPD는 ASA에서 리소스를 정리하기 위해 사용됩니다. 이렇게 하면 엔드포인트가 DPD ping에 응답하지 않는 경우 헤드엔드에서 데이터베이스의 연결을 유지하지 않습니다. ASA가 엔드포인트에 DPD를 전송하고 응답하면 아무 작업도 수행되지 않습니다. 엔드포인트가 응답하지 않으면 최대 재전송 횟수(IKEv1 또는 IKEv2가 사용되는지 여부에 따라 다름) 이후에 ASA가 세션 데이터베이스의 터널을 해제하고 세션을 "Waiting to Resume" 모드로 이동합니다. 즉, 헤드엔드의 DPD가 시작되었고 헤드엔드가 더 이상 클라이언트와 통신하지 않습니다. 이러한 경우 ASA는 사용자가 네트워크를 로밍하고 절전 모드로 전환하여 세션을 복구할 수 있도록 상위 터널을 유지합니다. 이러한 세션은 활성 연결 세션에 대해 계산되며 다음 조건에서 지워집니다.
   사용자 유휴 시간 제한클라이언트가 원래 세션을 다시 시작하고 올바르게 로그아웃합니다.
   DPD를 구성하려면 **anyconnect dpd-interval** 그룹 정책 설정의 WebVPN 특성 아래에 있는 명령입니다. 기본적으로 DPD는 활성화되어 있으며 ASA(게이트웨이) 및 클라이언트 모두에 대해 30초로 설정됩니다.

   주의: Cisco 버그 ID CSCts66926에 유의하십시오 - 클라이언트 연결이 끊긴 후 DPD가 DTLS 터널을 종료하지 못합니다.

2. **Idle-Timeout** - SSL 터널의 연결을 끊는 두 번째 방법은 이 터널의 Idle-Timeout이 만료되는 것입니다. 그러나 유휴 상태가 되어야 하는 것은 SSL 터널뿐만이 아니라 DTLS 터널입니다. DTLS 세션이 시간 초과되지 않는 한 SSL-Tunnel은 데이터베이스에 유지됩니다.

DPD가 이미 활성화된 경우 Keepalive를 활성화해야 하는 이유는 무엇입니까?

앞에서 설명한 것처럼 DPD는 AnyConnect 세션 자체를 종료하지 않습니다. 클라이언트가 터널을

재설정할 수 있도록 해당 세션 내에서 터널을 중단하기만 합니다. 클라이언트가 터널을 다시 설정할 수 없는 경우 ASA에서 유휴 타이머가 만료될 때까지 세션이 유지됩니다. DPD는 기본적으로 활성화되므로 NAT(Network Address Translation), 방화벽 및 프록시 장치를 사용하는 한쪽 방향으로 흐름이 닫혀 클라이언트가 종종 연결이 끊어질 수 있습니다. 20초와 같은 낮은 간격에서 킵얼라이브를 활성화하면 이를 방지하는 데 도움이 됩니다.

Keepalive는 특정 그룹 정책의 WebVPN 특성에서 **anyconnect ssl keepalive** 명령을 실행합니다. 기본적으로 타이머는 20초로 설정됩니다.

재연결 시 AnyConnect 클라이언트 동작

AnyConnect는 연결이 중단될 경우 재연결을 시도합니다. 자동으로 구성할 수 없습니다. ASA의 VPN 세션이 여전히 유효하고 AnyConnect에서 물리적 연결을 다시 설정할 수 있는 경우 VPN 세션이 다시 시작됩니다.

다시 연결 기능은 세션 시간 초과 또는 연결 끊기 시간 초과(실제로 유휴 시간 초과)가 만료될 때까지(또는 시간 초과가 구성되지 않은 경우 30분) 계속됩니다. 이러한 세션이 만료되면 ASA에서 VPN 세션이 이미 삭제되었기 때문에 클라이언트를 계속할 수 없습니다. 클라이언트는 ASA에 VPN 세션이 여전히 있다고 생각하는 한 계속 진행합니다.

