VPN 클라이언트 FAQ

목차

소개

이 문서에서는 Cisco VPN Client에 대해 자주 묻는 질문과 답변을 제공합니다.

참고: 다양한 VPN 클라이언트에 대한 명명 규칙은 다음과 같습니다.

- Cisco Secure VPN Client 버전 1.0 ~ 1.1a 전용
- Cisco VPN 3000 Client 버전 2.x 전용
- Cisco VPN Client 3.x 이상만 해당

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

VPN 클라이언트 소프트웨어 다운로드

Q. Cisco VPN 클라이언트 소프트웨어는 어디에서 다운로드할 수 있습니까?

A. Cisco VPN 클라이언트 소프트웨어에 액세스하려면 로그인하고 유효한 서비스 계약을 보유해야 합니다.Cisco VPN Client 소프트웨어는 Cisco Download Software(등록된 고객만 해당) 페이지에서 다운로드할 수 있습니다.**Cisco.com 프로필과 연결된 유효한 서비스 계약이 없는 경우 로그인하고 VPN 클라이언트 소프트웨어를 다운로드할 수 없습니다.**

유효한 서비스 계약을 얻으려면 다음을 수행할 수 있습니다.

- 직접 구매 계약이 있는 경우 Cisco 어카운트 팀에 문의하십시오.
- 서비스 계약을 구매하려면 Cisco 파트너 또는 리셀러에게 문의하십시오.
- Cisco.com 프로필을 업데이트하고 서비스 계약에 대한 연결을 요청하려면 Profile Manager(등록된 고객만)를 사용합니다.

Q. Cisco VPN Client 다운로드 영역이 비어 있는 것 같습니다.왜?

A. 소프트웨어 센터의 VPN 클라이언트 영역(등록된 고객만)에 도달하는 경우 페이지 중간에 원하는 운영 체제에 대한 다운로드 영역을 선택해야 합니다.

Q. Cisco VPN 클라이언트를 설치하는 동안 상태 저장 방화벽 기능을 비활성화하려면 어떻게 해야 합니까?

A. 5.0 이전 VPN 클라이언트 버전의 경우:

"MSI를 사용하여 Windows VPN Client without Stateful Firewall 설치" 및 "InstallShield를 사용하여 Windows VPN 클라이언트를 Stateful Firewall 없이 설치"와 같은 두 항목에 대해 알아보려면 VPN Client Rel 4.7 릴리스 정보의 Documentation Changes 섹션을 참조하십시오.

5.0 이후 VPN 클라이언트 버전의 경우:

Cisco VPN Client 릴리스 5.0.3.0560부터 방화벽 파일에 길드 설치를 방지하기 위해 MSI 설치 플래그가 추가되었습니다.

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

이 내용에 대한 자세한 내용은 상태 저장 방화벽이 필요하지 않을 때 방화벽 파일 설치 우회 섹션을 참조하십시오.

Q. Cisco VPN 클라이언트를 제거하거나 업그레이드하려면 어떻게 해야 합니까?

A. Windows 2000 및 Windows XP의 경우 수동으로 설치(InstallShield)한 다음 Cisco VPN Client Version 3.5 이상을 업그레이드하는 방법에 대한 자세한 내용은 MSI 설치 프로그램과 함께 설치된 VPN 클라이언트 버전 제거를 참조하십시오.

Windows 2000 및 Windows XP용 Cisco VPN Client 소프트웨어는 알림을 제공할 수 있는 VPN 3000 Concentrator 또는 기타 VPN 서버에서 터널을 통해 자동으로 업데이트와 새 버전을 안전하게 다운로드할 수 있습니다.자동 업데이트 기능을 사용하려면 원격 사용자가 PC에 Windows 4.6 이상의 VPN 클라이언트를 설치해야 합니다.

자동 업데이트 기능을 사용하면 사용자는 이전 버전의 소프트웨어를 제거하고 재부팅하고 새 버전을 설치한 다음 다시 재부팅할 필요가 없습니다.대신 관리자는 웹 서버에서 업데이트 및 프로파일을 사용할 수 있게 하고 원격 사용자가 VPN 클라이언트를 시작하면 소프트웨어가 다운로드가 사용 가능한 것을 감지하여 자동으로 가져옵니다.자세한 내용은 자동 업데이트 관리 및 자동 업데이트 작동 방식을 참조하십시오.

ASDM을 사용하여 Cisco ASA Series 5500 Adaptive Security Appliance에서 클라이언트 업데이트를 구성하는 방법에 대한 자세한 내용은 ASDM을 사용하여 클라이언트 소프트웨어 업데이트 구성을 참조하십시오.

Q. Vista용 VPN 클라이언트를 사용자 지정하려고 합니다.Vista용 새 VPN 클라이언트 버전에는 oem.mst와 같은 파일이 없다는 것을 알고 있습니다.새 VPN 클라이언트 버전(5.x)을 사용자 정의하거나 이 파일을 찾을 수 있는 위치를 지정하려면 어떻게 해야 합니까?

A. MST 파일은 더 이상 VPN 클라이언트와 함께 제공되지 않지만 소프트웨어 다운로드(등록된 고

객만 해당) 페이지에서 다운로드할 수 있습니다.

파일 이름:국제 버전의 Windows에 설치하는 Readme 및 MST

운영 체제

Q. Cisco는 Windows Vista용 VPN 클라이언트를 제공합니까?

A. 새로운 Cisco VPN Client 5.0.07 릴리스는 x86(32비트) 및 x64에서 모두 Windows Vista를 지원합니다. 자세한 내용은 5.0.07.0240 릴리스 정보를 참조하십시오.

참고: Cisco VPN Client는 Windows Vista 클린 설치에서만 지원됩니다. 즉, 모든 Windows 운영 체제를 Windows Vista로 업그레이드하는 것은 VPN 클라이언트 소프트웨어에서 지원되지 않습니다.Windows Vista를 새로 설치한 다음 Vista VPN 클라이언트 소프트웨어를 설치해야 합니다.

