

VPN 3000 Concentrator 컨피그레이션을 사용하는 IOS 라우터에서 NEM을 사용하는 EzVPN

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN 3000 Concentrator 구성](#)

[작업](#)

[네트워크 다이어그램](#)

[단계별 지침](#)

[라우터 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[디버그 명령의 출력](#)

[문제 해결을 위한 관련 Cisco IOS show 명령](#)

[VPN 3000 Concentrator 디버그](#)

[문제가 될 수 있는 부분](#)

[관련 정보](#)

소개

이 문서에서는 Cisco VPN 3000 Concentrator에 연결하기 위해 [NEM\(Network Extension Mode\)](#)에서 Cisco IOS® 라우터를 EzVPN으로 구성하기 위해 사용하는 절차에 대해 설명합니다. 새로운 EzVPN Phase II 기능은 기본 NAT(Network Address Translation) 컨피그레이션을 지원하는 기능입니다. EzVPN Phase II는 Unity Protocol(VPN 클라이언트 소프트웨어)에서 파생됩니다. 원격 디바이스는 항상 IPsec 터널의 개시자입니다. 그러나 IKE(Internet Key Exchange) 및 IPsec 제안서는 EzVPN 클라이언트에서 구성할 수 없습니다. VPN 클라이언트가 서버와 제안을 협상합니다.

Easy VPN을 사용하여 PIX/ASA 7.x와 Cisco 871 라우터 간에 IPsec을 구성하려면 [ASA 5500을 서버로 사용하는 PIX/ASA 7.x Easy VPN 및 Cisco 871을 Easy VPN Remote Configuration 예로](#) 참조하십시오.

Cisco IOS® Easy VPN Remote Hardware Client와 PIX Easy VPN Server 간에 IPsec을 구성하려면 PIX Easy [VPN Remote Hardware Client to a PIX Easy VPN Server Configuration Example](#)을 참조하십시오.

Cisco 7200 라우터를 EzVPN으로 구성하고 Cisco 871 라우터를 Easy VPN Remote로 구성하려면 [7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example](#)을 참조하십시오.

[사전 요구 사항](#)

[요구 사항](#)

이 컨피그레이션을 시도하기 전에 Cisco IOS 라우터가 EzVPN [Phase II 기능](#)을 지원하고 IPsec 터널을 설정하기 위해 엔드 투 엔드 연결을 사용하는 IP 연결을 설정했는지 확인합니다.

[사용되는 구성 요소](#)

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2(8)YJ(EzVPN Phase II)
- VPN 3000 Concentrator 3.6.x
- Cisco 1700 라우터

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.

참고: 이 컨피그레이션은 최근 Cisco IOS Software Release 12.4(8) 및 VPN 3000 Concentrator 4.7.x 버전이 포함된 Cisco 3640 라우터에서 테스트되었습니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

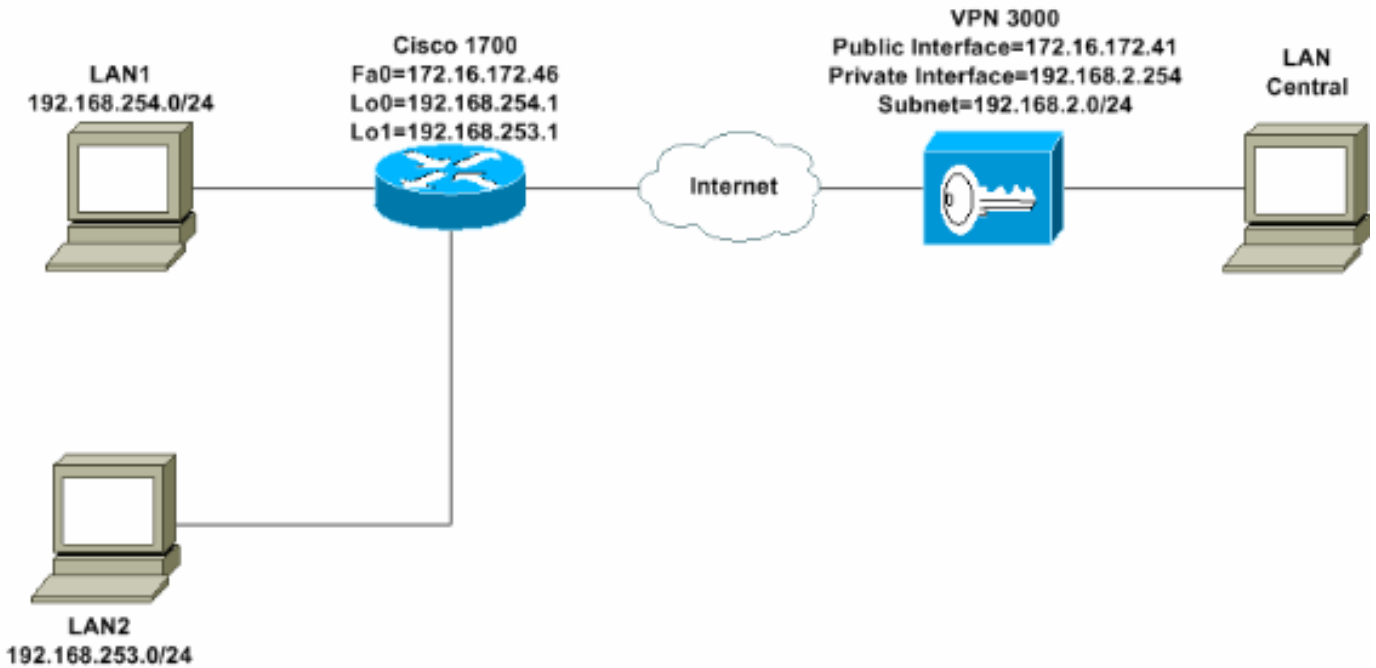
[VPN 3000 Concentrator 구성](#)

