

AnyConnect VPN 클라이언트 문제 해결 가이드 - 일반 문제

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제 해결 프로세스](#)

[설치 및 가상 어댑터 문제](#)

[연결 해제 또는 초기 연결 설정 불가](#)

[트래픽 통과 관련 문제](#)

[AnyConnect 충돌 문제](#)

[프래그먼트화/트래픽 통과 문제](#)

[자동 제거](#)

[클러스터 FQDN 채우기 문제](#)

[백업 서버 목록 설정](#)

[AnyConnect: 손상된 드라이버 데이터베이스 문제](#)

[수리](#)

[복구 실패](#)

[데이터베이스 분석](#)

[오류 메시지](#)

[오류: 세션 관리 데이터베이스를 업데이트할 수 없습니다.](#)

[해결 방법 1](#)

[해결 방법 2](#)

[오류: "모듈 c:\프로그램 파일\Cisco\Cisco AnyConnect VPN 클라이언트\vpnapi.dll을 등록하지 못했습니다."](#)

[솔루션](#)

[오류: "VPN 협상 요청에 대한 응답으로 보안 게이트웨이에서 오류가 발생했습니다. Please contact your network administrator"](#)

[솔루션](#)

[오류: 세션을 설정할 수 없습니다. Session limit of 2 reached.](#)

[해결 방법 1](#)

[해결 방법 2](#)

[오류: ASA에 anyconnect를 연결하는 동안 VPN 서버에서 Anyconnect가 활성화되지 않았습니다.](#)

[솔루션](#)

[오류:- %ASA-6-722036: Group client-group User xxxx IP x.x.x Transmitting large packet 1220\(임계값 1206\)](#)

[솔루션](#)

[오류: 보안 게이트웨이에서 에이전트의 VPN 연결 또는 다시 연결 요청을 거부했습니다.](#)

[솔루션](#)

[오류: "세션 관리 데이터베이스를 업데이트할 수 없습니다."](#)

솔루션

오류: "VPN 클라이언트 드라이버에 오류가 발생했습니다."

솔루션

오류: "xxx.xxx.xxx.xxx에서 응답을 처리할 수 없습니다."

솔루션

오류: "로그인 거부, 무단 연결 메커니즘, 관리자에게 문의"

솔루션

오류: "Anyconnect 패키지를 사용할 수 없거나 손상되었습니다. Contact your system administrator"

솔루션

오류: "보안 게이트웨이의 AnyConnect 패키지를 찾을 수 없습니다."

솔루션

오류: "원격 데스크톱을 통한 보안 VPN은 지원되지 않습니다."

솔루션

오류: "받은 서버 인증서 또는 해당 체인이 FIPS를 준수하지 않습니다. A VPN connection will not be established"

솔루션

오류: "인증서 유효성 검사 실패"

솔루션

오류: "VPN 에이전트 서비스에 문제가 발생하여 서비스를 닫아야 합니다. We are sorry for the inconvenience"

솔루션

오류: "이 설치 패키지를 열 수 없습니다. Verify that the package exists"

솔루션

오류: "변환을 적용하는 동안 오류가 발생했습니다. Verify that the specified transform paths are valid."

솔루션

오류: "VPN 클라이언트 드라이버에 오류가 발생했습니다."

솔루션

오류: "VPN을 다시 연결하면 다른 구성 설정이 발생했습니다. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored."

솔루션

로그인 도중 AnyConnect 오류 발생

솔루션

Windows 7에서 AnyConnect 연결이 해제된 후 IE 프록시 설정이 복구되지 않음

솔루션

오류: 이 모든 세션이 닫힐 때까지 AnyConnect Essentials를 활성화할 수 없습니다.

솔루션

오류: Internet Explorer의 인터넷 옵션에 있는 연결 탭은 AnyConnect 클라이언트에 연결된 후 숨겨집니다.

솔루션

오류: 다른 사용자가 AnyConnect VPN을 통해 성공적으로 연결할 수 있는 경우 로그인 실패 오류 메시지를 수신하는 사용자가 거의 없음

솔루션

오류: 보고 있는 인증서가 보려는 사이트의 이름과 일치하지 않습니다.

솔루션

Windows 7 시스템의 CSD Vault에서 AnyConnect를 시작할 수 없음

[솔루션](#)

[파일오버 후 AnyConnect 프로파일이 대기여 복제되지 않음](#)

[솔루션](#)

[Internet Explorer가 오프라인 상태가 되면 AnyConnect 클라이언트가 충돌함](#)

[솔루션](#)

[오류 메시지: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER](#)

[솔루션](#)

[오류 메시지: "잘못된 호스트 항목으로 인해 연결 시도가 실패했습니다."](#)

[솔루션](#)

[오류: "Always-on VPN을 구성하는 경우 서버 인증서가 엄격 모드를 통과할 수 있는지 확인하십시오."](#)

[솔루션](#)

[오류: "Microsoft Windows HTTP 서비스에서 내부 오류가 발생했습니다."](#)

[솔루션](#)

[오류: "SSL 전송이 보안 채널 오류를 수신했습니다. May be a result of a unsupported crypto configuration on the Secure Gateway."](#)

[솔루션](#)

[관련 정보](#)

소개

이 문서에서는 Cisco AnyConnect VPN Client를 통해 작동하지 않는 애플리케이션에 적용되는 문제 해결 시나리오를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 버전 8.x를 실행하는 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

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

문제 해결 프로세스

이 일반적인 문제 해결 시나리오는 Microsoft Windows 기반 컴퓨터를 사용하는 최종 사용자의 Cisco AnyConnect VPN Client를 통해 작동하지 않는 애플리케이션에 적용됩니다. 이 섹션에서는 다음 문제에 대한 해결책을 제공합니다.

- [설치 및 가상 어댑터 문제](#)

- [연결 해제 또는 초기 연결 설정 불가](#)
- [트래픽 통과 관련 문제](#)
- [AnyConnect 충돌 문제](#)
- [프래그먼트화/트래픽 통과 문제](#)

설치 및 가상 어댑터 문제

다음 단계를 완료하십시오.

1. 디바이스 로그 파일 가져오기:

- Windows XP / Windows 2000:

```
<#root>
```

```
\Windows\setupapi.log
```

- Windows Vista:



참고: 이러한 파일을 보려면 숨겨진 폴더를 표시해야 합니다.

```
<#root>
```

```
\Windows\Inf\setupapi.app.log
```

```
\Windows\Inf\setupapi.dev.log
```

setupapi 로그 파일에 오류가 표시된 경우 자세한 정도를 0x2000FFFF로 설정할 수 있습니다.

2. MSI 설치 프로그램 로그 파일 가져오기:

초기 웹 구축 설치인 경우, 로그 파일은 사용자별 임시 디렉토리에 있습니다.

- Windows XP / Windows 2000:

이언트의 버전에 대한 최근 파일을 확보하십시오. x.xxxx는 버전에 따라 다르며(예: 2.0.0343), yyyyyyyyyyyyyyy는 설치 날짜 및 시간입니다.

3. PC 시스템 정보 파일 가져오기:


a. 명령 프롬프트/DOS box에서 다음을 입력합니다.