참고: Cisco.com 프로필과 연결된 유효한 서비스 계약이 없는 경우 로그인하고 VPN 클라이언트 소프트웨어를 다운로드할 수 없습니다.자세한 내용은 VPN 클라이언트 소프트웨어 다운로드를 참조하십시오.

팁: Cisco AnyConnect VPN Client는 이제 Vista 32 및 64비트를 포함하는 Windows 운영 체제에 사용할 수 있습니다.AnyConnect 클라이언트는 SSL 및 DTLS를 지원합니다.현재는 IPsec을 지원하지 않습니다.또한 AnyConnect는 버전 8.0(2) 이상을 실행하는 Cisco ASA에서만 사용할 수 있습니다.버전 12.4(15)T를 실행하는 IOS 어플라이언스에서 웹 실행 모드에서도 클라이언트를 사용할 수 있습니다.VPN 3000은 지원되지 않습니다.

Cisco AnyConnect VPN Client 및 ASA 8.0은 Software Center에서 가져올 수 있습니다(등록된 고객만 해당). AnyConnect 클라이언트에 대한 자세한 내용은 Cisco AnyConnect VPN 클라이언트 릴리스 정보를 참조하십시오.ASA 8.0에 대한 자세한 내용은 Cisco ASA 5500 Series Adaptive Security Appliances 릴리스 정보를 참조하십시오.

참고: Cisco.com 프로필과 연결된 유효한 서비스 계약이 없는 경우 AnyConnect VPN Client 또는 ASA 소프트웨어를 로그인하여 다운로드할 수 없습니다. 자세한 내용은 VPN 클라이언트 소프트웨어 다운로드를 참조하십시오.

Q: Microsoft Windows PC에서 PPTP 연결을 설정하려면 어떻게 해야 합니까?

A. 설치 프로그램은 실행하는 Microsoft Windows 버전에 따라 다릅니다.자세한 내용은 Microsoft에 문의하십시오.다음은 Windows의 일부 공통 버전에 대한 설정 지침입니다.

Windows 95

1. Msdun13.exe를 설치합니다.
2. 프로그램 **> 보조프로그램 > 전화 접속 네트워킹을 선택합니다**.
3. "PPTP"라는 새 연결을 만듭니다.
4. VPN **어댑터**를 연결 디바이스로 선택합니다.
5. 스위치의 공용 인터페이스의 IP 주소를 입력하고 **Finish**를 클릭합니다.
6. 방금 생성한 연결로 돌아가 마우스 오른쪽 단추를 클릭한 다음 **속성**을 선택합니다.
7. Allowed Network Protocols 아래에서 최소한 netbeui의 선택을 **취소합니다**.
8. 고급 **옵션** 설정**을** 구성합니다. 스위치와 클라이언트가 인증 방법을 자동 협상할 수 있도록 기본 설정을 유지합니다.Require **Encrypted Password**(암호화된 비밀번호 필요)를 활성화하여

CHAP(Challenge Handshake Authentication Protocol) 인증을 적용합니다.Require **Encrypted Password(암호화된 비밀번호 필요)**를 활성화하고 **Require Data Encryption(데이터 암호화 필요)**을 사용하여 MS-CHAP 인증을 적용합니다.

Windows 98

1. PPTP 기능을 설치하려면 다음 단계를 완료하십시오. **[시작] > [설정] > [제어판] > [새 하드웨어 추가]**를 선택하고 **다음**을 클릭합니다.Select **from List(목록에서 선택)**를 클릭하고 **Network Adapter(네트워크 어댑터)**를 선택한 다음 **Next(다음)를 클릭합니다**.왼쪽 패널에서 **Microsoft**를 선택하고 오른쪽 패널에서 **Microsoft VPN Adapter**를 선택합니다.
2. PPTP 기능을 구성하려면 다음 단계를 완료합니다. 시작 **> 프로그램 > 보조프로그램 > 통신 > 전화 접속 네트워킹을 선택합니다**.Make **new connection(새 연결 만들기)**을 클릭하고 **Microsoft VPN Adapter** for Select a device(디바이스 선택)를 선택합니다.VPN Server IP address= 3000 터널 엔드포인트입니다.
3. PAP(Password Authentication Protocol)를 허용하도록 PC를 변경하려면 다음 단계를 완료하십시오. **참고:** Windows 98 기본 인증은 암호 암호화(CHAP 또는 MS-CHAP)를 사용하는 것입니다.Properties **> Server types를 선택합니다**.Require encrypted password(**암호화된 비밀번호 필요)를 선택 취소합니다**.이 영역에서 데이터 암호화(Microsoft MPPE[Point-to-Point Encryption] 또는 MPPE 없음)를 구성할 수 있습니다.

Windows 2000

1. 시작 **> 프로그램 > 보조프로그램 > 통신 > 네트워크 및 전화 접속 연결을 선택합니다**.
2. Make **new connection(새 연결 만들기)**을 클릭한 다음 **Next(다음)**를 클릭합니다.
3. **인터넷을 통해 사설 네트워크에 연결 및 먼저 연결**을 선택(LAN이 있는 경우 이 옵션을 선택하지 않음)하고 **다음**을 클릭합니다.
4. 터널 엔드포인트(3000)의 호스트 이름 또는 IP 주소를 입력합니다.
5. 비밀번호 유형을 변경해야 하는 경우 **Properties > Security for the connection > Advanced를** 선택합니다.기본값은 MS-CHAP 및 MS-CHAP v2(CHAP 또는 PAP 아님)입니다. 이 영역에서 데이터 암호화(MPPE 또는 MPPE 없음)를 구성할 수 있습니다.

Windows NT

Microsoft 클라이언트 및 서버와 함께 PPTP 설치, 구성 및 사용을 참조하십시오 .

Q. Cisco VPN Client를 지원하는 운영 체제 버전은 무엇입니까?

A. VPN 클라이언트에 대한 추가 운영 체제 지원이 지속적으로 추가됩니다.VPN 클라이언트 5.0.07의 릴리스 노트에서 시스템 요구 사항을 참조하거나 IPsec/PPTP/L2TP를 지원하는 Cisco 하드웨어 및 VPN 클라이언트를 참조하십시오.

