# Cisco VPN 3000 Concentrator FAQ

## 목차



## 소개

이 문서에서는 Cisco VPN 3000 Series Concentrator에 대한 FAQ(자주 묻는 질문)에 대해 설명합니다.

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

## 일반

### Q. 오류 메시지 " 손실"은 무엇을 의미합니까?

**A.** 일정 기간 VPN Concentrator와 VPN 클라이언트 간에 전송된 트래픽이 없는 경우 DPD(Dead Peer Detection) 패킷이 VPN Concentrator에서 VPN 클라이언트로 전송되어 피어가 계속 있는지 확인합니다.VPN Client가 VPN Concentrator에 응답하지 않는 두 피어 간에 연결 문제가 발생할 경우 VPN Concentrator는 일정 기간 동안 DPD 패킷을 계속 전송합니다.그러면 터널이 종료되고 해당 시간 동안 응답을 받지 못할 경우 오류가 생성됩니다.Cisco 버그 ID CSCdz45586(지원 계약 필요)을 참조하십시오.

오류는 다음과 같이 표시됩니다.

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

**원인:**원격 IKE 피어가 예상 기간 내에 keepalive에 응답하지 않아 IKE 피어에 대한 연결이 삭제되었습니다.메시지에 사용된 연결 유지 메커니즘이 포함되어 있습니다.이 문제는 활성 터널 세션 동안 공용 인터페이스의 연결이 끊어진 경우에만 재발생할 수 있습니다.고객은 잠재적인 네트워크 연결 문제의 근본 원인을 정확하게 파악하기 위해 이러한 이벤트가 생성되므로 네트워크 연결을 모니터링해야 합니다.

문제가 발생하는 클라이언트 PC에서 **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles**로 이동하여 IKE keepalive를 비활성화하고 연결에 대한 **PCF 파일**(해당되는 경우)을 편집합니다.

'ForceKeepAlives=0'(기본값)을 'ForceKeepAlives**=1'로** 변경합니다.

문제가 계속되면 Cisco 기술 지원을 통해 서비스 요청을 열고 문제가 발생하면 클라이언트 "로그 뷰어" 및 VPN Concentrator 로그를 제공합니다.

## Q. EMQ1 대기열에 대해 탐지된 오류 메시지 "q_send" 오류는 무엇을 의미합니까?

**A.** 이 오류 메시지는 버퍼에 디버그 이벤트/정보가 너무 많을 때 발생합니다.이벤트 메시지를 몇 개 손실하는 것 외에는 부정적인 영향을 미치지 않습니다.메시지를 방지하는 데 필요한 최소 수로 이벤트를 줄여 보십시오.

## Q. 삭제된 그룹은 VPN Concentrator 컨피그레이션에 계속 표시됩니다.이를 삭제하려면 어떻게 해야 합니까?

**A.** 구성을 텍스트 편집기(예: 메모장)에 복사하고 **[ipaddrgrouppool #.0]**로 표시된 영향을 받는 그룹 정보를 수동으로 편집하거나 삭제합니다.컨피그레이션을 저장하고 VPN Concentrator에 업로드합니다.여기에 예시가 나와 있습니다.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

## Q. 여러 개의 기본 SDI 서버가 있을 수 있습니까?

**A.** VPN 3000 Concentrator는 한 번에 하나의 노드 비밀 파일만 다운로드할 수 있습니다.SDI Version pre-5.0에서 여러 SDI 서버를 추가할 수 있지만 모두 동일한 노드 암호 파일을 공유해야 합니다(기본 및 백업 서버로 간주함). SDI 버전 5.0에서는 하나의 기본 SDI 서버(백업 서버가 노드 암호 파일에 나열됨) 및 복제본 서버만 입력할 수 있습니다.