[작업](#)

이 섹션에서는 VPN 3000 Concentrator를 구성하는 방법에 대한 정보를 제공합니다.

[네트워크 다이어그램](#)

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다. 루프백 인터페이스는 내부 서브넷으로 사용되며 FastEthernet 0은 인터넷의 기본값입니다.



단계별 지침

다음 단계를 완료하십시오.

1. Configuration(컨피그레이션) > User Management(사용자 관리) > Groups(그룹) > Add and define a group name and password(그룹 이름 및 비밀번호 추가)를 선택하여 사용자에게 대한 IPsec 그룹을 구성합니다. 이 예에서는 그룹 이름 **turaro**를 password/verify tulo와 함께 사용합니다.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	turaro	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

2. IPsec을 활성화하고 PPTP(Point-to-Point Tunneling Protocol) 및 L2TP(Layer 2 Tunnel Protocol)를 비활성화하려면 **Configuration > User Management > Groups > turaro > General**을 선택합니다. 원하는 항목을 선택하고 Apply를 클릭합니다

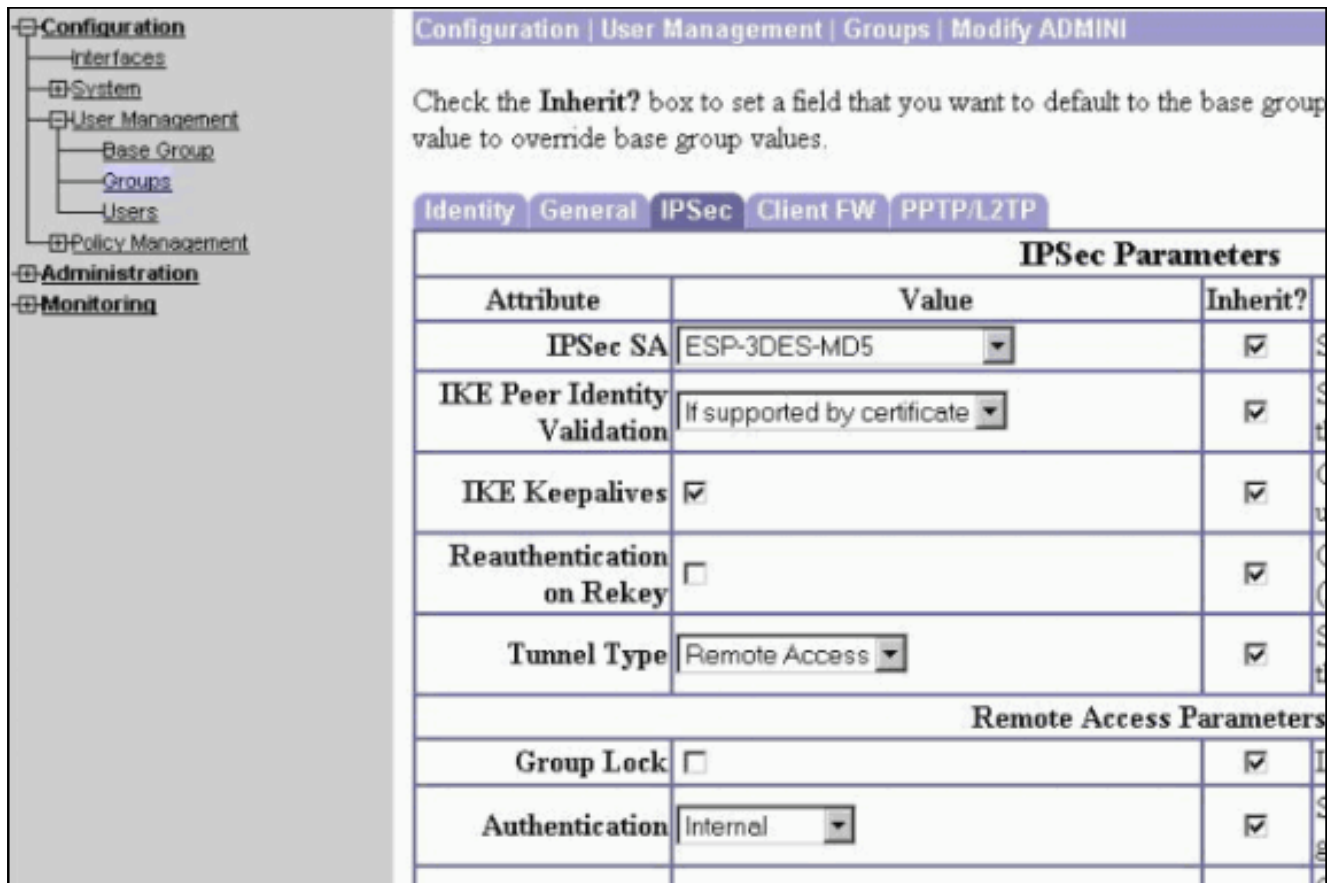
- [-] Configuration
 - Interfaces
 - [-] System
 - [-] User Management
 - Base Group
 - Groups
 - Users
 - [-] Policy Management
- [-] Administration
- [-] Monitoring