참고:

- VPN 클라이언트에는 Windows XP 및 Windows Vista용 듀얼 프로세서 및 듀얼 코어 워크스테이션이 지원됩니다.
- Windows VPN Client Release 4.8.00.440은 Windows 98 운영 체제를 공식적으로 지원하는 최종 버전입니다.
- Windows VPN Client Release 4.6.04.0043은 Windows NT 운영 체제를 공식적으로 지원하는 최종 버전입니다.
- Cisco VPN Client 버전 5.0.07은 x86(32비트) 및 x64(64비트) 버전 모두에서 Windows Vista 및 Windows 7을 지원합니다.

- Cisco VPN Client는 Windows XP 32비트만 지원하지만 Windows XP 64비트는 지원되지 않습니다.**참고:** Windows Vista 32비트 지원은 모든 5.x 릴리스에서 제공되었습니다.Cisco VPN 클라이언트 버전 5.0.07은 64비트 지원을 추가했습니다.

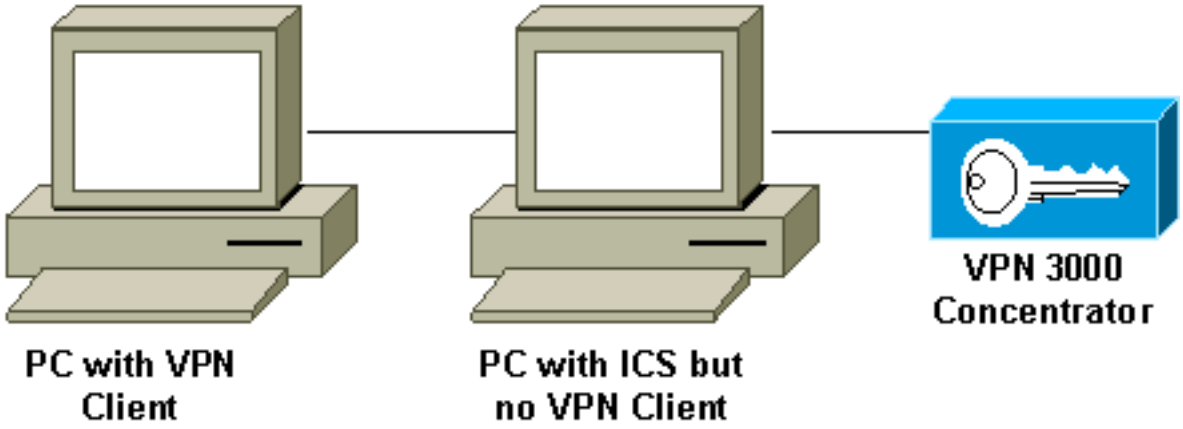
Q. VPN 클라이언트를 로드하려면 Windows NT/2000 시스템의 관리자가 되어야 합니까?

A. 예. 이러한 운영 체제에는 기존 네트워크 드라이버에 바인딩하거나 새 네트워크 드라이버를 설치하려면 관리자 권한이 필요하므로 Windows NT 및 Windows 2000에 VPN 클라이언트를 설치하려면 관리자 권한이 있어야 합니다.VPN 클라이언트 소프트웨어는 네트워킹 소프트웨어입니다.설치하려면 관리자 권한이 있어야 합니다.

Q. Cisco VPN Client는 동일한 시스템에 설치된 Microsoft ICS(Internet Connection Sharing)와 연동할 수 있습니까?

A. 아니요. Cisco VPN 3000 Client는 동일한 시스템의 Microsoft ICS와 호환되지 않습니다.VPN 클라이언트를 설치하려면 먼저 ICS를 제거해야 합니다.자세한 내용은 Microsoft Windows XP에서 Cisco VPN Client 3.5.x 설치 또는 업그레이드를 준비할 때 ICS 비활성화를 참조하십시오.

동일한 PC에 VPN 클라이언트와 ICS를 사용하는 것은 작동하지 않지만 이 방식은 작동합니다.



Q. 내 VPN 클라이언트는 특정 주소에만 연결되는 것 같습니다.Windows XP를 실행합니다.어떻게 해야 합니까?

A. Windows XP의 기본 제공 방화벽이 비활성화되었는지 확인합니다.

Q. Cisco VPN Client는 Windows XP 스테이트풀 방화벽과 호환됩니까?

A. 이 문제가 해결되었습니다.자세한 내용은 Bug Toolkit에서 Cisco Bug ID CSCdx15865(등록된 고객만)를 참조하십시오.

Q. Windows XP 및 Windows 2000에 VPN 클라이언트를 설치할 때 다중 사용자 인터페이스가 비활성화됩니까?

A. 설치 시 시작 화면과 빠른 사용자 전환이 비활성화됩니다.자세한 내용은 Bug Toolkit에서 Cisco Bug ID CSCdu24073(등록된 고객만)을 참조하십시오.

Q. 실행 후 Linux용 VPN 클라이언트를 백그라운드로 이동하려면 어떻게 해야 합니까?vpnclient connect foo와 같은 연결을 시작하면 로그인하지만 셸이 반환됩니다.

A. 로그온한 후 다음을 입력합니다.

- **^Z**
- **브루노**

Q. Windows XP Home Edition에 Cisco VPN 클라이언트를 설치하면 작업 표시줄이 표시되지 않습니다.어떻게 취소합니까?

A. **[제어판] > [네트워크 연결] > [네트워크 브리지 제거]**를 선택하여 이 설정을 조정합니다.

Q. RedHat 8.0에 Linux VPN Client를 설치하려고 할 때 모듈이 GCC 2로 컴파일되고 커널이 GCC 3.2로 컴파일되었으므로 모듈을 로드할 수 없다는 오류가 발생합니다. 어떻게 해야 합니까?

A. RedHat의 새 릴리스에 최신 버전의 GCC 컴파일러(3.2 이상)가 있어 현재 Cisco VPN 클라이언트가 실패하기 때문입니다.이 문제는 해결되었으며 Cisco VPN 3.6.2a에서 사용할 수 있습니다.자세한 내용은 Bug Toolkit에서 Cisco Bug ID CSCdy49082(등록된 고객만)를 보거나 VPN Software Center(등록된 고객만 해당)에서 소프트웨어를 다운로드합니다.