- Windows XP / Windows 2000:

```
<#root>  
winmsd /nfo c:\msinfo.nfo
```

- Windows Vista:

```
<#root>  
msinfo32 /nfo c:\msinfo.nfo
```

 참고: 이 프롬프트에 입력한 후 기다리십시오. 파일이 완료되는 데 2~5분 정도 걸릴 수 있습니다.

b. 명령 프롬프트에서 systeminfo 파일 덤프 가져오기:

Windows XP 및 Windows Vista:

```
<#root>  
systeminfo c:\sysinfo.txt
```

드라이버 문제를 [디버깅하려면 AnyConnect: 손상된 드라이버 데이터베이스](#) 문제를 참조하십시오.

연결 해제 또는 초기 연결 설정 불가

AnyConnect 클라이언트에서 연결 해제 또는 초기 연결 설정 불가 등의 연결 문제가 발생하는 경우 다음 파일을 가져오십시오.

- 설정에서 연결 실패를 유발하는 항목이 있는지 확인하기 위한 ASA의 설정 파일:

ASA 콘솔에서 `write net x.x.x.x:ASA-Config.txt`를 입력합니다. 여기서 `x.x.x.x`는 네트워크에 있는 TFTP 서버의 IP 주소입니다.

또는

ASA 콘솔에서 `show running-config`를 입력합니다. 화면에서 설정을 완료한 다음 텍스트 편집기에 잘라낸 다음 붙여넣고 저장합니다.

- ASA 이벤트 로그:

1. auth, WebVPN, SSL(Secure Sockets Layer) 및 SVC(SSL VPN Client) 이벤트에 대해 ASA에서 로깅을 활성화하려면 다음 CLI 명령을 실행합니다.

```
<#root>
```

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

2. AnyConnect 세션을 시작하고 실패를 재현할 수 있는지 확인합니다. 콘솔에서 로깅 출력을 텍스트 편집기로 캡처하고 저장합니다.
3. 로깅을 비활성화하려면 `no logging enable`을 실행합니다.


- 클라이언트 PC의 Windows 이벤트 뷰어에서의 Cisco AnyConnect VPN Client 로그:

1. 시작 > 실행을 선택합니다.
2. 입력 사항:

```
eventvwr.msc /s
```

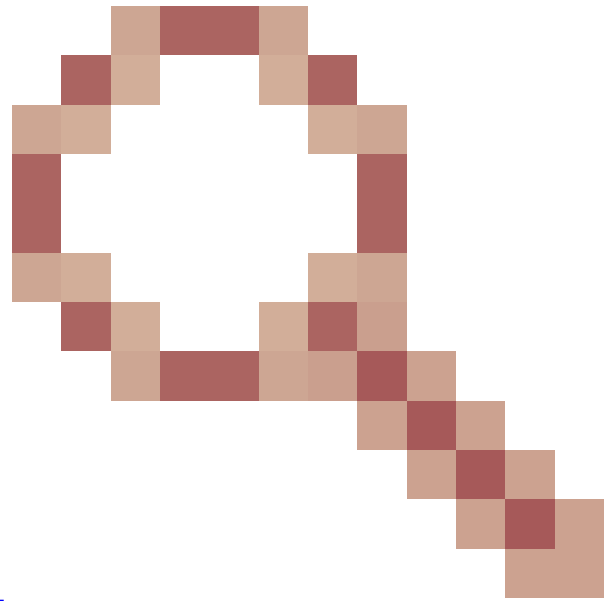
3. Cisco AnyConnect VPN Client 로그를 마우스 오른쪽 버튼으로 클릭하고

AnyConnect.evt로 Save Log File(로그 파일 저장)을 선택합니다.


 참고: 항상 .evt 파일 형식으로 저장하십시오.

사용자가 AnyConnect VPN 클라이언트에 연결할 수 없는 경우, 클라이언트 PC에서 활성화된 RDP(Remote Desktop Protocol) 세션 또는 빠른 사용자 전환과 관련된 문제일 수 있습니다.

AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection will not be established error message 오류 메시지가 클라이언트 PC에 표시됩니다. 이 문제를 해결하려면 설정된 RDP 세션의 연결을 해제하고 빠른 사용자 전환을 비활성화합니다. 이 동작은 클라이언트 프로파일의 [Windows Logon Enforcement](#) 속성에 의해 제어되지만, 현재는 여러 사용자가 동일한 시스템에서 동시에 로그인하는 동안 사용자의 VPN 연결 설



정을 허용하는 설정이 없습니다. 개선 요청 [CSCsx15061](#) 이(가) 이 기능을 해결하기 위해 제출되었습니다.

 참고: AnyConnect 클라이언트가 ASA에 연결할 수 있도록 포트 443이 차단되어 있지 않은지 확인하십시오.

사용자가 AnyConnect VPN 클라이언트를 ASA에 연결할 수 없는 경우, AnyConnect 클라이언트 버전과 ASA 소프트웨어 이미지 버전이 호환되지 않아 문제가 발생할 수 있습니다. 이 경우 사용자에게 다음과 같은 오류 메시지가 표시됩니다. 설치 관리자가 Cisco VPN 클라이언트를 시작할 수 없으므로 클라이언트리스 액세스를 사용할 수 없습니다.

이 문제를 해결하려면 AnyConnect 클라이언트 버전을 ASA 소프트웨어 이미지와 호환되도록 업그레이드하십시오.

AnyConnect에 처음 로그인하면 로그인 스크립트가 실행되지 않습니다. 연결을 해제하고 다시 로그인하면 로그인 스크립트가 정상적으로 실행됩니다. 이는 정상적인 동작입니다.

AnyConnect VPN 클라이언트를 ASA에 연결할 때 다음 오류가 발생할 수 있습니다. AnyConnect 클라이언트 액세스에 권한이 없는 사용자는 관리자에게 문의하십시오.

이 오류는 AnyConnect 이미지가 ASA에서 누락된 경우 표시됩니다. 이미지가 ASA에 로드되면

AnyConnect는 ASA에 문제 없이 연결할 수 있습니다.

이 오류는 DTLS(Datagram Transport Layer Security)를 비활성화하여 해결할 수 있습니다.
Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크 (클라이언트) 액세스) > AnyConnect Connection Profiles(AnyConnect 연결 프로파일)로 이동한 다음 Enable DTLS(DTLS 활성화) 확인란의 선택을 취소합니다. 이를 통해 DTLS가 비활성화됩니다.

dartbundle 파일은 사용자의 연결이 끊어질 때 이 오류 메시지를 표시합니다.

TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE:보안 게이트웨이가 데드 피어 감지 패킷에 응답하지 못했습니다. 이 오류는 DPD(Dead Peer Detection) 오류로 인해 DTLS 채널이 끊어졌음을 의미합니다. 이 오류는 DPD keepalive를 조정하고 다음 명령을 실행하면 해결됩니다.

```
<#root>
```

```
webvpn
  svc keepalive 30
  svc dpd-interval client 80
  svc dpd-interval gateway 80
```

svc keepalive 및 svc dpd-interval 명령은 여기에 표시된 것과 같이 ASA 버전 8.4(1) 이상에서는 각각 anyconnect keepalive 및 anyconnect dpd-interval 명령으로 대체됩니다.

```
<#root>
```

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

트래픽 통과 관련 문제

ASA를 통해 AnyConnect 세션이 포함된 프라이빗 네트워크로 트래픽이 통과할 때 문제가 감지되는 경우 다음 데이터 수집 단계를 완료합니다.