## Q. "SSL 가 28 " 발급자 오류 메시지가 표시됩니다.어떻게 해야 합니까?

**A.** 메시지는 SSL(Secure Socket Layer) 인증서가 28일 후에 만료됨을 나타냅니다.이 인증서는 HTTPS를 통해 웹 관리를 검색하는 데 사용됩니다.인증서를 기본 설정으로 남겨두거나 새 인증서를 생성하기 전에 다른 옵션을 구성할 수 있습니다.Configuration **> System > Management Protocols > SSL을 선택하여** 이 작업을 수행합니다.Administration(**관리) > Certificate Management(인증서 관리**)를 선택하고 **Generate(생성)를** 클릭하여 인증서를 갱신합니다.

VPN Concentrator의 보안에 대해 우려하며 무단 액세스를 방지하려면 Configuration(컨피그레이션) > Policy Management(정책 관리) **> Traffic Management(트래픽 관리) > Filters(필터)**로 이동하여 공용 인터페이스에서 HTTP 및/또는 HTTPS를 비활성화하십시오.HTTP 또는 HTTPS를 통해 인터넷을 통해 VPN Concentrator에 액세스해야 하는 경우 **Administration(관리) > Access Rights(액세스 권한) > Access Control List(액세스 제어 목록)**로 이동하여 소스 주소를 기반으로 액세스를 지정할 수 있습니다.자세한 내용은 창의 오른쪽 상단에 있는 도움말 메뉴를 참조하십시오.

## Q: 내부 사용자 데이터베이스에서 사용자 정보를 보려면 어떻게 해야 합니까?구성 파일을 볼 때는 표시되지 않습니다.

**A.** Administration(관리) **> Access Rights(액세스 권한) > Access Settings(액세스 설정)를 선택하고** Config **File Encryption=None(구성 파일 암호화=**없음)을 선택한 다음 컨피그레이션을 저장하여 사용자 및 암호를 봅니다.특정 사용자를 검색할 수 있어야 합니다.

## Q. 내부 데이터베이스를 저장할 수 있는 사용자는 몇 명입니까?

**A.** 사용자 수는 버전에 따라 다르며 VPN 3000 Concentrator 릴리스에 대한 사용 설명서의 Configuration(컨피그레이션) **> User Management(사용자 관리)** 섹션에 지정됩니다.VPN 3000 릴리스 2.2부터 2.5.2까지 총 100명의 사용자 또는 그룹(사용자 및 그룹의 합계가 100 이하여야 함)이 가능합니다. VPN 3000 릴리스 3.0 이상에서는 3005 및 3015 Concentrator의 수가 100으로 유지됩니다. VPN 3030 및 302020의 경우 숫자는 500이고, VPN 3060 또는 3080 Concentrator의 경우 번호는 1000입니다.또한 외부 인증 서버를 사용하면 확장성 및 관리 용이성이 향상됩니다.

## Q. 터널 기본 게이트웨이와 기본 게이트웨이의 차이점은 무엇입니까?

**A.** VPN 3000 Concentrator는 터널 기본 게이트웨이를 사용하여 프라이빗 네트워크(대개 내부 라우터)에서 터널링된 사용자를 라우팅합니다. VPN Concentrator는 기본 게이트웨이를 사용하여 패킷을 인터넷(일반적으로 외부 라우터)으로 라우팅합니다.

## Q. VPN 3000 Concentrator를 액세스 제어 목록을 실행하는 방화벽 또는 라우터 뒤에 놓으면 어떤 포트와 프로토콜을 통과하도록 허용해야 합니까?

**A.** 이 차트에는 포트와 프로토콜이 나열됩니다.

| 서비스 | 프로토콜 번호 | 소스 포트 | 대상 포트 |
|---|---|---|---|
| PPTP 제어 연결 | 6(TCP) | 1023 | 1723 |
| PPTP 터널 캡슐화 | 47(GRE) | 해당 없음 | 해당 없음 |
| ISAKMP/IPSec 키 관리 | 17(UDP) | 500 | 500 |
| IPSec 터널 캡슐화 | 50(ESP) | 해당 없음 | 해당 없음 |
| IPSec NAT 투명성 | 17(UDP) | 10000(기본값) | 10000(기본값) |

**참고:** NAT(Network Address Translation) 투명도 포트는 4001~49151 범위의 모든 값으로 구성할 수 있습니다.버전 3.5 이상에서는 Configuration(구성) > System(시스템) **> Tunneling Protocols(터널링 프로토콜) > IPSec > IPSec over TCP로 이동하여 TCP를 통한 IPsec을 구성할 수 있습니다**.최대 10개의 쉼표로 구분된 TCP 포트(1 - 65535)를 입력할 수 있습니다. 이 옵션이 구성된 경우 이러한 포트가 방화벽이나 액세스 제어 목록을 실행하는 라우터에서 허용되는지 확인합니다.