AnyConnect는 네트워크 인터페이스가 어떻게 변경되더라도 재연결됩니다. NIC(Network Interface Card)의 IP 주소가 변경되거나 한 NIC에서 다른 NIC로(무선 또는 유선) 연결이 전환되어도 상관없습니다.

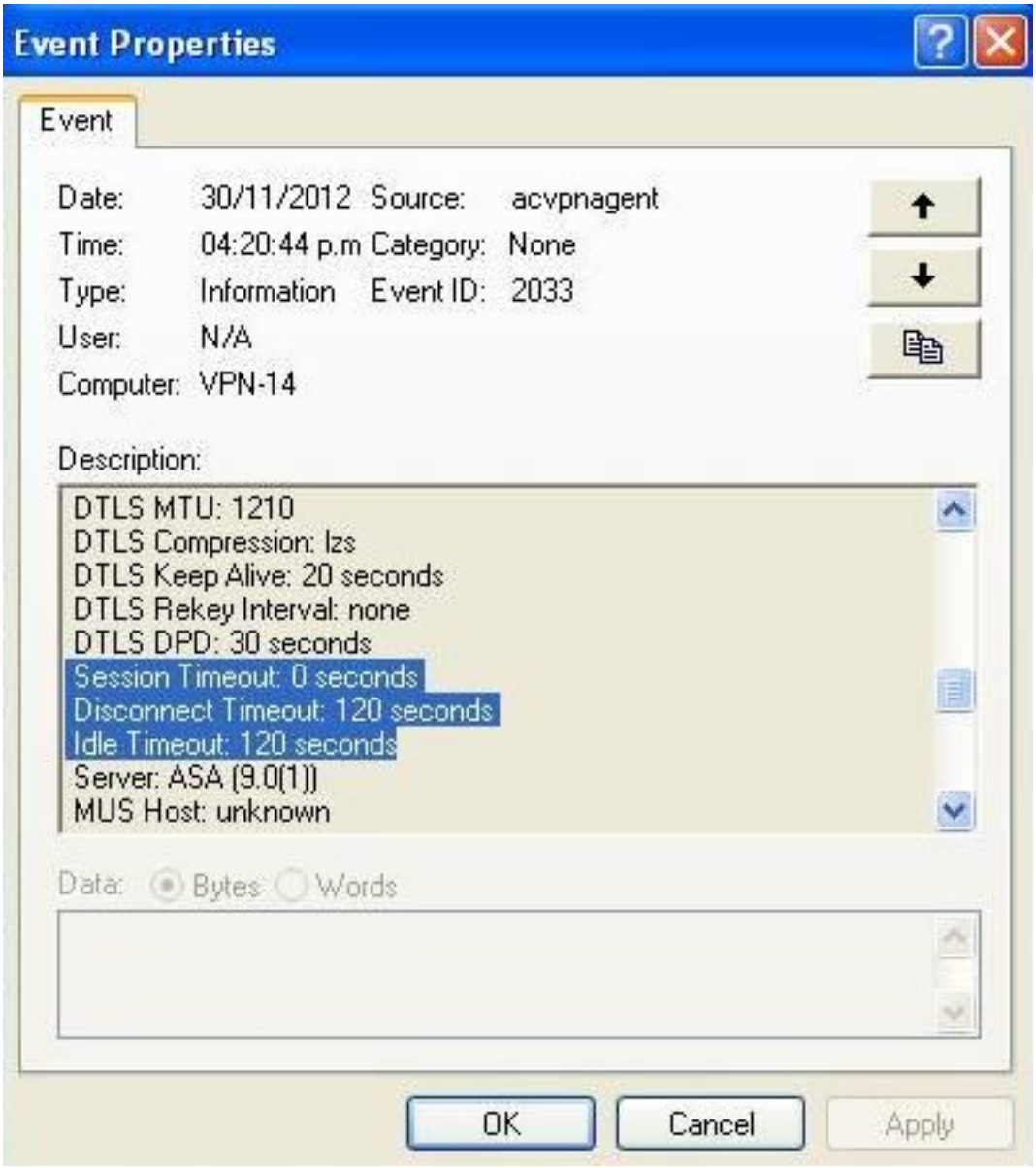
AnyConnect에 대한 재연결 프로세스를 고려하는 경우, 반드시 기억해야 할 세 가지 세션 레벨이 있습니다. 또한 이러한 각 세션의 재연결 동작은 느슨하게 결합되어 이전 레이어의 세션 요소에 의존하지 않고 재설정할 수 있습니다.