1. 콘솔에서 show vpn-sessiondb detail svc filter name <username> ASA 명령의 출력을 가져옵니다. 출력에 Filter Name(필터 이름): xxxxx가 표시되면, show access-list XXXXX에 대한 출력을 수집합니다. access-list XXXXX가 의도한 트래픽 흐름을 차단하지 않는지 확인합니다.
2. AnyConnect VPN Client(AnyConnect VPN 클라이언트) > Statistics(통계) > Details(세부 정보) > Export(내보내기)에서 AnyConnect 통계를 내보냅니다(AnyConnect-ExportedStats.txt).
3. nat 명령문에 대한 ASA 설정 파일을 확인합니다. NAT(Network Address Translation)를 활성화한 경우, NAT의 결과로 인해 클라이언트로 반환되는 데이터를 제외해야 합니다. 예를 들어 AnyConnect 풀에서 IP 주소를 NAT 제외(nat 0)시키려면 CLI에서 이 명령을 사용합니다.

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. 설정에 터널링된 기본 게이트웨이를 활성화해야 하는지 결정합니다. 기존의 기본 게이트웨이는 암호 해독되지 않은 트래픽을 위한 최종 경로입니다.

예:

```
<#root>
```

```
!--- Route outside 0 0 is an incorrect statement.
```

```
route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2
```

```
tunneled
```

예를 들어 VPN 클라이언트가 VPN 게이트웨이의 라우팅 테이블에 없는 리소스에 액세스해야 하는 경우, 패킷은 표준 기본 게이트웨이를 통해 라우팅됩니다. VPN 게이트에는 이를 해결하기 위해 내부 라우팅 테이블 전체가 필요하지 않습니다. 이 경우에는 tunneled 키워드를 사용할 수 있습니다.

5. AnyConnect 트래픽이 ASA의 검사 정책에 의해 삭제되었는지 확인합니다. Cisco ASA의 Modular Policy Framework를 구현하는 경우 AnyConnct 클라이언트에서 사용하는 특정 애플리케이션을 제외할 수 있습니다. 예를 들어, 다음 명령을 사용하여 skinny 프로토콜을 제외할 수 있습니다.

```
<#root>
```

```
ASA(config)#
```

```
policy-map global_policy
```

```
ASA(config-pmap)#
```

```
class inspection_default
```

```
ASA(config-pmap-c)#
```

```
no inspect skinny
```

AnyConnect 충돌 문제

데이터 수집 단계를 완료하십시오.

1. Microsoft Utility Dr Watson이 활성화되어 있어야 합니다. 이를 위해 Start(시작) > Run(실행)을 선택하고 Drwtsn32.exe를 실행합니다. 설정한 다음 OK(확인)를 클릭합니다.

```
Number of Instructions      : 25
Number of Errors To Save   : 25
Crash Dump Type            : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts   : Checked
Append To Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File     : Checked
```

충돌이 발생하는 경우 C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson에서 .log 및 .dmp 파일을 수집합니다. 이러한 파일이 사용 중인 것으로 표시되는 경우 ntbackup.exe를 사용합니다.

2. 클라이언트 PC의 Windows 이벤트 뷰어에서의 Cisco AnyConnect VPN Client 로그를 가져옵니다.

a. 시작 > 실행을 선택합니다.

b. 입력 사항:

```
<#root>
```

```
eventvwr.msc /s
```

- c. Cisco AnyConnect VPN Client 로그를 마우스 오른쪽 버튼으로 클릭하고 AnyConnect.evt로 Save Log File(로그 파일 저장)을 선택합니다.



참고: 항상 .evt 파일 형식으로 저장하십시오.

프래그먼트화/트래픽 통과 문제

Microsoft Outlook과 같은 일부 애플리케이션은 작동하지 않습니다. 하지만 터널은 소규모 ping과 같은 다른 트래픽을 전달할 수 있습니다.

이는 네트워크의 프래그먼트화 문제에 대한 단서를 제공할 수 있습니다. 사용자 라우터는 패킷 프래그먼트화 및 리어셈블리에 특히 열악합니다.

특정 크기에서 실패가 발생하는지 확인하려면 여러 크기의 ping 집합을 사용해 보십시오. ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000을 예로 들 수 있습니다.

프래그먼트화를 경험하는 사용자를 위해 특수 그룹을 설정하고 이 그룹에 대한 SVC MTU(Maximum Transition Unit)를 1200으로 설정하는 것이 좋습니다. 이렇게 하면 사용자에게 발생한 이 문제를 교정하면서 폭넓은 사용자 기반에는 영향을 미치지 않습니다.

문제

AnyConnect와 연결되면 TCP 연결은 중단됩니다.

솔루션

사용자에게 프래그먼트화 문제가 있는지 확인하려면 ASA의 AnyConnect 클라이언트에 대한 MTU를 조정하십시오.

```
ASA(config)#group-policy <name> attributes
                        webvpn
                        svc mtu 1200
```

자동 제거

문제

연결이 종료되면 AnyConnect VPN 클라이언트가 자동으로 제거됩니다. 클라이언트 로그에는 keep installed가 비활성화로 설정되어 있음이 표시됩니다.

솔루션

AnyConnect는 keep installed 옵션이 ASDM(Adaptive Security Device Manager)에서 선택되어 있는 경우에도 자동으로 제거됩니다. 이 문제를 해결하려면 group-policy에서 svc keep-installer installed 명령을 설정합니다.

클러스터 FQDN 채우기 문제

문제: AnyConnect 클라이언트가 클러스터 FQDN(정규화된 도메인 이름) 대신 호스트 이름으로 미리 채워져 있습니다.

SSL VPN에 대해 로드 밸런싱 클러스터가 설정되어 있고 클라이언트가 클러스터에 연결하려고 하면 요청이 노드 ASA로 리디렉션되고 클라이언트 로그인은 성공합니다. 잠시 후에 클라이언트가 다시 클러스터에 연결을 시도하면 클러스터 FQDN이 Connect to(연결 대상) 항목에 표시되지 않습니

다. 대신 클라이언트가 리디렉션된 노드 ASA 항목이 표시됩니다.

솔루션

이러한 현상은 AnyConnect 클라이언트가 마지막으로 연결된 호스트 이름을 유지하기 때문에 발생합니다. 이 동작은 관측되었으며 버그가 제기되었습니다. 버그에 대한 자세한 내용은 Cisco 버그 ID CSCsz39019를 [참조하십시오](#). 권장 해결 방법은 Cisco AnyConnect를 버전 2.5로 업그레이드하는 것입니다.

백업 서버 목록 설정

사용자가 선택한 기본 서버에 연결할 수 없는 경우 백업 서버 목록이 설정됩니다. 이는 AnyConnect 프로파일의 Backup Server(백업 서버) 창에서 정의됩니다. 다음 단계를 완료하십시오.