Q. Windows XP에 VPN 클라이언트 3.1을 설치할 때 소프트웨어에서 빠른 사용자 스위칭을 비활성화하는 이유는 무엇입니까?

A. Microsoft는 레지스트리에 GINA.dll이 지정되어 있으면 Windows XP에서 빠른 사용자 전환을 자동으로 비활성화합니다.Cisco VPN Client는 CSgina.dll을 설치하여 "로그인 전 시작" 기능을 구현합니다.빠른 사용자 전환이 필요한 경우 "로그인 전 시작" 기능을 비활성화합니다.등록된 사용자는 Bug Toolkit에서 Cisco Bug ID CSCdu24073(등록된 고객만)에서 자세한 정보를 얻을 수 있습니다.

Q. IPsec VPN 클라이언트는 Windows 7에서 SBL(Start Before Logon) 기능을 지원합니까?

A. SBL 기능은 Windows7의 IPsec VPN 클라이언트에서 지원되지 않습니다. AnyConnect VPN 클라이언트에서 지원됩니다.

오류 메시지

Q. Cisco VPN Client 4.x를 설치하면 다음 오류 메시지가 표시됩니다. **201: VPN . VPN .**

A. 이 문제는 VPN 클라이언트 컴퓨터에 설치된 방화벽 패키지로 인해 발생할 수 있습니다.이 오류 메시지를 방지하려면 설치 시 PC에 방화벽이나 안티바이러스 프로그램이 설치되지 않았거나 실행되고 있지 않은지 확인하십시오.

Q. Mac OS X 10.3("Pander"라고 함)으로 업그레이드했지만 이제 Cisco VPN Client 4.x에 다음 오류 메시지가 표시됩니다. **VPN . .**

A. UseLegacyIKEPort=0을 Mac OS X 10.3("Pander")에서 작동하려면 Cisco VPN Client 4.x의 /etc/CiscoSystemsVPNClient/Profiles/ 디렉토리에 있는 프로파일(.pcf 파일)에 추가해야 합니다.

Q. VPN 클라이언트를 제거하려고 하면 다음 오류 메시지가 표시됩니다. : ...이 오류 메시지는 무엇을 의미하며 제거를 성공적으로 완료하려면 어떻게 해야 합니까?

A. 네트워킹 제어판을 확인하여 Deterministic NDIS Extender(DNE)가 설치되지 않았는지 확인하십시오.또한 **Microsoft > Current Version > Uninstall**을 선택하여 제거 파일을 확인합니다 .HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ **{5624C000-B109-11D4-9DB4-00E0290FCAC5}** 파일을 제거하고 제거를 다시 시도하십시오.

Q. Windows 2000 Professional에는 VPN 클라이언트를 설치할 수 없습니다.다음 오류가 표시됩니다. .심각한 장애.어떻게 해야 합니까?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall 키를 제거합니다.그런 다음 컴퓨터를 재부팅하고 VPN 클라이언트를 다시 설치합니다.

참고: Cisco VPN Client 소프트웨어의 올바른 키를 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*key to be determined*> 경로에서 찾으려면 HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\으로 이동한 다음 **VPN Client**를 클릭합니다.오른쪽 창에서 Name(이름) 열 아래의 Uninstall Path(제거 경로)를 확인합니다. 해당 Data(데이터) 열에는 VPN 클라이언트 키 값이 표시됩니다.이 키를 기록하고 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\으로 이동하여 확인된 키를 선택한 다음 삭제합니다.

자세한 내용은 초기화 오류 문제 해결 을 참조하고 버그 툴킷의 Cisco 버그 ID CSCdv15391(등록된 고객만)을 참조하십시오.

Q. RedHat 8.0에 Linux VPN Client를 설치하려고 할 때 모듈이 GCC 2로 컴파일되고 커널이 GCC 3.2로 컴파일되었으므로 모듈을 로드할 수 없다는 오류 메시지가 표시됩니다. 어떻게 해야 합니까?

A. 이 문제는 RedHat의 새 릴리스에 최신 버전의 GCC 컴파일러(3.2 이상)가 있어 현재 Cisco VPN Client가 실패하기 때문에 발생합니다.이 문제는 해결되었으며 Cisco VPN 3.6.2a에서 사용할 수 있습니다.자세한 내용은 Bug Toolkit에서 Cisco 버그 ID CSCdy49082(등록된 고객만)를 보거나 VPN Software Center(등록된 고객만)에서 소프트웨어를 다운로드합니다.

Q. Linux Client 3.5에서 PIX 또는 VPN 3000 Concentrator에 대한 IPsec 연결을 설정하려고 시도할 때 "피어가 더 이상 응답하지 않음" 오류 메시지가 나타납니다.어떻게 해야 합니까?

A. 이 문제의 원인은 Linux 클라이언트가 연결을 시도하는 것처럼 보이지만 게이트웨이 장치에서 응답을 받지 못한다는 것입니다.

Linux OS에는 UDP 포트 500, UDP 포트 1000 및 ESP(Encapsulating Security Payload) 패킷을 차단하는 내장형 방화벽(ipchains)이 있습니다.방화벽이 기본적으로 켜져 있으므로 문제를 해결하려면 방화벽을 비활성화하거나 인바운드 및 아웃바운드 연결 모두에 대해 IPsec 통신을 위한 포트를 열어야 합니다.

Q. Mac OS X 10.3에서 Cisco VPN 5000 5.2.2 Client를 실행하려고 하면 커널 확장

오류가 발생합니다. 어떻게 해야 합니까?

A. 제품 릴리스 정보에 명시된 대로 Cisco VPN 5000 클라이언트는 최대 버전 10.1.x까지 지원되므로 버전 10.3에서는 지원되지 않습니다. 설치 스크립트를 실행한 후 설치된 두 파일에 대한 권한을 재설정하면 VPN 클라이언트가 작동할 수 있습니다.예를 들면 다음과 같습니다.