1. TCP 또는 UDP 다시 연결 [OSI 레이어 3]
2. TLS, DTLS 또는 IPSec(IKE+ESP) [OSI Layer 4] - TLS 재개는 지원되지 않습니다.
3. VPN [OSI 레이어 7] - VPN 세션 토큰은 보안 채널을 통해 중단 시 VPN 세션을 재설정하기 위해 인증 토큰으로 사용됩니다. 이는 Kerberos 토큰 또는 클라이언트 인증서가 인증에 사용되는 방법과 개념상 매우 유사한 독점 메커니즘입니다. 토큰은 헤드엔드에서 고유하며 암호로 생성됩니다. 헤드엔드는 세션 ID와 암호로 생성되는 랜덤 페이로드를 포함합니다. 헤드엔드에 대한 보안 채널이 설정된 후 초기 VPN 설정의 일부로 클라이언트에 전달됩니다. 헤드엔드에서 세션 수명 동안 유효하며 특별 권한 프로세스인 클라이언트 메모리에 저장됩니다.
   팁: 이 ASA 릴리스 이상에는 더 강력한 암호화 세션 토큰이 포함되어 있습니다. 9.1(3) 및 8.4(7.1)

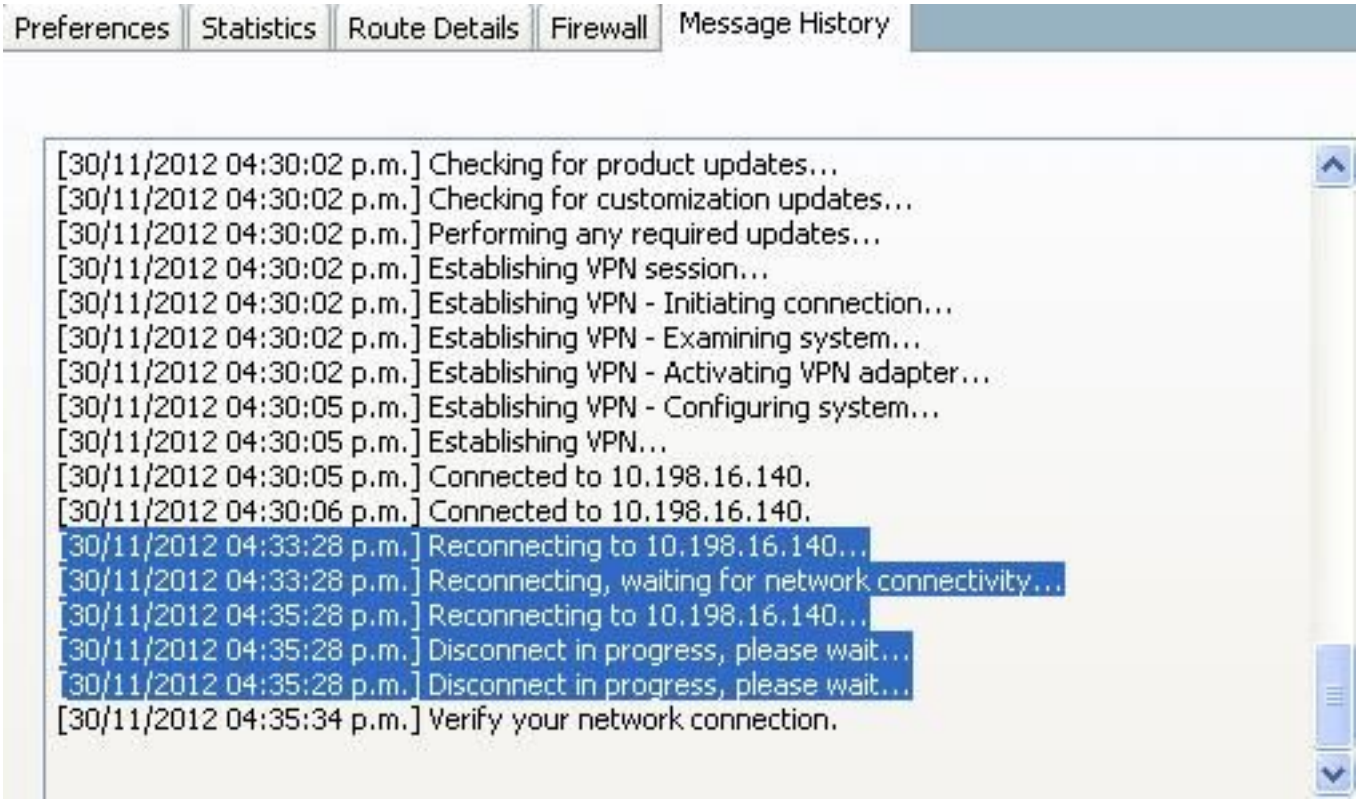
실제 프로세스

네트워크 연결이 중단되는 즉시 연결 끊기 시간 초과 타이머가 시작됩니다. 이 타이머가 만료되지 않는 한 AnyConnect 클라이언트는 계속 재연결을 시도합니다. 연결 끊기 시간 제한은 그룹 정책 유휴 시간 제한 또는 **최대 연결 시간** 중 가장 낮은 **설정으로 설정됩니다**.