## Q. VPN Concentrator를 공장 기본값으로 다시 설정하려면 어떻게 해야 합니까?

**A.** File Management(파일 관리) 화면에서 "config" 파일을 삭제하고 재부팅합니다.이 파일이 실수로 삭제되면 백업 복사본인 "config.bak"가 유지됩니다.

## Q. 관리 인증에 TACACS+를 사용할 수 있습니까?이 작업을 수행하는 동안 무엇을 기억해야 합니까?

**A.** 예, VPN 3000 Concentrator Release 3.0부터 관리 인증에 TACACS+를 사용할 수 있습니다.TACACS+를 구성한 후 로그아웃하기 전에 인증을 테스트해야 합니다.TACACS+를 잘못 구성하면 잠길 수 있습니다.TACACS+를 비활성화하고 문제를 해결하려면 콘솔 포트 로그인이 필요합니다.

## Q. 관리자 비밀번호를 잊어버린 경우 어떻게 해야 합니까?

**A.** 버전 2.5.1 이상에서는 PC가 설정된 straight-through RS-232 직렬 케이블을 사용하여 PC를 VPN Concentrator의 콘솔 포트에 연결합니다.

- 초당 9600비트
- 8 데이터 비트
- 패리티 없음
- 정지 비트
- 하드웨어 흐름 제어
- VT100 에뮬레이션

VPN Concentrator를 재부팅합니다.진단 검사가 완료되면 콘솔에 3개의 점으로 구성된 줄(...)이 나타납니다.이 점이 표시된 후 3초 이내에 **CTRL-C**를 누릅니다.시스템 비밀번호를 기본값으로 재설정할 수 있는 메뉴가 표시됩니다.

## Q. 그룹 이름 및 그룹 비밀번호의 용도는 무엇입니까?

**A.** 그룹 이름과 그룹 암호는 해시를 만드는 데 사용되며, 해시는 보안 연결을 만드는 데 사용됩니다.

## Q. VPN Concentrator 프록시 ARP는 터널링된 사용자를 대신하여 수행됩니까?

**A.** 네.

## Q. 네트워크 방화벽과 관련하여 VPN 3000 Concentrator는 어디에 배치해야 합니까?

**A.** VPN 3000 Concentrator는 방화벽의 DMZ(demilitarized zone)의 앞, 뒤, 평행 또는 전방에 배치할 수 있습니다.공용 인터페이스와 전용 인터페이스를 동일한 VLAN(virtual LAN)에 사용하는 것은 바람직하지 않습니다.