Identity
General
IPSec
Client FW
PPTP/L2TP

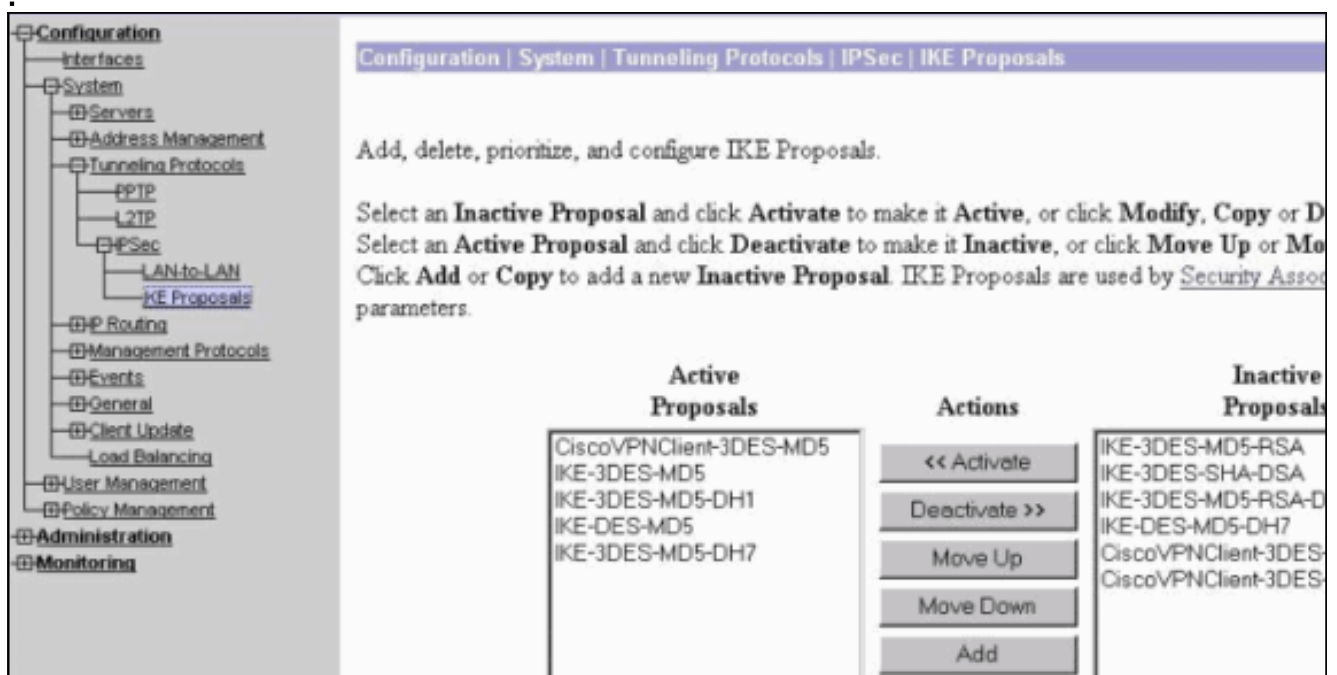
General Parameters

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter be a
Idle Timeout	30	<input checked="" type="checkbox"/>	(min
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(min
Filter	-None-	<input checked="" type="checkbox"/>	Enter
Primary DNS		<input checked="" type="checkbox"/>	Enter
Secondary DNS		<input checked="" type="checkbox"/>	Enter
Primary WINS		<input checked="" type="checkbox"/>	Enter
Secondary WINS		<input checked="" type="checkbox"/>	Enter
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec	<input type="checkbox"/>	Select