이 타이머의 값은 협상의 AnyConnect 세션에 대한 이벤트 뷰어에 표시됩니다.



이 예에서 세션은 2분(120초) 후에 연결이 끊기며, 이는 AnyConnect의 Message History(메시지 기록)에서 확인할 수 있습니다.



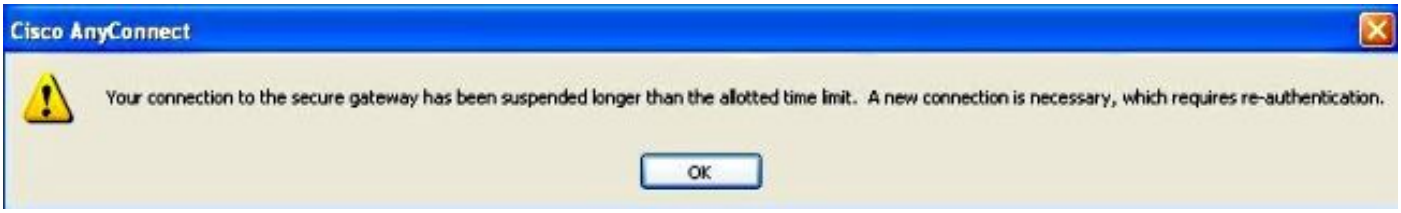
팁: ASA가 재연결을 시도하는 클라이언트에 응답하려면 ASA 데이터베이스에 상위 터널 세션이 여전히 존재해야 합니다. 장애 조치 시 재연결 동작이 작동하려면 DPD도 활성화해야 합니다.

이전 메시지에서 볼 수 있듯이 다시 연결하지 못했습니다. 그러나 재연결에 성공하면 다음과 같은 결과가 발생합니다.

1. Parent-Tunnel은 동일하게 유지됩니다. 이 터널은 재연결을 위해 세션에 필요한 세션 토큰을 유지 관리하므로 재협상되지 않습니다.
2. 새 SSL 및 DTLS 세션이 생성되고, 재연결에서 서로 다른 소스 포트가 사용됩니다.
3. 모든 Idle-Timeout 값이 복원됩니다.
4. Inactivity Timeout이 복원됩니다.