1. [AnyConnect Profile Editor](#)([등록](#) 고객 전용)를 다운로드하십시오. 파일 이름은 AnyConnectProfileEditor2_4_1.jar입니다.
2. AnyConnect Profile Editor를 사용하여 XML 파일을 생성합니다.
 - a. 서버 목록 탭으로 이동합니다.
 - b. Add(추가)를 클릭합니다.
 - c. Hostname(호스트 이름) 필드에 기본 서버를 입력합니다.
 - d. Host address(호스트 주소) 필드의 백업 서버 목록 아래에 백업 서버를 추가합니다. 그런 다음 Add(추가)를 클릭합니다.
3. XML 파일이 있으면 ASA에서 사용하는 연결에 해당 파일을 할당해야 합니다.
 - a. ASDM에서 Configuration(설정) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > AnyConnect Connection Profiles(AnyConnect 연결 프로파일)를 선택합니다.
 - b. 프로파일을 선택하고 Edit(편집)를 클릭합니다.
 - c. Default Group Policy(기본 그룹 정책) 섹션에서 Manage(관리)를 클릭합니다.
 - d. 그룹 정책을 선택하고 Edit(편집)를 클릭합니다.
 - e. Advanced(고급)를 선택한 다음 SSL VPN Client(SSL VPN 클라이언트)를 클릭합니다.
 - f. 새로 만들기를 클릭합니다. 그런 다음 프로파일의 이름을 입력하고 XML 파일을 할당해야 합니다.

4. XML 파일을 다운로드하려면 클라이언트를 세션에 연결합니다.

AnyConnect: 손상된 드라이버 데이터베이스 문제

SetupAPI.log 파일의 이 항목은 카탈로그 시스템이 손상되었음을 나타냅니다.

W239 드라이버 서명 클래스 목록 "C:\WINDOWS\INF\certclas.inf"가 누락되었거나 잘못되었습니다. 오류 0xfffffde5: 알 수 없는 오류입니다. 모든 장치 클래스가 드라이버 서명 정책의 적용을 받는다고 가정합니다.

Error(3/17): Unable to start VA, setup shared queue, or VA forged up shared queue(VA를 시작할 수 없음, 공유 큐 설정 또는 VA가 공유 큐를 포기함)라는 오류 메시지도 받을 수 있습니다.

클라이언트에서 이 로그를 받을 수 있습니다. "VPN 클라이언트 드라이버에서 오류가 발생했습니다".

수리

이 문제는 Cisco 버그 ID CSCsm54689 [때문입니다](#). 이 문제를 해결하려면 AnyConnect를 시작하기 전에 라우팅 및 원격 액세스 서비스가 비활성화되어 있는지 확인하십시오. 이로 인해 문제가 해결되지 않는 경우 다음 단계를 완료하십시오.