참고: 이 컨피그레이션은 Cisco에서 지원하지 않습니다.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. 새 버전의 Cisco VPN Client를 설치할 수 없습니다.설치 시 다음 오류 메시지 중 하나가 표시됩니다."DNE DNEinst . -2146500093" 또는 "InstallDNE :DNE DNEinst . -2147024891." 이 문제는 Deterministic Network Enhancer를 설치할 때 발생합니다.

A. Deterministic Networks에서 최신 DNE 업그레이드를 설치합니다 .

Q. 연결을 할 때 Cisco VPN Client에 대한 로그를 가져옵니다.

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

A. 이 메시지는 상당히 일반적인 오류 메시지로, 일반적으로 클라이언트를 수동으로 제거해야 합니다.이 링크의 지침을 따릅니다.MSI 설치 프로그램과 함께 설치된 VPN 클라이언트 버전을 제거하는 중입니다.

제거를 완료했으면 재부팅해야 합니다.그런 다음 클라이언트를 다시 설치합니다.로컬 컴퓨터에 관리자 권한이 있는 사용자로 로그온했는지 확인합니다.

Q. Mac OS에서 Cisco VPN Client를 연결하려고 하면 다음 오류 메시지가 표시됩니다. 51 - VPN .이 문제를 어떻게 해결할 수 있습니까?

A. 다음과 같이 VPN 클라이언트를 닫은 후 서비스를 다시 시작하면 이 문제를 해결할 수 있습니다.

중지하려면

```
sudo kextunload -b com.cisco.nke.ipsec
```

시작하려면 다음을 수행합니다.

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

또한 VPN 클라이언트가 설치된 동일한 시스템에서 실행 중인 다음 항목을 확인하고 이를 비활성화합니다.

- 모든 가상 소프트웨어(예: VMWare Fusion, Parallels, crossovers).

- 모든 안티바이러스/방화벽 소프트웨어
- VPN 클라이언트와 64비트 운영 체제의 호환성Cisco VPN Client 릴리스 정보를 참조하십시오.

Q. "이유 442:가상 어댑터를 사용하도록 설정하지 못했습니다." 오류이 오류를 해결하려면 어떻게 해야 합니까?

A. `442:Vista` 중복 IP 주소가 탐지되었다고 보고한 후 를 활성화하지 못했습니다 오류가 나타납니다.후속 연결은 동일한 메시지로 실패하지만 Vista에서는 중복 IP 주소가 탐지되었다고 보고하지 않습니다.이 문제 해결 방법에 대한 자세한 내용은 Windows Vista에서 IP 주소 트리거 오류 442를 참조하십시오.

Q. Cisco VPN 클라이언트를 설치하면 Deterministic `Network Enhancer Add Plugin Failed` 오류 수신됩니다.이 오류는 어떻게 해결됩니까?

A. DNE 어댑터를 설치하면 문제가 해결될 수 있습니다.MSI 대신 Installshield 버전을 설치하는 것이 좋습니다.

Q. 다음 오류가 발생했습니다. `442:` .이 문제를 어떻게 해결할 수 있습니까?

A. 이 오류는 Windows 7과 Windows Vista에서 중복 IP 주소가 탐지된 후 나타납니다.후속 연결은 동일한 메시지로 실패하지만 OS는 중복 IP 주소가 탐지되었다고 보고하지 않습니다.이 문제 해결 방법에 대한 자세한 내용은 Windows 7 및 Vista에서 IP 주소 트리거 오류 442를 참조하십시오.

Q. MAC OS 10.6용 VPN Client 4.9를 실행하려고 하면 다음 오류가 발생합니다. `51:vpn` .이 문제를 해결하는 방법

A. 이 문제는 MAC OS 릴리스 4.9용 Cisco VPN 클라이언트에서 64비트 지원을 사용할 수 없기 때문에 발생합니다. 해결 방법으로 32비트 커널 모드에서 부팅할 수 있습니다.자세한 내용은 Cisco Bug ID CSCth11092(등록된 고객만)와 MAC OSX 릴리스 정보용 Cisco VPN 클라이언트를 참조하십시오.

타사 호환성

Q. Nortel Client는 Cisco VPN 3000 Concentrator와 호환됩니까?

A. 아니요. Nortel 클라이언트가 Cisco VPN 3000 Concentrator에 연결할 수 없습니다.

Q. Nortel Connectivity VPN Client와 함께 다른 공급업체의 VPN 클라이언트를 설치할 수 있습니까?

A. 아니요. 동일한 PC에 여러 VPN 클라이언트가 설치된 경우 알려진 문제가 있습니다.

Q. Cisco VPN 클라이언트는 타사 VPN Concentrator에서 지원됩니까?

A. Cisco VPN 클라이언트는 서드파티 VPN 집중기에서 지원되지 않습니다.

인증

Q. Cisco VPN Clients 버전 1.1 및 3.x는 내부적으로 디지털 인증서(X.509v3)를 어떻게 저장합니까?

A. Cisco VPN Client 1.1에는 자체 인증서 저장소가 있습니다.Cisco VPN Client 3.x는 CAPI(Common-Application Programming Interface)를 사용하여 Microsoft 저장소에 인증서를 저장하거나, Cisco의 자체 저장소(RSA Data Security)에 인증서를 저장할 수 있습니다.

Q. VPN Concentrator에서 동일한 그룹 이름과 사용자 이름을 사용할 수 있습니까?

A. 아니요, 그룹 이름과 사용자 이름은 같을 수 없습니다.이는 소프트웨어 버전 2.5.2 및 3.0에서 발견되고 3.1.2에 통합된 알려진 문제입니다. 자세한 내용은 버그 툴킷에서 Cisco 버그 ID CSCdw29034(등록된 고객만)를 참조하십시오.

Q: Defender와 같은 전체 챌린지 카드는 Cisco VPN 클라이언트에서 PIX로 지원됩니까?