## Q. Cisco VPN 3000 Concentrator에서 프록시 ARP를 비활성화하는 방법이 있습니까?

**A.** Cisco VPN 3000 Concentrator에서는 ARP(Proxy Address Resolution Protocol)를 비활성화할 수 없습니다.

## Q. VPN 3000 Concentrator에 대해 발생한 버그는 어디에서 찾을 수 있습니까?

**A.** 사용자는 버그 검색 도구(지원 계약 필요)를 사용하여 버그에 대한 자세한 정보를 찾을 수 있습니다.

## Q. VPN 3000 Concentrator의 컨피그레이션 예는 어디에서 찾을 수 있습니까?

**A.** VPN 3000 Concentrator 설명서 외에도 Cisco VPN 3000 Series Concentrator 지원 페이지에서 더 많은 구성 예를 확인할 수 있습니다.

## Q. 특정 이벤트에 대한 더 나은 디버그를 얻기 위해 로깅을 늘리려면 어떻게 해야 합니까?

**A.** Configuration(컨피그레이션) **> System(시스템) > Events(이벤트) > Classes(클래스)로 이동하여** 특정 이벤트(예: IPsec 또는 PPTP)를 구성하여 더 나은 디버그를 얻을 수 있습니다.디버깅은 성능 저하를 일으킬 수 있으므로 문제 해결 연습 기간 동안에만 켜야 합니다.IPsec 디버그의 경우 IKE, IKEDBG, IPSEC, IPSECDBG, AUTH 및 AUTHDBG를 설정합니다.인증서를 사용하는 경우 목록에 CERT 클래스를 추가합니다.

## Q. VPN 3000 Concentrator에 대한 트래픽을 모니터링하려면 어떻게 해야 합니까?

**A.** VPN 3000 Concentrator와 함께 제공되는 HTML 인터페이스를 사용하면 Monitoring(모니터링) **> Sessions(세션)**에서 기본 모니터링 기능을 사용할 수 있습니다.VPN 3000 Concentrator는 SNMP 관리자를 사용하여 SNMP(Simple Network Management Protocol)를 통해 모니터링할 수도 있습니다.또는 Cisco VPN/VMS(Security Management Solution)를 구매할 수도 있습니다. Cisco VMS는 VPN 3000 Concentrator Series를 구축할 때 도움이 되는 주요 기능을 제공하며 IPsec, L2TP 및 PPTP를 기반으로 원격 액세스 및 사이트 간 VPN에 대한 심층적인 모니터링이 필요합니다.VMS에 대한 자세한 내용은 VPN 보안 관리 솔루션을 참조하십시오.

## Q. Cisco VPN 3000 Concentrator Series에 통합 방화벽이 있습니까?그렇다면 어떤 기능이 지원됩니까?

**A.** 이 시리즈에는 스테이트리스 포트/필터링 기능 및 NAT가 통합되어 있지만, Cisco에서는 기업 방화벽에 Cisco Secure PIX Firewall과 같은 디바이스를 사용하는 것이 좋습니다.

## Q. Cisco VPN 3000 Concentrator Series에서 어떤 라우팅 옵션과 VPN 프로토콜을 지원합니까?

**A.** 시리즈는 다음 라우팅 옵션을 지원합니다.

- RIP(Routing Information Protocol)
- RIP2
- OSPF(Open Shortest Path First)
- 고정 경로
- VRRP(Virtual Router Redundancy Protocol)

지원되는 VPN 프로토콜에는 VPN 3000과 최종 클라이언트 간에 NAT 디바이스를 사용하거나 사용하지 않는 IPsec(Point-to-Point Tunneling Protocol), L2TP, L2TP/IPsec 및 IPsec이 포함됩니다.NAT를 통한 IPsec은 NAT 투명도라고 합니다.