주의: Cisco 버그 ID CSCtg33110에 유의하십시오. AnyConnect가 다시 연결될 때 VPN 세션 데이터베이스는 ASA 세션 데이터베이스의 공용 IP 주소를 업데이트하지 않습니다.

에서 재연결 시도가 실패한 경우 다음과 같은 메시지가 표시됩니다.



참고: Cisco 버그 ID CSCsl52873 - ASA에서 AnyConnect에 대해 구성 가능한 연결 끊김 시간 제한을 설정하지 않기 위해 이 개선 요청이 제출되었습니다.

시스템 일시 중단 시 AnyConnect 클라이언트 동작

PC 절전 모드 후 AnyConnect에서 다시 연결할 수 있는 로밍 기능이 있습니다. 클라이언트는 유휴 또는 세션 시간 제한이 만료될 때까지 계속 시도하며 시스템이 최대 절전 모드/대기 모드로 전환될 때 클라이언트가 터널을 즉시 해제하지 않습니다. 이 기능을 원하지 않는 사용자의 경우 절전/다시 연결을 방지하기 위해 세션 시간 초과를 낮은 값으로 설정합니다.

> **참고**: Cisco 버그 ID CSCso17627(버전 2.3(111)+)을 수정한 후 이 재시작 기능을 비활성화하기 위해 제어 노브가 도입되었습니다.

AnyConnect에 대한 자동 재연결 동작은 AnyConnect XML 프로파일을 통해 다음 설정으로 제어할 수 있습니다.

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

이 변경 사항으로 AnyConnect는 컴퓨터가 절전 모드에서 다시 돌아올 때 다시 연결을 시도합니다. AutoReconnectBehavior 기본 설정은 기본적으로 DisconnectOnSuspend입니다. 이 동작은 AnyConnect 클라이언트 릴리스 2.2와 다릅니다. 다시 시작한 후 다시 연결하려면 네트워크 관리자가 프로필에서 ReconnectAfterResume을 설정하거나 사용자가 설정할 수 있도록 프로필에서 AutoReconnect 및 AutoReconnectBehavior 기본 설정을 사용자가 제어할 수 있도록 해야 합니다.

자주 묻는 질문(FAQ)

1분기 Anyconnect DPD에는 간격이 있지만 재시도가 없습니다. 원격 끝을 Dead로 표시하기 전에 몇 개의 패킷을 누락해야 합니까?

A. 클라이언트 관점에서 DPD는 터널 설정 단계에서 터널을 분리할 뿐입니다. 클라이언트가 터널 설정 단계에서 세 번의 재시도(패킷 4개 전송)를 경험하고 기본 VPN 서버에서 응답을 받지 못하면, 구성된 백업 서버 중 하나를 사용하는 것으로 돌아갑니다. 그러나 터널이 설정되면 클라이언트 관점에서 누락된 DPD는 터널에 영향을 주지 않습니다. DPD가 VPN 서버에 미치는 실제 영향은 DPDs and Inactivity Timers 섹션에서 설명한 것과 같습니다.

2분기 DPD 프로세스는 IKEv2를 사용하는 AnyConnect와 다릅니까?

A. 예, IKEv2는 재시도 횟수가 고정되어 있습니다(재시도 횟수 6회/패킷 7회).

3분기 AnyConnect 상위 터널에 다른 목적이 있습니까?

A. ASA에서 매핑하는 것 외에도, 상위 터널은 업그레이드 프로세스 중에 클라이언트가 능동적으로 연결되지 않으므로 ASA에서 클라이언트로 AnyConnect 이미지 업그레이드를 푸시하기 위해 사용됩니다.

4분기 비활성 세션만 필터링하고 로그오프할 수 있습니까?

A. show vpn-sessiondb anyconnect filter inactive **명령을 사용하여 비활성 세션을 필터링할** 수 있습니다. 그러나 비활성 세션만 로그오프하는 명령은 없습니다. 대신 특정 세션을 로그오프하거나 사용자(인덱스 - 이름), 프로토콜 또는 터널 그룹당 모든 세션을 로그오프해야 합니다. 비활성 세션만 로그오프하는 옵션을 추가하기 위해 개선 요청인 Cisco 버그 ID CSCuh55707이 제출되었습니다.