1. PC에서 관리자 권한으로 명령 프롬프트를 엽니다(Vitas에서는 권한 상승 프롬프트).
2. `net stop CryptSvc`를 실행합니다.
3. 실행:

```
esentutl /p%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. 프롬프트가 표시되면 OK(확인)를 선택하여 복구를 시도하십시오.
5. 명령 프롬프트를 종료합니다.
6. 재부팅합니다.

복구 실패

복구에 실패하는 경우 다음 단계를 완료하십시오.

1. PC에서 관리자 권한으로 명령 프롬프트를 엽니다(Vitas에서는 권한 상승 프롬프트).
2. `net stop CryptSvc`를 실행합니다.

3. %WINDIR%\system32\catroot2 to catroot2_old 디렉터리 이름을 변경합니다.
4. 명령 프롬프트를 종료합니다.
5. 재부팅합니다.

데이터베이스 분석

언제든 데이터베이스를 분석하여 유효한지 여부를 확인할 수 있습니다.

1. PC에서 관리자 권한으로 명령 프롬프트를 엽니다.
2. 실행:

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

자세한 내용은 [시스템 카탈로그 데이터베이스 무결성](#)을 참조하십시오.

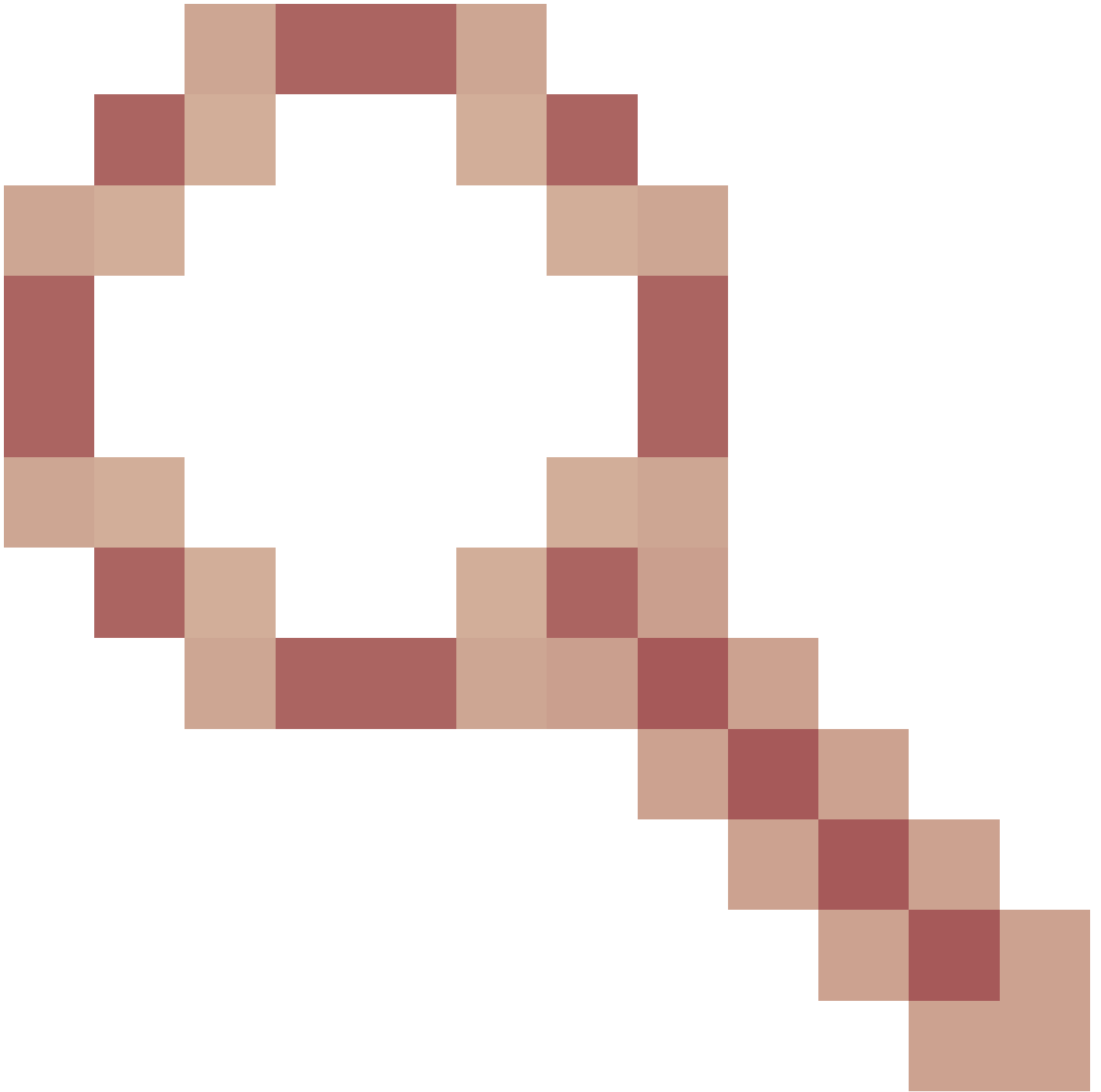
오류 메시지

오류: 세션 관리 데이터베이스를 업데이트할 수 없습니다.

SSL VPN이 웹 브라우저를 통해 연결되어 있는 동안 Unable to Update the Session Management Database. 오류 메시지가 나타나고, ASA 로그에 %ASA-3-211001: Memory allocation Error가 표시됩니다. The adaptive security appliance failed to allocate RAM system memory.

해결 방법 1

이 문제는 Cisco 버그 ID CSCsm51093 [때문입니다](#). 이 문제를 해결하려면 ASA를 다시 로드하거나 ASA 소프트웨어를 버그에 언급된 중간 릴리스로 업그레이드하십시오. Cisco 버그 ID CSCsm을 [참조하십시오51093](#)



추가 정보.

해결 방법 2

위협 탐지가 사용되는 경우 ASA에서 위협 탐지를 비활성화하여 이 문제를 해결할 수 있습니다.

오류: "모듈 c:\프로그램 파일\Cisco\Cisco AnyConnect VPN 클라이언트\vpnapi.dll을 등록하지 못했습니다."

노트북 또는 PC에서 AnyConnect 클라이언트를 사용하는 경우 설치 중에 오류가 발생합니다.

"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."

이 오류가 발생하면 설치 프로그램을 진행할 수 없으며 클라이언트가 제거됩니다.

솔루션

다음은 이 오류를 해결할 수 있는 방법입니다.

- 최신 AnyConnect 클라이언트는 Microsoft Windows 2000에서 더 이상 공식적으로 지원되지 않습니다. 이는 2000 컴퓨터의 레지스트리 문제입니다.
- VMware 애플리케이션을 제거합니다. AnyConnect가 설치되면 VMware 애플리케이션을 PC에 다시 추가할 수 있습니다.
- 신뢰할 수 있는 사이트에 ASA를 추가합니다.
- \ProgramFiles\Cisco\CiscoAnyconnect 폴더에서 새 폴더로 파일을 복사하고 regsvr32 vpnapi.dll 명령 프롬프트를 실행합니다.
 - vpnapi.dll
 - vpncommon.dll
 - vpncommoncrypt.dll
- 노트북/PC에서 운영 체제 이미지를 다시 설치합니다.

AnyConnect 클라이언트에서 이 오류와 관련된 로그 메시지는 다음과 유사합니다.

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
Info 1721. There is a problem with this Windows Installer package. A program required for
this install to complete could not be run. Contact your support personnel or package
vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN
Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application
Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

오류: "VPN 협상 요청에 대한 응답으로 보안 게이트웨이에서 오류가 발생했습니다.
Please contact your network administrator"

클라이언트가 Cisco AnyConnect VPN Client를 사용하여 VPN에 연결하려고 하면 이 오류가 표시

됩니다.

이 메시지는 보안 게이트웨이에서 수신되었습니다.

"Illegal address class", "Host or network is 0" 또는 "Other error"

솔루션

이 문제는 ASA 로컬 IP 풀 소진으로 인해 발생합니다. VPN 풀 리소스가 소진되면 IP 풀 범위를 확장해야 합니다.


이 문제에 대해 Cisco 버그 ID [CSCs182188](#)이 제출되었습니다. 이 오류는 일반적으로 주소 할당을 위한 로컬 풀이 소진되었거나 주소 풀에 32비트 서브넷 마스크가 사용되는 경우에 발생합니다. 해결 방법은 주소 풀을 확장하고 풀에 24비트 서브넷 마스크를 사용하는 것입니다.

오류: 세션을 설정할 수 없습니다. Session limit of 2 reached.

AnyConnect VPN 클라이언트에 셋 이상의 클라이언트를 연결하려 할 때 클라이언트에서 Login Failed 오류 메시지를 수신하고 ASA 로그에 session could not be established. 경고 메시지가 표시됩니다. Session limit of 2 reached. ASA에 AnyConnect essential 라이선스가 있으며, 버전 8.0.4를 실행합니다.

해결 방법 1

이 오류는 ASA 버전 8.0.4에서 AnyConnect 필수 라이선스가 지원되지 않기 때문에 발생합니다. ASA를 버전 8.2.2로 업그레이드해야 합니다. 이렇게 하면 오류가 해결됩니다.

 참고: 사용된 라이선스와 상관없이 세션 한도에 도달하면 사용자는 로그인 실패 오류 메시지를 수신합니다.

해결 방법 2

이 오류는 vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit 명령을 사용하여 설정 허용된 VPN 세션 제한을 설정하는 경우 발생할 수 있습니다. session-limit가 2로 설정된 경우 설치된 라이선스가 그 이상을 세션을 지원하는 경우에도 사용자가 2개를 초과하는 세션을 설정할 수 없습니다. 이 오류 메시지를 방지하려면 session-limit를 필요한 VPN 세션 수로 설정합니다.

오류: ASA에 anyconnect를 연결하는 동안 VPN 서버에서 Anyconnect가 활성화되지 않았습니다.

ASA에 AnyConnect를 연결하려 할 때 오류 메시지 anyconnect not enabled on VPN server가 표시됩니다.

솔루션

이 오류는 ASDM을 사용하여 ASA의 외부 인터페이스에서 AnyConnect를 활성화하는 경우 해결됨

니다. 외부 인터페이스에서 AnyConnect를 활성화하는 방법에 대한 자세한 내용은 [ASA에 클라이언 트리스 SSL VPN\(WebVPN\) 설정](#)을 참조하십시오.

오류:- %ASA-6-722036: Group client-group User xxxx IP x.x.x Transmitting large packet 1220(임계값 1206)

%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) 오류 메시지가 ASA의 로그에 나타납니다. 이 로그는 무엇을 의미하며 어떻게 해결 됩니까?

솔루션

이 로그 메시지는 대용량 패킷이 클라이언트로 전송되었음을 나타냅니다. 패킷의 소스가 클라이언 트의 MTU를 인식하지 못합니다. 이는 비압축 데이터의 압축 때문일 수도 있습니다. 해결 방법은 svc compression none 명령을 사용하여 SVC 압축을 해제하는 것입니다. 이렇게 하면 문제가 해결 됩니다.

오류: 보안 게이트웨이에서 에이전트의 VPN 연결 또는 다시 연결 요청을 거부했습니다.

AnyConnect 클라이언트에 연결할 때 다음 오류가 수신됩니다. "보안 게이트웨이가 에이전트의 vpn 연결 또는 재연결 요청을 거부했습니다. A new connection requires re-authentication and must be started manually. Please contact your network administrator if this problem persists. 보안 게이트웨이에서 다음 메시지를 받았습니다. 할당된 주소가 없습니다.

이 오류는 AnyConnect 클라이언트에 연결할 때도 발생합니다. "보안 게이트웨이에서 연결 시도를 거부했습니다. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication. The following message was received from the secure gateway:Host or network is 0".

이 오류는 AnyConnect 클라이언트에 연결할 때도 발생합니다. "보안 게이트웨이가 에이전트의 vpn 연결 또는 다시 연결 요청을 거부했습니다. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. 보안 게이트웨이에서 다음 메시지를 받았습니다. 라이선스 없음".

솔루션

다시 로드한 후 라우터에 풀 설정이 누락되었습니다. 관련 설정을 라우터에 다시 추가해야 합니다.

<#root>

Router#

show run | in pool

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254
  svc address-pool SSLP00
```

"The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. 보안 게이트웨이에서 다음 메시지를 받았습니다. AnyConnect 모바일리티 라이선스가 없을 때 "라이선스 없음" 오류가 발생합니다. 라이선스가 설치되면 문제가 해결됩니다.