## Q. Cisco VPN 3000 Concentrator Series는 클라이언트 PC에 어떤 인증 메커니즘/시스템을 지원합니까?

**A.** NT 도메인, RADIUS 또는 RADIUS 프록시, RSA SDI(Security SecurID), 디지털 인증서 및 내부 인증이 지원됩니다.

## Q. VPN 3000 Concentrator를 통해 나가는 사용자를 위해 고정 NAT(Network Address Translation)를 수행할 수 있습니까?

**A.** 나가는 사용자의 경우 PAT(Port Address Translation)만 수행할 수 있습니다.VPN 3000 Concentrator에서는 고정 NAT를 수행할 수 없습니다.

## Q. VPN 3000 Concentrator를 통해 특정 PPTP(Point-to-Point Tunneling Protocol) 또

## 는 IPsec 사용자에게 고정 IP 주소를 할당하려면 어떻게 해야 합니까?

**A.** 이 목록은 고정 IP 주소를 할당하는 방법에 대해 설명합니다.

- **PPTP 사용자**IP Address Management 섹션에서 풀 또는 DHCP(Dynamic Host Configuration Protocol) 옵션을 선택하는 것 외에도 **Use Client Address** 옵션을 선택합니다.그런 다음 VPN 3000 Concentrator에서 사용자 및 IP 주소를 정의합니다.이 사용자는 연결할 때 항상 VPN Concentrator에 구성된 IP 주소를 가져옵니다.
- **IPsec 사용자**IP Address Management 섹션에서 풀 또는 DHCP 옵션을 선택하는 것 외에도 **Use Address from Authentication Server** 옵션을 선택합니다.그런 다음 VPN 3000 Concentrator에서 사용자 및 IP 주소를 정의합니다.이 사용자는 연결할 때 항상 VPN Concentrator에 구성된 IP 주소를 가져옵니다.동일한 그룹 또는 다른 그룹에 속하는 다른 모든 그룹은 전역 풀 또는 DHCP에서 IP 주소를 가져옵니다.Cisco VPN 3000 Concentrator 소프트웨어 버전 3.0 이상에서는 그룹을 기준으로 주소 풀을 구성할 수 있습니다.이 기능을 사용하면 특정 사용자에게 고정 IP 주소를 할당할 수도 있습니다.그룹에 대한 풀을 구성할 경우 고정 IP를 가진 사용자는 자신에게 할당된 IP 주소를 얻고 동일한 그룹의 다른 구성원은 그룹 풀에서 IP 주소를 가져옵니다.이는 VPN Concentrator를 인증 서버로 사용하는 경우에만 적용됩니다.

**참고:** 외부 인증 서버를 사용하는 경우 외부 서버를 사용하여 주소를 올바르게 할당해야 합니다.

## Q. Microsoft의 PPTP 제품 및 VPN 3000 Concentrator와 관련하여 알려진 호환성 문제는 무엇입니까?

**A.** 이 정보는 VPN 3000 Series Concentrator Software Release 3.5 이상을 기반으로 합니다.VPN 3000 Series Concentrator, 모델 3005, 3015, 3020, 3030, 3060, 3080;및 Microsoft 운영 체제 Windows 95 이상

- **Windows 95 DUN(전화 접속 네트워킹) 1.2**DUN 1.2에서는 Microsoft MPPE(Point-to-Point Encryption)가 지원되지 않습니다. MPPE를 사용하여 연결하려면 Windows 95 DUN 1.3을 설치하십시오. Microsoft 웹 사이트에서 Microsoft DUN 1.3 업그레이드를 다운로드할 수 있습니다.
- **Windows NT 4.0**Windows NT는 VPN Concentrator에 대한 PPTP(Point-to-Point Tunneling Protocol) 연결에 대해 완벽하게 지원됩니다.서비스 팩 3(SP3) 이상이 필요합니다.SP3을 실행 중인 경우 PPTP 성능 및 보안 패치를 설치해야 합니다.WinNT 4.0용 Microsoft PPTP 성능 및 보안 업그레이드에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.128비트 서비스 팩 5는 MPPE 키를 올바르게 처리하지 않으며 PPTP에서 데이터를 전달하지 못할 수 있습니다.이 경우 이벤트 로그에 다음 메시지가 표시됩니다.

```
103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
User [ testuser ]
disconnected. Experiencing excessive packet decrypt failure.
```

이 문제를 해결하려면 최신 Windows NT 서비스 팩 6a 및 Windows NT 4.0 서비스 팩 6a 사용 가능의 업그레이드를 다운로드하십시오.자세한 내용은 128비트 MS-CHAP 요청에 대한 Microsoft 문서 MPPE 키가 올바르게 처리되지 않음 을 참조하십시오.

## Q. VPN 3000 Concentrator에서 허용되는 최대 필터 수는 얼마입니까?

**A.** VPN 30xx 유닛(3030 또는 3060도)에 추가할 수 있는 최대 필터 수는 100개로 고정되어 있습니다. 사용자는 Cisco 버그 ID CSCdw86558(지원 계약 필요)를 통해 이 문제에 대한 추가 정보를 찾을 수 있습니다.