A. 아니요. 이 유형의 카드는 지원되지 않습니다.

VPN 클라이언트 소프트웨어 버전

Q. Cisco VPN Client 버전 2.5.2 이전 버전의 "MTU 유틸리티 설정" 옵션은 어떻게 되었습니까?

A. Cisco VPN Client가 이제 MTU(Maximum Transmission Unit) 크기를 조정합니다.MTU 유틸리티 설정 옵션은 더 이상 필수 설치 단계가 아닙니다.Set MTU 옵션은 주로 연결 문제를 해결하는 데 사용됩니다.Windows 시스템의 SetMTU 옵션을 선택하는 경로는 Start(시작) **> Programs(프로그램) > Cisco Systems VPN Client(Cisco Systems VPN 클라이언트) > SetMTU입니다**.SetMTU 옵션 및 다른 운영 체제에서 이 옵션을 설정하는 방법에 대한 자세한 내용은 SetMTU 옵션을 통해 MTU 크기 변경을 참조하십시오.

Q. 4.0 이후 버전의 Cisco VPN Client GUI에서 지원되는 언어는 무엇입니까?

A. Cisco VPN Client GUI 4.0 이상 버전에서 지원되는 언어는 캐나다, 프랑스어 및 일본어입니다.

Q. Cisco VPN Client에서 지원되는 개인 방화벽은 무엇입니까?

A. 더 높은 수준의 보안을 제공하기 위해 VPN 클라이언트는 지원되는 방화벽의 작업을 적용하거나 인터넷 바인딩 트래픽에 대해 푸시된 상태 저장 방화벽 정책을 수신할 수 있습니다.

현재 VPN Client 5.0은 다음과 같은 개인 방화벽을 지원합니다.

- 블랙아이스 디펜더
- Cisco 보안 에이전트
- Sygate 개인 방화벽
- Sygate Personal Firewall Pro
- Sygate 보안 에이전트
- 영역 경보
- 영역 경보 프로

버전 3.1부터 VPN 3000 Concentrator에 새로운 기능이 추가되어 원격 사용자가 설치한 개인 방화벽 소프트웨어를 감지하고 적절한 소프트웨어가 없는 경우 사용자가 연결할 수 없습니다 .Configuration(**구성) > User Management(사용자 관리) > Groups(그룹) > Client FW(클라이언트 FW)**를 선택하고 이 기능을 구성할 그룹의 탭을 클릭합니다.

Cisco VPN 클라이언트 시스템에서 방화벽 정책을 적용하는 방법에 대한 자세한 내용은 방화벽 구성 시나리오를 참조하십시오.

Q. Cisco VPN Client 3.x와 AOL 7.0을 함께 사용할 때 연결 문제가 있습니까?

A. Cisco VPN 클라이언트는 스플릿 터널링을 사용하지 않으면 AOL 7.0에서 작동하지 않습니다.자세한 내용은 Bug Toolkit에서 Cisco 버그 ID CSCdx04842(등록된 고객만)를 참조하십시오.

VPN 클라이언트 소프트웨어 구성

Q. Cisco VPN Client가 30분 후에 연결이 끊기는 이유는 무엇입니까?이 기간을 연장할 수 있습니까?

A. 이 30분 동안 사용자 연결에 대한 통신 활동이 없으면 연결이 종료됩니다.기본 유휴 시간 제한 설정은 30분이며 최소 허용 값은 1분이고 최대 허용 값은 2,147,483,647분(4,000년 이상)입니다.

Configuration(**구성) > User Management(사용자 관리) > Groups(그룹)**를 선택하고 유휴 시간 제한 설정을 수정할 적절한 그룹 이름을 선택합니다.Modify **Group(그룹 수정)**을 선택하고 **HW Client(HW 클라이언트)** 탭을 클릭한 다음 User Idle Timeout(사용자 유휴 시간 제한) 필드에 원하는 값을 입력합니다.시간 제한을 비활성화하고 무제한 유휴 기간을 허용하려면 **0**을 입력합니다.

Q. Cisco VPN Client를 사전 구성된 모든 매개변수와 함께 구축할 수 있습니까?

A. vpnclient.ini 파일이 처음 설치될 때 VPN 클라이언트 소프트웨어와 함께 번들된 경우 설치 중에 자동으로 VPN 클라이언트를 구성합니다.자동 컨피그레이션을 위해 미리 구성된 연결 프로파일로 프로파일 파일(각 연결 항목에 대해 하나의 .pcf 파일)을 배포할 수도 있습니다.설치를 위해 VPN 클라이언트 소프트웨어의 사전 구성된 사본을 사용자에게 배포하려면 다음 단계를 완료하십시오.

1. 배포 CD-ROM의 VPN 클라이언트 소프트웨어 파일을 vpnclient.ini(전역) 파일을 생성한 각 디렉터리와 사용자 집합에 대한 별도의 연결 프로파일을 복사합니다.**참고:** Mac OS X 플랫폼의 경우 사전 구성된 파일은 VPN 클라이언트를 설치하기 전에 Profiles and Resources 폴더에 배치됩니다.vpnclient.ini 파일은 설치 관리자 디렉토리에 저장됩니다.사용자 지정 vpnclient.ini 파일을 VPN Client Installer 디렉터리에 Profiles and Resources 폴더와 동일한 수준으로 배치해야 합니다.자세한 내용은 Mac OS X용 VPN 클라이언트 사용 설명서의 2장을 참조하십시오.
2. 번들 소프트웨어를 준비하고 배포합니다.CD-ROM 또는 네트워크 배포.vpnclient.ini 파일 및 프로파일 파일이 모든 CD-ROM 이미지 파일과 동일한 디렉토리에 있는지 확인합니다.사용자가 네트워크 연결을 통해 이 디렉터리에서 설치하도록 할 수 있습니다.모든 파일을 배포용 새 CD-ROM에 복사할 수도 있습니다.또는 이 디렉터리의 모든 파일이 포함된 자동 압축 해제 ZIP 파일을 만들어 사용자가 다운로드한 다음 소프트웨어를 설치할 수 있습니다.
3. 사용자에게 기타 필요한 구성 정보 및 지침을 제공합니다.플랫폼에 대한 VPN 클라이언트 사용 설명서의 2장을 참조하십시오.