5분기 DTLS 또는 TLS 터널의 유휴 시간 제한이 만료되면 상위 터널은 어떻게 됩니까?

A. SSL-Tunnel 또는 DTLS-Tunnel이 해제된 후 AnyConnect-Parent 세션의 "Idle TO Left" 타이머가 재설정됩니다. 이렇게 하면 "idle-timeout"이 "disconnected" 시간 제한으로 작동할 수 있습니다. 이렇게 하면 클라이언트가 다시 연결할 수 있는 시간이 됩니다. 클라이언트가 타이머 내에 재연결하지 않으면 Parent-Tunnel이 종료됩니다.

Q6. DPD 타이머의 세션 연결이 끊겼을 때 세션을 유지하는 이유와 ASA에서 IP 주소를 해제하지 않는 이유는 무엇입니까?

A. 헤드엔드는 고객의 상태를 알지 못합니다. 이 경우 ASA는 유휴 타이머에 세션이 시간 초과될 때까지 클라이언트가 다시 연결되기를 기다립니다. DPD는 AnyConnect 세션을 종료하지 않습니다. 클라이언트가 터널을 재설정할 수 있도록 터널(해당 세션 내)을 중단합니다. 클라이언트가 터널을 재설정하지 않으면 유휴 타이머가 만료될 때까지 세션이 유지됩니다.

사용 중인 세션에 대한 문제인 경우 동시 로그인을 1과 같은 낮은 값으로 설정합니다. 이 설정을 사용하면 세션 데이터베이스에 세션이 있는 사용자가 다시 로그인할 때 이전 세션이 삭제됩니다.

Q7 ASA가 Active에서 Standby로 장애 조치될 경우 어떻게 됩니까?

A. 처음에 세션이 설정되면 3개의 터널(상위, SSL 및 DTLS)이 스탠바이 유닛에 복제됩니다. ASA가 장애 조치되면 DTLS 및 TLS 세션이 스탠바이 유닛에 동기화되지 않으므로 재설정되지만 AnyConnect 세션이 재설정된 후에는 터널을 통과하는 데이터 흐름이 중단 없이 작동해야 합니다.

SSL/DTLS 세션은 상태 저장 세션이 아니므로 SSL 상태 및 시퀀스 번호가 유지되지 않으며 상당한 부담으로 작용할 수 있습니다. 따라서 이러한 세션은 처음부터 다시 설정해야 합니다. 이 작업은 상위 세션 및 세션 토큰으로 수행됩니다.

> **팁**: 장애 조치 이벤트의 경우 keepalive가 비활성화된 경우 SSL VPN 클라이언트 세션이 대기 디바이스로 전달되지 않습니다.

8분기 유휴 시간 제한과 연결이 끊긴 시간 제한의 두 가지 시간 제한이 같은 경우, 그 이유는 무엇입니까?

A. 프로토콜이 개발되었을 때 다음 두 가지 시간 제한이 제공되었습니다.

- Idle timeout - 유휴 시간 제한은 어떤 데이터도 연결을 통해 전달되지 않는 경우에 사용됩니다.
- Disconnected timeout(연결 끊김 시간 제한) - 연결 끊김 시간 제한은 연결이 끊어져 다시 설정할 수 없기 때문에 VPN 세션을 포기할 때 사용합니다.

연결이 끊긴 시간 제한은 ASA에서 구현되지 않았습니다. 대신 ASA는 유휴 시간 제한 및 연결 해제된 시간 제한 모두에 대한 유휴 시간 제한 값을 클라이언트에 전송합니다.

ASA에서 유휴 시간 제한을 처리하므로 클라이언트는 유휴 시간 제한을 사용하지 않습니다. 클라이언트는 ASA에서 세션을 삭제했기 때문에 재연결 시도를 중단할 시기를 파악하기 위해 유휴 시간 제한 값과 동일한 연결 해제된 시간 제한 값을 사용합니다.