## Q. VPN Concentrator 30xx 라인의 최대 경로 수는 얼마입니까?

**A.** 최대 경로 수는 다음과 같습니다.

- VPN 3005 Concentrator는 이전에는 최대 200개의 경로를 보유했습니다.이 수는 이제 350개의 경로로 늘어났습니다.자세한 내용은 Cisco 버그 ID CSCeb35779(지원 계약 필요)를 참조하십시오.
- VPN 3030 Concentrator는 최대 10,000개의 경로를 테스트했습니다.
- VPN 3030, 3060 및 3080 Concentrator의 라우팅 테이블 제한은 각 디바이스에서 사용 가능한 리소스/메모리에 비례합니다.
- VPN 3015 Concentrator에는 미리 정의된 최대 제한이 없습니다.이는 RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First) 프로토콜에 적용됩니다.
- VPN 3020 Concentrator - Microsoft 제한 때문에 Windows XP PC는 많은 수의 CSR(Classless Static Routes)을 수신할 수 없습니다. VPN 3000 Concentrator는 DHCP INFORM 메시지 응답에 삽입되는 CSR의 수를 제한합니다(DHCP INFORM 메시지 응답 구성 시).VPN 3000 Concentrator는 클래스에 따라 경로 수를 28-42로 제한합니다.

## Q. VPN 3000 Concentrator에서 인터페이스 통계를 완전히 지우려면 어떻게 해야 합니까?

**A. Monitoring > Statistics > MIB-II > Ethernet을 선택하고** 통계를 재설정하여 현재 세션에 대한 통계를 지웁니다.이것이 통계를 완전히 지우지는 않는다는 것을 기억하세요.실제로 통계를 재설정하려면(모니터링을 위해 재설정하는 경우와 다름) 재부팅해야 합니다.

## Q. NTP(Network Time Protocol) 통신에서 어떤 포트를 허용해야 합니까?

**A.** TCP 및 UDP 포트 123을 허용합니다.

## Q. UDP 포트 625xx의 기능은 무엇입니까?

**A.** 포트는 PC의 실제 shim/Deterministic NDIS Extender(DNE)와 TCP/IP 스택 간의 VPN 클라이언트 통신에 사용되며 내부 개발 용도로만 사용됩니다.예를 들어 포트 62515는 VPN 클라이언트에서 VPN 클라이언트 로그에 정보를 보내는 데 사용됩니다.다른 포트 기능은 여기에 나와 있습니다.

- 62514 - Cisco Systems, Inc. VPN Service to Cisco Systems IPsec Driver
- 62515 - Cisco Systems IPsec Driver to Cisco Systems, Inc. VPN Service
- 62516 - XAUTH에 대한 Cisco Systems, Inc. VPN 서비스
- 62517 - Cisco Systems, Inc. VPN 서비스에 대한 XAUTH
- 62518 - Cisco Systems, Inc. VPN Service to CLI
- 62519 - Cisco Systems, Inc VPN 서비스에 대한 CLI
- 62520 - Cisco Systems, Inc. VPN Service to UI
- 62521 - Cisco Systems, Inc. VPN 서비스에 대한 UI
- 62522 - 로그 메시지
- 62523 - Cisco Systems, Inc. VPN 서비스에 대한 연결 관리자
- 62524 - Cisco Systems, Inc. VPN 서비스에 대한 PPTool

## Q. WebVPN 부동 표시줄을 제거할 수 있습니까?

**A.** WebVPN 세션을 설정하는 동안에는 부동 도구 모음을 제거하거나 부동 도구 모음을 로드하지 않을 수 없습니다.이 창을 닫으면 세션이 즉시 종료되고 다시 로그인을 시도하면 창이 다시 로드되

기 때문입니다.이는 WebVPN 세션이 원래 설계된 방식입니다.주 창을 닫을 수는 있지만 부동 창을 닫을 수는 없습니다.