오류: "세션 관리 데이터베이스를 업데이트할 수 없습니다."

WebPortal에서 인증을 시도할 때 "세션 관리 데이터베이스를 업데이트할 수 없습니다."라는 오류 메시지가 표시 됩니다.

솔루션

이 문제는 ASA의 메모리 할당과 관련이 있습니다. 이 문제는 ASA 버전이 8.2.1일 때 주로 발생합니다. 원래는 완전한 기능을 위해서는 512MB RAM이 필요합니다.

영구적인 해결 방법은 메모리를 512MB로 업그레이드하는 것입니다.

임시 해결 방법은 다음 단계를 수행하여 메모리를 확보하는 것입니다.

1. 위협 탐지를 비활성화합니다.
2. SVC 압축을 비활성화합니다.
3. ASA를 다시 로드합니다.

오류: "VPN 클라이언트 드라이버에 오류가 발생했습니다."

이는 AnyConnect에 연결을 시도할 때 클라이언트 시스템에 표시되는 오류 메시지입니다.

솔루션

이 오류를 해결하려면 다음 절차를 완료하여 AnyConnect VPN 에이전트를 대화형으로 수동 설정합니다.

1. 마우스 오른쪽 버튼으로 My Computer(내 컴퓨터)를 클릭하고 Manage(관리) > Services and Applications(서비스 및 애플리케이션) > Services(서비스)를 클릭한 다음 Cisco AnyConnect VPN Agent(Cisco AnyConnect VPN 에이전트)를 선택합니다.
2. 마우스 오른쪽 버튼으로 Properties(속성)을 클릭하고 로그인한 다음 Allow service to interact with the desktop(서비스의 데스크톱과의 상호 작용 허용)을 선택합니다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent에 대한 레지스트리 Type 값 DWORD를 110으로 설정합니다(기본값은 010).



참고: 이 옵션을 사용하려면 이 인스턴스에서 .MST 변환을 사용하는 것이 좋습니다. 이러한 방법을 사용하여 수동으로 설정하는 경우 모든 설치/업그레이드 프로세스 후에 이를 설정해야 하기 때문입니다. 따라서 이 문제를 유발하는 애플리케이션을 식별해야 합니다.

Windows PC에서 RRAS(Routing and Remote Access Service)를 사용하도록 설정하면 VPN 클라이언트 드라이버에서 오류가 발생하여 AnyConnect가 실패합니다. 오류 메시지 이 문제를 해결하려면 AnyConnect를 시작하기 전에 RRAS가 비활성화되어 있는지 확인하십시오. 자세한 내용은 Cisco 버그 ID [CSCsm54689](#)를 참조하십시오.

오류: "xxx.xxx.xxx.xxx에서 응답을 처리할 수 없습니다."

AnyConnect 클라이언트가 Cisco ASA 연결에 실패합니다. AnyConnect 창의 오류는 "Unable to process response from xxx.xxx.xxx.xxx"입니다.

솔루션

이 오류를 해결하려면 다음 해결 방법을 시도해 보십시오.

- ASA에서 WebVPN을 제거하고 다시 활성화합니다.
- 포트 번호를 기존 443에서 444로 변경하고 443에서 다시 활성화합니다.

WebVPN을 활성화하고 WebVPN용 포트를 변경하는 방법에 대한 자세한 내용은 이 [솔루션](#)을 참조하십시오.

오류: "로그인 거부, 무단 연결 메커니즘, 관리자에게 문의"

AnyConnect 클라이언트가 Cisco ASA 연결에 실패합니다. AnyConnect 창의 오류는 "Login Denied , unauthorized connection mechanism , contact your administrator"입니다.

솔루션

이 오류 메시지는 주로 부적절하거나 불안정한 설정 문제로 인해 발생합니다. 설정을 확인하고 문제를 해결하는 데 필요한지 확인합니다.

<

오류: "Anyconnect 패키지를 사용할 수 없거나 손상되었습니다. Contact your system administrator"

이 오류는 ASA에 연결하기 위해 Macintosh 클라이언트에서 AnyConnect 소프트웨어를 실행하려고 할 때 발생합니다.

솔루션

이 문제를 해결하려면 다음 단계를 수행합니다.

1. Macintosh AnyConnect 패키지를 ASA의 플래시에 업로드합니다.
2. 사용되는 AnyConnect 패키지를 지정하려면 WebVPN 설정을 수정합니다.

```
webvpn
svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

svc image 명령은 다음과 같이 ASA 버전 8.4(1) 이상에서 anyconnect image 명령으로 대체됩니다.

```
<#root>
```

```
hostname(config)#
```

```
webvpn
```

```
hostname(config-webvpn)#
```

```
anyconnect image disk0:/
```

```
anyconnect-win-3.0.0527-k9.pkg 1
```

```
hostname(config-webvpn)#
```

```
anyconnect image disk0:/
```

```
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

오류: "보안 게이트웨이의 AnyConnect 패키지를 찾을 수 없습니다."

이 오류는 AnyConnect를 실행하여 ASA에 연결을 시도할 때 사용자의 Linux 시스템에서 발생합니다. 전체 오류는 다음과 같습니다.

```
<#root>
```

```
"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."
```

솔루션

이 오류 메시지를 해결하려면 클라이언트 시스템에서 사용되는 OS(운영 체제)가 AnyConnect 클라이언트에서 지원되는지 확인합니다.

OS가 지원되는 경우 AnyConnect 패키지가 WebVPN 설정에 지정되어 있는지 확인합니다. 자세한 내용은 이 문서의 [Anyconnect 패키지를 사용할 수 없거나 손상됨](#) 섹션을 참조하십시오.

오류: "원격 데스크톱을 통한 보안 VPN은 지원되지 않습니다."

사용자가 원격 데스크톱 액세스를 수행할 수 없습니다. `Secure VPN via remote desktop is not supported` 오류 메시지가 표시됩니다.

솔루션

이 문제는 CSCsu22088 및 CSCso42825와 같은 Cisco 버그 ID [때문입니다](#). AnyConnect VPN 클라이언트를 업그레이드할 경우 문제를 해결할 수 있습니다. 자세한 내용은 이 버그를 참조하십시오.

오류: "받은 서버 인증서 또는 해당 체인이 FIPS를 준수하지 않습니다. A VPN connection will not be established"

ASA 5505에 VPN을 시도하면 `The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established` 오류 메시지가 표시됩니다.

솔루션

이 오류를 해결하려면 AnyConnect 로컬 정책 파일에서 FIPS(Federal Information Processing Standards)를 비활성화해야 합니다. 이 파일은 일반적으로 `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml`에서 찾을 수 있습니다. 이 파일이 이 경로에 없는 경우 `C:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`과 같은 경로의 다른 디렉터리에서 파일을 찾습니다. xml 파일을 찾은 후 다음과 같이 이 파일을 변경합니다.

구문 변경:

```
<FipsMode>참</FipsMode>
```

수신:

```
<FipsMode>거짓</FipsMode>
```

그런 다음 컴퓨터를 재시작합니다. 이 파일을 수정하려면 사용자에게 관리 권한이 있어야 합니다.