Q. Cisco VPN Client가 내 NIC 카드와 충돌하는 것 같습니다.이 문제를 어떻게 해결

해야 합니까?

A. NIC 카드에서 최신 드라이버를 실행해야 합니다.항상 권장됩니다.가능하면 운영 체제, PC 하드웨어 및 기타 NIC 카드와 관련된 문제가 있는지 테스트합니다.

Q. 전화 접속 네트워킹에서 Cisco VPN 클라이언트 연결을 어떻게 자동화합니까?

A. VPN 연결에 대한 전화 접속을 완전히 자동화하려면 Options(옵션) > **Properties(속성) > Connections(연결)**를 선택하고 Cisco VPN Client가 전화 접속 네트워킹 전화 번호부 항목을 풀다운하도록 합니다.

Q. 원격 사용자에게 VPN 클라이언트 업데이트를 알리도록 Cisco VPN 3000 Concentrator를 구성하려면 어떻게 해야 합니까?

A. 원격 시스템에서 VPN 클라이언트 소프트웨어를 업데이트할 때 VPN 클라이언트 사용자에게 알릴 수 있습니다.단계별 접근 방식은 원격 사용자에게 클라이언트 업데이트에 대한 알림을 참조하십시오.프로세스의 7단계에서 설명한 대로 릴리스 정보를 "(Rel)"로 입력해야 합니다.

Q. 특히 "로그온 전 시작" 옵션이 활성화된 경우 Cisco VPN 클라이언트가 표시되기 전에 지연될 수 있는 원인은 무엇입니까?

A. Cisco VPN Client가 *폴백 모드에 있습니다.*이는 지연에 기여합니다.대체 모드에서 VPN 클라이언트는 로그온을 사용하기 전에 시작할 때 다르게 수행됩니다.대체 모드에서 작동할 때 VPN 클라이언트는 필요한 Windows 서비스가 시작되었는지 확인하지 않습니다.따라서 너무 빨리 시작되면 VPN 연결이 실패할 수 있습니다.Cisco VPN 클라이언트를 제거하고 "뒤로" 모드에 있지 않은 상태에서 시작할 수 있도록 잘못된 애플리케이션을 제거하십시오.그런 다음 Cisco VPN 클라이언트를 다시 설치합니다.대체 모드에 대한 자세한 내용은 로그온 전 시작을 참조하십시오.

자세한 내용은 Bug Toolkit에서 Cisco 버그 ID CSCdt88922(등록된 고객만) 및 CSCdt55739(등록된 고객만 해당)를 참조하십시오.

Q. ipsecdialer.exe와 vpngui.exe의 차이점을 이해해야 합니다.Windows XP의 STARTUP에 vpngui.exe가 설치된 이유는 무엇입니까? 하지만 회사 리소스에 도달하려면 ipsecdialer를 수동으로 시작해야 합니까?그리고 (크기와 별개로) 이러한 프로그램은 같은 것을 트리거하는 것처럼 보입니다.회사 네트워크에 대한 VPN 로그온입니다.

A. ipsecdialer.exe는 Cisco VPN Client 버전 3.x의 원래 실행 메커니즘입니다.4.x 버전에서 GUI를 변경하면 vpngui.exe라는 새 실행 파일이 생성되었습니다.ipsecdialer.exe 파일은 이전 버전과의 호환성을 위해서만 이름으로 전달되었으며 vpngui.exe만 실행합니다.이것이 파일 크기의 차이를 확인할 수 있는 이유입니다.

따라서 Cisco VPN Client 버전 4.x에서 버전 3.x로 다운그레이드할 경우 ipsecdialer.exe 파일을 사용하여 이 파일을 시작해야 합니다.

Q. 시작 VPN 아이콘을 안전하게 제거할 수 있습니까?필요한 이유

A. 시작 폴더의 Cisco VPN 클라이언트는 "로그온 전 시작" 기능을 지원합니다.이 기능을 사용하지 않으면 시작 폴더에 이 기능이 필요하지 않습니다.

Q. ipsecdialer.exe 바로 가기에 "user_logon"이 추가되고 추가되지 않은 이유는 무엇입니까?"사용자 로그온"의 목적은 무엇입니까?

A. "로그온 전 시작" 기능을 사용하려면 "user_logon"이 필요하지만 사용자가 Cisco VPN 클라이언트를 정상적으로 실행해도 이 기능이 필요하지 않습니다.

NAT/PAT 문제

Q. PAT(Port Address Translation) 디바이스를 통해 연결할 수 있는 VPN 클라이언트(릴리스 3.3 이하)가 하나뿐이어서 문제가 발생했습니다.이 문제를 해결하기 위해 어떻게 해야 합니까?

A. 1024 미만의 포트가 변환되지 않도록 하는 여러 NAT(Network Address Translation)/PAT 구현에 버그가 있습니다.Cisco VPN Client 3.1에서 NAT 투명성이 활성화된 경우에도 ISAKMP(Internet Security Association and Key Management Protocol) 세션에서는 UDP 512를 사용합니다. 첫 번째 VPN 클라이언트는 PAT 디바이스를 통과하고 소스 포트 512를 외부에 유지합니다.두 번째 VPN 클라이언트가 연결되면 포트 512가 이미 사용 중입니다.시도가 실패합니다.

해결 방법은 세 가지가 있습니다.

- PAT 디바이스를 수정합니다.
- VPN 클라이언트를 3.4로 업그레이드하고 TCP 캡슐화를 사용합니다.
- 모든 VPN 클라이언트를 대체하는 VPN 3002를 설치합니다.

Q. 두 랩톱을 동일한 위치에서 Cisco VPN Client에 연결할 수 있습니까?

A. 두 클라이언트가 SOHO 라우터/방화벽과 같은 PAT를 수행하는 디바이스 뒤에 있지 않으면 동일한 위치에서 동일한 헤드엔드에 연결할 수 있습니다.많은 PAT 디바이스는 ONE VPN 연결을 그 뒤에 있는 클라이언트에 매핑할 수 있지만 2는 매핑할 수 없습니다.두 개의 VPN 클라이언트가 PAT 디바이스 뒤의 동일한 위치에서 연결하도록 허용하려면 헤드엔드에서 NAT-T, IPSec over UDP 또는 IPsec over TCP와 같은 일종의 캡슐화를 활성화합니다.일반적으로 NAT 디바이스가 클라이언트와 헤드엔드 사이에 있는 경우 NAT-T 또는 다른 캡슐화를 활성화해야 합니다.