# 소프트웨어

## Q. WebVPN은 OWA(Outlook Web Access) 2003을 지원합니까?

**A.** VPN 3000 Concentrator의 WebVPN에 대한 OWA 2003 지원은 이제 버전 4.1.7 다운로드(지원 계약 필요)와 함께 제공됩니다.

## Q. VPN 3000 Concentrator의 최신 소프트웨어 버전은 어디에서 얻을 수 있습니까?

**A.** 모든 Cisco VPN 3000 Concentrator는 최신 코드와 함께 제공되지만, 사용자는 다운로드(지원 계약 필요)를 확인하여 최신 소프트웨어가 더 있는지 확인할 수 있습니다.

VPN 3000 Concentrator에 대한 최신 설명서는 Cisco VPN 3000 Series Concentrator 설명서 페이지를 참조하십시오.

## Q. VPN 3000 Concentrator를 업그레이드하려면 TFTP 서버가 필요합니까?시스템을 업그레이드할 수 있는 다른 방법이 있습니까?

**A.** TFTP를 사용하는 것 외에도 최신 소프트웨어를 하드 드라이브에 다운로드하여 VPN Concentrator를 업그레이드할 수 있습니다.그런 다음 소프트웨어가 있는 시스템의 브라우저에서 **Administration(관리) > Software Update(소프트웨어 업데이트)로 이동하여** 하드 드라이브에서 다운로드한 소프트웨어를 찾습니다(파일 열기와 마찬가지로). 찾으면 **업로드** 탭을 선택합니다.

## Q. "k9"는 최신 코드 이름(예: "vpn3000-3.0.4.Rel-k9.bin"에서)에서 무엇을 의미합니까?

**A.** 이미지 이름에 대한 "k9" 지정이 원래 사용된 3DES 지정을 대체했습니다(예: vpn3000-2.5.2.F-3des.bin). 따라서 이제 "k9"는 3DES 이미지입니다.

## Q: 모든 사용자의 경우 IPsec 그룹 아래에 있는 데이터 압축 옵션을 사용해야 합니까?

**A.** 데이터 압축은 각 사용자 세션에 대한 메모리 요구 사항 및 CPU 사용률을 증가시키고 결과적으로 VPN Concentrator의 전체 처리량을 감소시킵니다.따라서 그룹의 모든 구성원이 모뎀과 연결하는 원격 사용자일 경우에만 데이터 압축을 활성화하는 것이 좋습니다.그룹의 구성원이 광대역을 통해 연결하는 경우 그룹에 대해 데이터 압축을 활성화하지 마십시오.대신 그룹을 두 그룹으로 나누십시오. 하나는 모뎀 사용자이고 다른 하나는 광대역 사용자입니다.모뎀 사용자 그룹에 대해서만 데이터 압축을 활성화합니다.

# 기타 고급 기능

## Q. 로드 밸런싱은 LAN-to-LAN 연결에서 작동합니까?

**A.** 로드 밸런싱은 Cisco VPN Software Client(릴리스 3.0 이상)에서 시작된 원격 세션에만 적용됩니다. 다른 모든 클라이언트(PPTP, L2TP) 및 LAN-to-LAN 연결은 로드 밸런싱이 활성화된 VPN

Concentrator에 연결할 수 있지만 로드 밸런싱에는 참여할 수 없습니다.

## Q. config 파일에서 비밀번호를 해독하려면 어떻게 해야 합니까?

**A.** Configuration(컨피그레이션) **> System(시스템) > Management Protocols(관리 프로토콜) > XML**로 이동한 다음 **관리**로 **이동합니다. | 파일 관리를 통해 XML 형식을 선택합니다**.같은 이름 또는 다른 이름을 사용하고 암호를 보려면 파일을 엽니다.

## Q. VRRP(Virtual Router Redundancy Protocol)와 로드 밸런싱을 함께 사용할 수 있습니까?

**A.** VRRP에서는 로드 밸런싱을 사용할 수 없습니다.VRRP 컨피그레이션에서는 활성 VPN Concentrator에 장애가 발생하지 않는 한 백업 디바이스가 유휴 상태로 유지됩니다.로드 밸런싱 컨피그레이션에서는 유휴 디바이스가 없습니다.