오류: "인증서 유효성 검사 실패"

사용자가 AnyConnect를 시작할 수 없고 `Certificate Validation Failure` 오류가 표시됩니다.

솔루션

인증서 인증은 IPsec 클라이언트와 비교해 AnyConnect에서 다르게 작동합니다. 인증서 인증이 작동하려면 클라이언트 인증서를 브라우저로 가져오고 연결 프로파일을 변경하여 인증서 인증을 사용해야 합니다. 또한 외부 인터페이스에서 SSL 클라이언트 인증서를 사용하려면 ASA에서 이 명령을 활성화해야 합니다.

```
ssl certificate-authentication interface outside port 443
```

오류: "VPN 에이전트 서비스에 문제가 발생하여 서비스를 닫아야 합니다. We are sorry for the inconvenience"

AnyConnect 버전 2.4.0202가 Windows XP PC에 설치될 때 현지화 파일 업데이트가 중지되고 vpnagent.exe가 실패한다는 오류 메시지가 표시됩니다.

솔루션

이 동작은 Cisco 버그 ID CSCsq49102에 기록됩니다. 권장 해결 방법은 Citrix 클라이언트를 비활성화하는 것입니다.

오류: "이 설치 패키지를 열 수 없습니다. Verify that the package exists"

AnyConnect를 다운로드할 때 이 오류 메시지가 표시됩니다.

```
"Contact your system administrator. 다음 오류로 인해 설치 프로그램이 실패했습니다. 이 설치 패키지를 열 수 없습니다. Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package."
```

솔루션

이 문제를 해결하려면 다음 단계를 수행합니다.

1. 모든 안티 바이러스 소프트웨어를 제거합니다.
2. Windows 방화벽을 비활성화합니다.
3. 1단계 또는 2단계가 도움이 되지 않으면 시스템을 포맷하고 설치합니다.
4. 문제가 지속되는 경우 [TAC 사례](#)를 엽니다.

오류: "변환을 적용하는 동안 오류가 발생했습니다. Verify that the specified transform paths are valid."

이 오류 메시지는 ASA에서 AnyConnect를 자동으로 다운로드하는 동안 표시됩니다.

<#root>

"Contact your system administrator. The installer failed with the following error:
Error applying transforms. Verify that the specified transform paths are valid."

다음은 MacOS용 AnyConnect에 연결할 때 표시되는 오류 메시지입니다.

<#root>

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

솔루션

이 문제를 해결하려면 다음 해결 방법 중 하나를 완료하십시오.

1. 이 오류의 근본 원인은 손상된 MST 변환 파일(예: 가져온 파일) 때문일 수 있습니다. 이를 해결하려면 다음 단계를 수행하십시오.
 - a. MST 변환 테이블을 제거합니다.
 - b. ASA에서 MacOS용 AnyConnect 이미지를 설정합니다.
2. ASDM에서 Network (Client) Access(네트워크(클라이언트) 액세스) > AnyConnect Custom(AnyConnect 사용자 지정) > Installs(설치)로 이동한 다음 AnyConnect 패키지 파일을 삭제합니다. 패키지가 Network (Client) Access(네트워크(클라이언트) 액세스) > Advanced(고급) > SSL VPN > Client Setting(클라이언트 설정)에 있어야 합니다.

이러한 해결 방법으로 문제가 해결되지 않는 경우 [Cisco 기술 지원](#)에 문의하십시오.

오류: "VPN 클라이언트 드라이버에 오류가 발생했습니다."

다음 오류가 표시됩니다.

<#root>

The VPN client driver has encountered an error when connecting through Cisco AnyConnect Client.

솔루션

이 문제는 AnyConnect 클라이언트를 제거한 다음 안티 바이러스 소프트웨어를 제거하면 해결될 수 있습니다. 그런 다음 AnyConnect 클라이언트를 다시 설치하십시오. 이 해결 방법으로 문제가 해결되지 않으면 PC를 다시 포맷하여 이 문제를 해결하십시오.

오류: "VPN을 다시 연결하면 다른 구성 설정이 발생했습니다. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored."

이 오류는 AnyConnect를 시작하려고 할 때 표시됩니다.

<#root>

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

솔루션

이 오류를 해결하려면 다음을 사용하십시오.

```
group-policy <Name> attributes
  webvpn
    svc mtu 1200
```

svc mtu 명령은 다음과 같이 ASA 버전 8.4(1) 이상에서 anyconnect mtu 명령으로 대체됩니다.

<#root>

```
hostname(config)#
```

```
group-policy
```

```
  attributes
```

```
hostname(config-group-policy)#
```

```
webvpn
```

```
hostname(config-group-webvpn)#
```

```
anyconnect mtu 500
```

로그인 도중 AnyConnect 오류 발생

문제

클라이언트에 연결할 때 AnyConnect에 오류가 표시됩니다.

The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.

솔루션

AnyConnect 프로파일을 다음과 같이 변경하면 문제를 해결할 수 있습니다.

AnyConnect 프로파일에 이 라인을 추가합니다.

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

Windows 7에서 AnyConnect 연결이 해제된 후 IE 프록시 설정이 복구되지 않음

문제

Windows 7에서 IE 프록시 설정이 자동 설정 탐지로 설정되어 있고 AnyConnect가 새 프록시 설정을 푸시 다운하는 경우, 사용자가 AnyConnect 세션을 종료한 후 IE 프록시 설정이 자동 설정 탐지로 다시 복원되지 않습니다. 이로 인해 프록시 설정이 자동 설정 탐지로 설정되어야 하는 사용자에게 LAN 문제가 발생합니다.

솔루션

이 동작은 Cisco 버그 ID CSCtj51376에 [기록됩니다](#). 권장 해결 방법은 AnyConnect [3.0](#)으로 [업그레이드하는 것입니다](#).

오류: 이 모든 세션이 닫힐 때까지 AnyConnect Essentials를 활성화할 수 없습니다.

이 오류 메시지는 AnyConnect Essentials 라이선스를 활성화하려고 시도할 때 Cisco ASDM에서 표시됩니다.

<#root>

There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.

솔루션

이는 ASA의 정상적인 동작입니다. AnyConnect Essentials는 별도로 라이선싱된 SSL VPN 클라이언트입니다. ASA에서 완전히 설정되어 있고 다음을 제외한 전체 AnyConnect 기능을 제공합니다.

- Cisco Secure Desktop(CSD) 없음(HostScan/Vault/Cache Cleaner 포함)
- 클라이언트리스 SSL VPN 없음
- 선택적 Windows Mobile 지원

이 라이선스는 공유 SSL VPN 프리미엄 라이선스와 동시에 사용할 수 없습니다. 하나의 라이선스를 사용해야 하는 경우 다른 라이선스를 비활성화해야 합니다.

오류: Internet Explorer의 인터넷 옵션에 있는 연결 탭은 AnyConnect 클라이언트에 연결된 후 숨겨집니다.

AnyConnect 클라이언트에 연결된 이후 Internet Explorer의 인터넷 옵션에 있는 연결 탭이 숨겨집니다.

솔루션

이는 msie-proxy lockdown 기능 때문입니다. If you enable this feature, it hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. 이 기능을 비활성화 하는 경우 연결 탭의 표시가 변경되지 않은 상태로 유지됩니다.