기타

Q. 랩톱을 사용하여 사무실의 네트워크에 연결한 다음 노트북을 집에 가져가면 집에서 VPN 3000 Concentrator에 연결하는 데 문제가 있습니다.뭐가 문제죠?

A. 랩톱에서 LAN 연결에서 라우팅 정보를 유지할 수 있습니다.이 문제를 해결하는 방법에 대한 자세한 내용은 Microsoft 라우팅 문제가 있는 VPN 클라이언트를 참조하십시오.

Q. VPN 클라이언트가 VPN Concentrator에 연결되어 있는지 어떻게 알 수 있습니까?

A. HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished이라는 레지스트리 키를 확인하십시오.터널이 활성 상태이면 값은 1입니다. 터널이 없는 경우 값은 0입니다.

Q. VPN Concentrator의 뒤에 있는 PC에서 VPN 클라이언트로 NetMeeting 연결에 문제가 있지만 VPN Concentrator 뒤에 있는 PC에서 VPN 클라이언트로 연결할 때 연결이 작동합니다.이를 해결하려면 어떻게 해야 합니까?

A. 연결 설정을 제어하려면 여기에 나열된 해당 단계를 따릅니다.

- PC의 기본 드라이브에서 **Program Files > Cisco Systems > VPN Client > Profiles**를 선택합니다.사용하는 프로파일을 마우스 오른쪽 단추로 클릭하고 **열기**를 선택하여 텍스트 편집기(예: 메모장)에서 프로파일을 엽니다.사용할 프로그램을 선택할 때 **항상 이 프로그램을 사용하여 이 파일을 열라는** 상자**의 선택을 취소해야 합니다**. ForcekeepAlives에 대한 프로필 매개 변수를 찾아 값을 0에서 1으로 변경한 다음 프로필을 저장합니다.또는
- VPN 클라이언트의 경우 **Options > Properties > General**을 선택하고 이 샘플 창에 표시된 대로 "Peer response timeout" 값을 입력합니다.시간 초과 민감도를 30초~480초로 지정할 수 있습니다.또는
- VPN Concentrator의 경우 Configuration(구성) **> User Management(사용자 관리) > Groups(그룹) > *modify group(그룹 수정)*을** 선택합니다.이 샘플 창에 표시된 대로 IPsec 탭에서 IKE Keepalive에 대한 옵션을 선택합니다.

DPD(Dead Peer Detection) 간격은 감도 설정에 따라 달라집니다.응답이 수신되지 않으면 더 적극적인 모드로 전환되고 피어 응답 임계값이 충족될 때까지 5초마다 패킷을 전송합니다.이때 연결이 끊깁니다.keepalive를 비활성화할 수 있지만 연결이 실제로 끊기면 시간 제한을 기다려야 합니다.처음에는 감도 값을 매우 낮게 설정하는 것이 좋습니다.

Q. Cisco VPN Client는 이중 인증을 지원합니까?

A. 아니요. 이중 인증은 Cisco VPN 클라이언트에서 지원되지 않습니다.

Q. Cisco VPN Client가 적극적인 모드가 아닌 주 모드로 연결되도록 구성하려면 어떻게 해야 합니까?

A. Cisco VPN Client가 주 모드로 연결되도록 하려면 디지털 서명(인증서)을 사용해야 합니다.이를 위해 다음 두 가지 방법이 있습니다.

1. 라우터와 모든 Cisco VPN 클라이언트의 서드파티 인증서 공급자(예: Verisign 또는 Entrust)로부터 CA 인증서를 가져옵니다.동일한 CA 서버에서 ID 인증서를 등록하고 Cisco VPN Client와 라우터 간의 인증 방법으로 디지털 서명을 사용합니다.이 컨피그레이션에 대한 자세한 내용은 Configuring IPSec Between Cisco IOS Routers and Cisco VPN Client Using Entrust Certificates를 참조하십시오.
2. 두 번째 옵션은 원격 액세스 VPN의 헤드엔드와 함께 라우터를 CA 서버로 구성하는 것입니다.인증서(및 기타 모든 항목)를 설치하는 경우 라우터가 CA 서버로 작동한다는 점을 제외하고 이전 링크에서 설명한 대로 유지됩니다.자세한 내용은 허브 컨피그레이션 예에서 IOS CA를 사용하는 Cisco IOS 라우터 간 동적 LAN-to-LAN VPN을 참조하십시오.

Q. VPN 클라이언트 액세스 파일의 필수 매개변수를 읽기 전용으로 설정하려면 어떻게 해야 합니까?

A. 각 사용자에 대해 .pcf 파일의 각 매개변수 앞에 느낌표(!)를 추가하여 매개변수를 읽기 전용으로 설정합니다.

느낌표(!)로 시작하는 매개 변수의 값은 VPN 클라이언트의 사용자가 변경할 수 없습니다.GUI 내의 이러한 값에 대한 필드는 회색으로 표시됩니다(읽기 전용).

다음은 샘플 컨피그레이션입니다.

원본 .pcf 파일

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
             1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

변경된 .pcf 파일

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

이 예에서 사용자는 *Description*, *Host*, GroupName 및 *Username* 값을 변경할 수 없습니다.

Q. MAC 주소를 기반으로 VPN 클라이언트에 대한 액세스를 제한/제한할 수 있습니까?

A. 아니요. MAC 주소를 기반으로 VPN 클라이언트에 대한 액세스를 제한/제한할 수 없습니다.

관련 정보

- Cisco VPN 3000 클라이언트 지원 페이지
- Cisco VPN 클라이언트 지원 페이지
- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- 기술 지원 및 문서 – Cisco Systems