## Q. 모든 원격 액세스 클라이언트 VPN 트래픽은 암호화된 터널을 통해 엔터프라이즈 또는 서비스 공급자의 VPN Concentrator로 이동해야 합니까?예를 들어, 다른 사이트에 대한 일반 웹 액세스는 ISP의 인터넷 연결을 통해 직접 개방적으로 이동할 수 있습니까?

**A.** 네.이 개념을 "스플릿 터널링"이라고 합니다. 스플릿 터널링을 사용하면 암호화된 터널을 통해 회사 리소스에 안전하게 액세스할 수 있는 동시에 ISP의 리소스를 통해 직접 인터넷에 액세스할 수 있습니다. 이렇게 하면 웹 액세스 경로에서 회사 네트워크가 제거됩니다. Cisco VPN Client 및 VPN 3002 하드웨어 클라이언트 모두에 대한 Cisco VPN 3000 Concentrator Series는 스플릿 터널링을 지원할 수 있습니다.추가 보안을 위해 이 기능은 사용자가 아니라 VPN Concentrator 관리자가 제어할 수 있습니다.

## Q. 스플릿 터널링을 사용하는 것이 안전합니까?

**A.** 스플릿 터널링을 사용하면 VPN 터널을 통해 연결하는 동안 편리하게 인터넷을 탐색할 수 있습니다.그러나 기업 네트워크에 연결된 VPN 사용자가 공격에 취약할 경우 약간의 위험이 발생합니다.이 경우 사용자는 개인 방화벽을 사용하는 것이 좋습니다.지정된 VPN 클라이언트 버전에 대한 릴리스 정보에서는 개인 방화벽과의 상호운용성을 설명합니다.

## Q. Cisco VPN 3000 Concentrator에서 로드 밸런싱은 어떻게 작동합니까?

**A.** 로드**는** 활성 연결에서 파생된 백분율로 구성된 최대 연결로 분할됩니다.디렉터는 모든 관리 LAN-to-LAN 세션을 유지 관리하고 다른 모든 클러스터 멤버 로드를 계산하며 모든 클라이언트 리디렉션을 담당하므로 항상 로드가 가장 적습니다.

새로 구성된 기능 클러스터의 경우 연결이 설정되기 전에 디렉터가 약 1% 로드됩니다.따라서 디렉터는 백업 로드 비율이 디렉터의 로드 비율보다 높을 때까지 백업 Concentrator로 연결을 리디렉션합니다.예를 들어 "유휴" 상태의 VPN 3030 Concentrator 2개가 있는 경우 디렉터는 1% 로드를 가집니다.이차에는 디렉터가 연결을 허용하기 전에 30개의 연결(2% 로드)이 지정됩니다.

디렉터가 연결을 허용하는지 확인하려면 Configuration(구성) **> System(시스템) > General(일반) > Sessions(세션)로 이동하여** 인위적으로 낮은 수의 연결 최대 수를 줄여 백업 VPN Concentrator의 로드를 빠르게 늘립니다.

### Q. VPN Monitor에서 추적할 수 있는 헤드엔드 장치는 몇 개입니까?

**A.** VPN 모니터는 20개의 헤드엔드 디바이스를 추적할 수 있습니다.허브 앤 스포크 시나리오에서는 헤드엔드에서 원격 사이트의 연결을 모니터링합니다.허브 라우터에서 해당 정보를 추적할 수 있으므로 모든 원격 사이트 및 사용자를 모니터링할 필요가 없습니다.이러한 헤드엔드 디바이스는 최대 20,000명의 원격 사용자 또는 2,500개의 원격 사이트를 지원할 수 있습니다.스포크 사이트로 이동하는 듀얼 홈 VPN 장치는 모니터링할 수 있는 최대 20개 디바이스 중 2개로 계산됩니다.

## 관련 정보

- Cisco VPN 3000 Concentrator 지원 페이지
- Cisco VPN 3000 클라이언트 지원 페이지
- 기술 지원 및 문서 – Cisco Systems