클라이언트에 능동적으로 연결되지 않은 동안에는 ASA가 유휴 시간 제한을 통해 세션을 시간 초과합니다. ASA에서 연결이 끊긴 시간 제한을 구현하지 않는 주된 이유는 모든 VPN 세션에 다른 타이

머가 추가되고 ASA에서 오버헤드가 증가하는 것을 방지하기 위해서입니다(두 사례는 상호 배타적이므로 시간 제한 값이 서로 다른 두 인스턴스에서 동일한 타이머를 사용할 수 있지만).

연결이 끊긴 시간 제한과 함께 추가되는 유일한 값은 클라이언트가 활성 상태가 아닌 경우와 유휴 상태가 아닌 경우에 대해 관리자가 다른 시간 제한을 지정할 수 있도록 허용하는 것입니다. 앞서 언급한 바와 같이, Cisco 버그 ID CSCsl52873이 이에 대해 접수되었습니다.

Q9 클라이언트 머신이 일시 중단되면 어떻게 됩니까?

A. 기본적으로 AnyConnect는 연결이 끊어지면 VPN 연결을 다시 설정하려고 시도합니다. 기본적으로 시스템이 다시 시작된 후에는 VPN 연결을 다시 설정하려고 시도하지 않습니다. 자세한 내용은 시스템 일시 중단의 경우 AnyConnect 클라이언트 동작을 참조하십시오.

Q10. 재연결이 발생하면 AnyConnect 가상 어댑터가 플랩 상태입니까, 아니면 라우팅 테이블이 전혀 변경됩니까?

A. 터널 레벨 재연결도 작동하지 않습니다. 이는 SSL 또는 DTLS에 대한 재연결입니다. 이들은 약 30초 후에 포기하게 됩니다. DTLS가 실패하면 삭제됩니다. SSL이 실패하면 세션 레벨의 재연결이 발생합니다. 세션 레벨 재연결은 라우팅을 완전히 재실행합니다. 재연결 시 할당된 클라이언트 주소 또는 VA(가상 어댑터)에 영향을 주는 다른 컨피그레이션 매개변수가 변경되지 않은 경우 VA는 비활성화되지 않습니다. ASA에서 받은 컨피그레이션 매개변수는 변경되지 않을 수 있지만, VPN 연결에 사용되는 물리적 인터페이스의 변경(예: 도킹을 해제하고 유선에서 WiFi로 전환하는 경우)은 VPN 연결에 대해 다른 MTU(Maximum Transmission Unit) 값을 가져올 수 있습니다. MTU 값은 VA에 영향을 미치며, 이 값이 변경되면 VA가 비활성화되었다가 다시 활성화됩니다.

질문 11. "Auto Reconnect(자동 재연결)"가 세션 지속성을 제공합니까? 그렇다면 AnyConnect 클라이언트에 추가된 추가 기능이 있습니까?

A. AnyConnect는 애플리케이션의 세션 지속성을 수용하기 위한 추가적인 "매직"을 제공하지 않습니다. 그러나 VPN 연결은 보안 게이트웨이에 대한 네트워크 연결이 재개된 직후 자동으로 복원됩니다. 단, ASA에 구성된 유휴 시간 및 세션 시간 초과가 만료되지 않았습니다. 그리고 IPsec 클라이언트와 달리 자동 재연결은 동일한 클라이언트 IP 주소를 초래합니다. AnyConnect가 재연결을 시도하는 동안 AnyConnect 가상 어댑터는 활성화 상태로 계속 연결되므로 클라이언트 IP 주소가 클라이언트 PC에서 항상 현재 상태로 유지되고 활성화되어 클라이언트 IP 주소가 지속됩니다. 그러나 클라이언트 PC 애플리케이션은 VPN 연결이 복원되는 데 시간이 너무 오래 걸리면 엔터프라이즈 네트워크에서 서버 연결이 끊어지는 것을 감지합니다.