오류: 다른 사용자가 AnyConnect VPN을 통해 성공적으로 연결할 수 있는 경우 로그인 실패 오류 메시지를 수신하는 사용자가 거의 없음

몇몇 사용자에게 로그인 실패 오류 메시지가 표시되는 반면 다른 사용자는 AnyConnect VPN을 통해 성공적으로 연결할 수 있습니다.

솔루션

사전 인증 불필요 확인란이 선택된 경우 이 문제를 해결할 수 있습니다.

오류: 보고 있는 인증서가 보려는 사이트의 이름과 일치하지 않습니다.

AnyConnect 프로파일 업데이트 도중 인증서가 유효하지 않다는 오류가 표시됩니다. 이는 Windows에서만 그리고 프로파일 업데이트 단계에서 발생합니다. 오류 메시지가 여기에 표시됩니

다.

```
<#root>
```


```
The certificate you are viewing does not match with the name of the site  
you are trying to view.
```

솔루션

인증서의 FQDN을 사용하기 위해 AnyConnect 프로파일의 서버 목록을 수정하는 경우 이 문제를 해결할 수 있습니다.

다음은 XML 프로파일의 샘플입니다.

```
<ServerList>  
  
  <HostEntry>  
    <HostName>vpn1.ccsd.net</HostName>  
  
  </HostEntry>  
</ServerList>
```

 참고: 서버의 공용 IP 주소에 대한 기존 항목(예: <HostAddress>)이 있는 경우 이 항목을 제거하고 서버의 FQDN만 유지합니다(예: <HostName>은 유지되지만 <Host Address>는 유지되지 않음).

Windows 7 시스템의 CSD Vault에서 AnyConnect를 시작할 수 없음

AnyConnect가 CSD 저장소에서 시작될 때 작동하지 않습니다. 이는 Windows 7 시스템에서 시도됩니다.

솔루션

현재는 지원되지 않으므로 불가능합니다.

파일오버 후 AnyConnect 프로파일이 대기예 복제되지 않음

ASA 버전 8.4.1 소프트웨어가 포함된 AnyConnect 3.0 VPN 클라이언트는 정상적으로 작동합니다. 하지만 파일오버 후에는 AnyConnect 프로파일 관련 설정에 대한 복제본이 없습니다.

솔루션

이 문제는 Cisco 버그 ID CSCtn71662에서 관찰되고 [기록되었습니다](#). 임시 해결 방법은 파일을 대

기 장치에 수동으로 복사하는 것입니다.

Internet Explorer가 오프라인 상태가 되면 AnyConnect 클라이언트가 충돌함

이 상황이 발생하면 AnyConnect 이벤트 로그에는 다음과 유사한 항목이 포함됩니다.

Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type

Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION

솔루션

이 동작은 Cisco 버그 ID CSCtx28970에서 [관찰되고 기록됩니다](#). 이 문제를 해결하려면 AnyConnect 애플리케이션을 종료하고 다시 시작합니다. 연결 항목이 다시 시작된 후에 다시 표시 됩니다.

오류 메시지: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

AnyConnect 클라이언트가 연결에 실패하고 `Unable to establish a connection` 오류 메시지가 표시 됩니다. AnyConnect 이벤트 로그에서 `TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER` 오류가 발견됩니다.

솔루션

헤드엔드가 매우 큰 스플릿 터널링 목록(약 180~200개 항목)을 사용한 분할 터널링으로 구성되고 하나 이상의 다른 클라이언트 속성이 그룹 정책에서 설정되어 있는 경우(예: dns-server) 이 오류가 발생합니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

1. 스플릿 터널 목록의 항목 수를 줄입니다.
2. DTLS를 비활성화하려면 이 설정을 사용합니다.

```
group-policy groupName attributes
  webvpn
    svc dtls none
```

자세한 내용은 Cisco 버그 ID [CSCtc41770](#)을 참조하십시오.

오류 메시지: "잘못된 호스트 항목으로 인해 연결 시도가 실패했습니다."

Connection attempt has failed due to invalid host entry 오류 메시지는 인증서를 사용하여 AnyConnect를 인증하는 도중 표시됩니다.

솔루션

이 문제를 해결하려면 다음 방법 중 하나를 시도해 보십시오.

- AnyConnect를 버전 3.0으로 업그레이드합니다.
- 컴퓨터에서 Cisco Secure Desktop을 비활성화합니다.

자세한 내용은 Cisco 버그 ID [CSCti73316](#)을 참조하십시오.

오류: "Always-on VPN을 구성하는 경우 서버 인증서가 엄격 모드를 통과할 수 있는지 확인하십시오."

AnyConnect에서 상시 가동 기능을 활성화하면 Ensure your server certificates can pass strict mode if you configure always-on VPN 오류 메시지가 표시됩니다.

솔루션

이 오류 메시지는 상시 가동 기능을 사용하려면 헤드엔드에 유효한 서버 인증서가 설정되어 있어야 함을 의미합니다. 유효한 서버 인증서가 없으면 이 기능이 작동하지 않습니다. 엄격한 인증서 모드는 연결에서 유효한 인증서를 사용하도록 하기 위해 AnyConnect 로컬 정책 파일에서 설정하는 옵션입니다. 정책 파일에서 이 옵션을 활성화하고 가짜 인증서로 연결하는 경우 연결이 실패합니다.

오류: "Microsoft Windows HTTP 서비스에서 내부 오류가 발생했습니다."

이 DART(Diagnostic AnyConnect Reporting Tool)에 실패한 시도가 표시됩니다.

<#root>

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1170

Invoked Function: HttpSendRequest

Return Code: 12004 (0x00002EE4)

Description:

An internal error occurred in the Microsoft Windows HTTP Services

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472

Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Connection attempt failed. Please try again.

또한 Windows 시스템의 이벤트 뷰어 로그를 참조하십시오.

솔루션

이는 Winsock 연결이 손상되었기 때문일 수 있습니다. 이 명령을 사용하여 prompt 명령에서 연결을 재설정하고 Windows 시스템을 재시작합니다.

```
netsh winsock reset
```

자세한 내용은 Windows Server 2003, Windows XP, Windows Vista에서 Winsock2 손상을 확인하고 복구하는 방법 기술 자료 문서를 참조하십시오.

오류: "SSL 전송이 보안 채널 오류를 수신했습니다. May be a result of a unsupported crypto configuration on the Secure Gateway."

이 DART(Diagnostic AnyConnect Reporting Tool)에 실패한 시도가 표시됩니다.

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::handleRequestError
File: .\CTransportWinHttp.cpp
Line: 854

The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configura

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1199

Invoked Function: CTransportWinHttp::handleRequestError
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 3026

Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE
Connection attempt failed. Please try again.

솔루션

Windows 8.1은 다음 KB 업데이트에 따라 RC4를 지원하지 않습니다.

<http://support2.microsoft.com/kb/2868725>

"ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1" 명령을 사용하여 ASA에서 SSL VPN에 대한 DES/3DES 암호를 설정하거나 클라이언트 시스템에 있는 Windows 레지스트리 파일을 아래와 같이 편집합니다.

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

관련 정보

- [Cisco ASA 5500 Series Adaptive Security Appliance](#)
- [AnyConnect VPN 클라이언트 FAQ](#)

- [Cisco Secure Desktop\(CSD\) FAQ](#)
- [Cisco AnyConnect VPN 클라이언트](#)
- [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.