AnyConnect 재연결로 인한 트래픽 흐름 중단 해결

목차

소개

이 문서에서는 AnyConnect 클라이언트가 ASA(Adaptive Security Appliance)에 1분 만에 다시 연결할 때 발생하는 상황에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이러한 제품은 다음과 같은 문제로 인해 영향을 받았습니다.

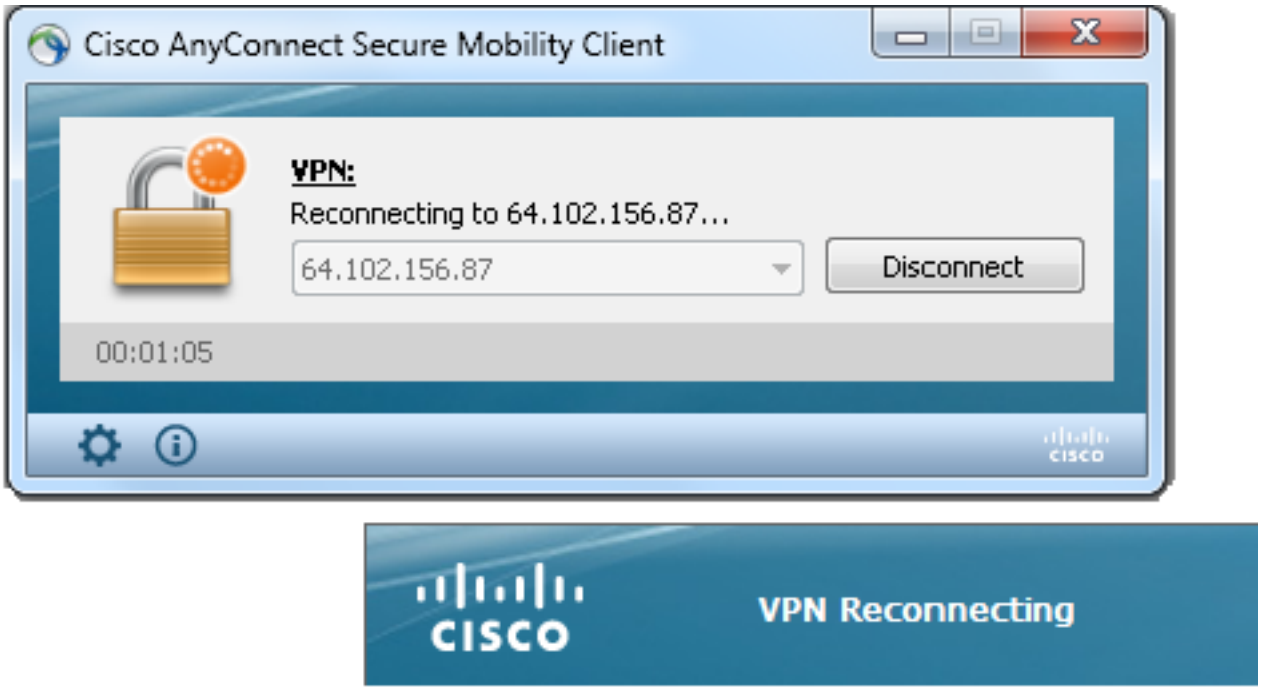
- ASA 릴리스 9.17
- AnyConnect 클라이언트 릴리스 4.10

배경 정보

AnyConnect 클라이언트가 정확히 1분 내에 ASA(Adaptive Security Appliance)에 다시 연결할 경우 사용자는 AnyConnect가 다시 연결될 때까지 TLS(Transport Layer Security) 터널을 통해 트래픽을 수신할 수 없습니다. 이는 이 문서에서 설명하는 몇 가지 다른 요소에 따라 달라집니다.

증상

이 예에서는 AnyConnect 클라이언트가 ASA에 다시 연결될 때 표시됩니다.



이 syslog는 ASA에 표시됩니다.

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

문제 설명

이러한 진단 및 Reporting 이 문제와 함께 툴(DART) 로그가 표시됨:

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

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.


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

원인

이 문제의 원인은 DTLS(데이터그램 전송 계층 보안) 터널을 구축하지 못했기 때문입니다. 이는 두 가지 이유 때문일 수 있습니다.

- DTLS가 경로 어딘가에서 차단됨
- 기본이 아닌 DTLS 포트 사용

DTLS가 경로 어딘가에서 차단됨

ASA Release 9.x 및 AnyConnect Release 4.x부터 클라이언트/ASA 간의 TLS/DTLS에 대해 협상되는 고유한 MTU(Maximum Transition Unit) 형식으로 최적화가 도입되었습니다. 이전에는 클라이언트가 TLS/DTLS를 모두 포함하는 대략적인 예상 MTU를 도출했으며, 이는 최적에 비해 매우 낮았습니다. 이제 ASA는 TLS/DTLS 모두에 대한 캡슐화 오버헤드를 계산하고 그에 따라 MTU 값을 파생합니다.