Q12. 이 기능은 Microsoft Windows(Vista 32비트 및 64비트, XP)의 모든 변형에서 작동합니다. 매킨토시는 어때요? OS X 10.4에서 작동합니까?

A. 이 기능은 Mac 및 Linux에서 작동합니다. Mac과 Linux에 문제가 있었지만, 특히 Mac에 대해서는 최근 개선이 이루어졌습니다. Linux는 여전히 일부 추가 지원(Cisco 버그 ID CSCsr16670, Cisco 버그 ID CSCsm69213)이 필요하지만 기본 기능도 있습니다. Linux와 관련하여 AnyConnect는 일시 중단/재개(절전/절전 모드 해제)가 발생했음을 인식하지 못합니다. 이는 기본적으로 두 가지 영향을 미칩니다.

- 일시 중단/다시 시작 지원 없이 Linux에서는 AutoReconnectBehavior 프로필/기본 설정을 지원할 수 없으므로 일시 중단/다시 시작 후 항상 다시 연결됩니다.
- Microsoft Windows 및 Macintosh에서는 재시작 후 세션 레벨에서 즉시 재연결이 수행되므로 다른 물리적 인터페이스로 더 빠르게 전환할 수 있습니다. Linux에서는 AnyConnect가 일시 중

단/재시작을 전혀 인식하지 못하므로 재연결이 먼저 터널 레벨(SSL 및 DTLS)에서 이루어지므로 재연결이 약간 더 오래 걸릴 수 있습니다. 그러나 다시 연결은 여전히 Linux에서 발생합니다.

Q13. 연결(유선, wi-fi, 3G 등) 측면에서 기능에 제한이 있습니까? Wi-Fi에서 3G, 3G에서 유선 등의 모드 전환을 지원합니까?

A. AnyConnect는 VPN 연결 수명 동안 특정 물리적 인터페이스에 연결되지 않습니다. VPN 연결에 사용된 물리적 인터페이스가 손실되거나 이를 통한 재연결 시도가 특정 실패 임계값을 초과하는 경우, AnyConnect는 유휴 또는 세션 타이머가 만료될 때까지 해당 인터페이스를 더 이상 사용하지 않고 사용 가능한 어떤 인터페이스로도 보안 게이트웨이에 도달하려고 시도합니다. 물리적 인터페이스를 변경하면 VA의 MTU 값이 달라질 수 있으며, 이로 인해 VA를 비활성화하고 다시 활성화해야 하지만 여전히 동일한 클라이언트 IP 주소를 사용해야 합니다.

네트워크 중단(인터페이스 중단, 변경된 네트워크, 변경된 인터페이스)이 있는 경우 AnyConnect는 재연결을 시도합니다. 재연결 시 재인증은 필요하지 않습니다. 이는 물리적 인터페이스의 스위치에도 적용됩니다.

예:

```
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
```

Q14. 재개 작업은 어떻게 인증됩니까?

A. 재시작에서 세션 수명 동안 유지되는 인증된 토큰을 다시 제출하면 세션이 다시 설정됩니다.

Q15. LDAP 권한 부여는 재연결 시 수행됩니까 아니면 인증만 수행됩니까?

A. 이 작업은 초기 연결에서만 수행됩니다.

Q16. 재시작 시 사전 로그인 및/또는 hostscan이 실행됩니까?

A. 아니요. 이러한 작업은 초기 연결에서만 실행됩니다. 이와 같은 것이 향후 정기 상태 평가 기능을 위해 예정될 것이다.

Q17. VPN LB(Load Balancing) 및 연결 재개와 관련하여 클라이언트는 이전에 연결했던 클러스터 멤버에 다시 직접 연결합니까?

A: 예, 현재 세션을 재설정하기 위해 DNS를 통해 호스트 이름을 재확인하지 않으므로 이는 정확합니다.

관련 정보

- **ASA DPD Reference: Cisco 버그 ID CSCsr63074 - 피어가 데드일 때 DPD가 전송되지 않고 s2에서 7.2.4로 터널링하지 않음**
- **기술 지원 및 문서 – Cisco Systems**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.