DTLS가 활성화된 경우 클라이언트는 최적의 성능을 보장하기 위해 VPN 어댑터(DTLS 터널이 설정되기 전에 활성화되며 경로/필터 시행에 필요한 어댑터)에서 DTLS MTU(이 경우 1418)를 적용합니다. DTLS 터널을 설정할 수 없거나 어느 시점에 터널이 삭제되면 클라이언트는 TLS로 장애 조치하고 VA(가상 어댑터)의 MTU를 TLS MTU 값으로 조정합니다(이 경우 세션 수준을 다시 연결해야 함).

해결

DTLS > TLS의 이 가시적인 전환을 없애기 위해 관리자는 DTLS 터널 설정에 문제가 있는 사용자(예: 방화벽 제한)를 위해 TLS 전용 액세스에 대해 별도의 터널 그룹을 구성할 수 있습니다.

1. 최상의 옵션은 AnyConnect MTU 값을 TLS MTU보다 낮게 설정한 다음 협상하는 것입니다.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect mtu 1300
   ```
   그러면 TLS 및 DTLS MTU 값이 같습니다. 이 경우에는 재연결이 표시되지 않습니다.
2. 두 번째 옵션은 단편화를 허용하는 것입니다.
   ```
   group-policy ac_users_group attributes
    webvpn
    anyconnect ssl df-bit-ignore enable
   ```
   조각화를 사용하면 크기가 MTU 값을 초과하는 큰 패킷을 조각화하여 TLS 터널을 통해 전송할 수 있습니다.
3. 세 번째 옵션은 여기에 표시된 MSS(Maximum Segment Size)를 1460으로 설정하는 것입니다.
   ```
   sysopt conn tcpmss 1460
   ```
   이 경우 TLS MTU는 DTLS MTU 1418(AES/SHA1/LZS)보다 큰 1427(RC4/SHA1)이 될 수 있습니다. 이렇게 하면 ASA에서 AnyConnect 클라이언트로의 TCP 문제가 해결되지만(MSS 덕분에), ASA에서 AnyConnect 클라이언트로의 대규모 UDP 트래픽은 AnyConnect 클라이언트 MTU 1418이 낮아 AnyConnect 클라이언트에서 삭제할 수 있으므로 문제가 발생할 수 있습니다. sysopt **conn tcpmss**가 수정되면 L2L(LAN-to-LAN) IPSec VPN 터널과 같은 다른 기능에 영향을 줄 수 있습니다.

워크플로 다시 연결

이러한 암호가 구성되었다고 가정합니다.

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

이 경우 다음과 같은 일련의 이벤트가 발생합니다.

- AnyConnect는 SSL 암호화로 AES256-SHA256을 사용하여 상위 터널 및 TLS 데이터 터널을 설정합니다.
- DTLS가 경로에서 차단되고 DTLS 터널을 설정할 수 없습니다.
- ASA는 AnyConnect에 대한 매개변수를 발표하며, 여기에는 두 개의 개별 값인 TLS 및 DTLS MTU 값이 포함됩니다.
- DTLS MTU는 기본적으로 1418입니다.
- TLS MTU는 sysopt conn tcpmss **값**에서 계산됩니다(기본값은 1380). TLS MTU가 파생되는 방법은 다음과 같습니다(debug webvpn anyconnect **출력에 표시됨**).

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

- AnyConnect는 VPN 어댑터를 가동하고 DTLS**를** 통해 연결할 수 있을 것으로 예상하여 DTLS MTU를 할당합니다.
- 이제 AnyConnect 클라이언트가 연결되고 사용자가 특정 웹 사이트로 이동합니다.
- 브라우저에서 TCP SYN을 전송하고 MSS = 1418-40 = 1378을 설정합니다.
- ASA 내부의 HTTP-server는 1418 크기의 패킷을 전송합니다.
- ASA는 DF(Do not Fragment) 비트가 설정되어 있으므로 이들을 터널에 넣을 수 없으며 프래그먼트화할 수 없습니다.
- ASA는 mp-svc-no-fragment-ASP 삭제 사유가 포함된 패킷을 인쇄 및 삭제합니다.

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

- 동시에 ASA는 ICMP Destination Unreachable, Fragmentation Needed를 전송자에게 전송합니다.

```
%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
```

- ICMP(Internet Control Message Protocol)가 허용되면 발신자는 삭제된 패킷을 다시 전송하며 모든 것이 작동하기 시작합니다. ICMP가 차단되면 ASA에서 트래픽이 블랙홀링됩니다.
- 여러 번 재전송한 후에는 DTLS 터널을 설정할 수 없으며 VPN 어댑터에 새 MTU 값을 다시 할당해야 함을 인식합니다.
- 이 재연결의 목적은 새 MTU를 할당하는 것입니다.

재연결 동작 및 타이머에 대한 자세한 내용은 을/를 참조하십시오.

관련 정보

- [Cisco 기술 지원 및 다운로드]

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.