3. Authentication(인증)을 Internal for Extended Authentication(Xauth)으로 설정하고 Tunnel Type(터널 유형)이 Remote Access(원격 액세스)이고 IPSec SA가 ESP-3DES-MD5인지 확인합니다



4. Cisco VPN Client(CiscoVPNClient-3DES-MD5)가 IKE용 활성 제안(1단계)에 있는지 확인하려면 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPsec > IKE Proposals(IKE 제안)를 선택합니다.참고: VPN Concentrator 4.1.x에서 Cisco VPN Client가 IKE에 대한 활성 제안(1단계) 목록에 있는지 확인하는 절차는 다릅니다. Configuration > Tunneling and Security > IPsec > IKE Proposals를 선택합니다



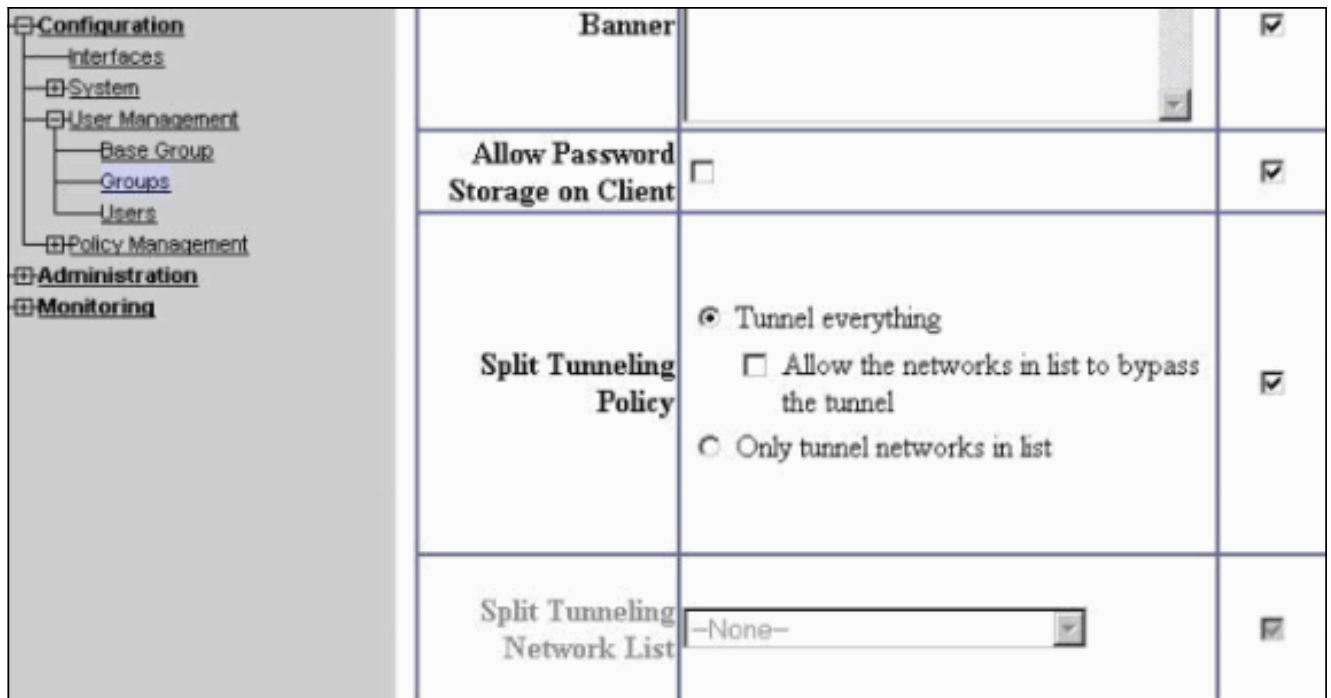
5. IPsec SA(Security Association)를 확인합니다.3단계에서 IPsec SA는 ESP-3DES-MD5입니다. 원하는 경우 새 SA를 생성할 수 있지만 그룹에서 올바른 IPsec SA를 사용해야 합니다. 사용하는 IPsec SA에 대해 PFS(Perfect Forward Secrecy)를 비활성화해야 합니다. Configuration(컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > SAs(SA)를 선택하여 Cisco VPN Client를 IKE 제안으로 선택합니다. 텍스트 상자에 SA 이름을

입력하고 다음과 같이 적절한 항목을 선택합니다

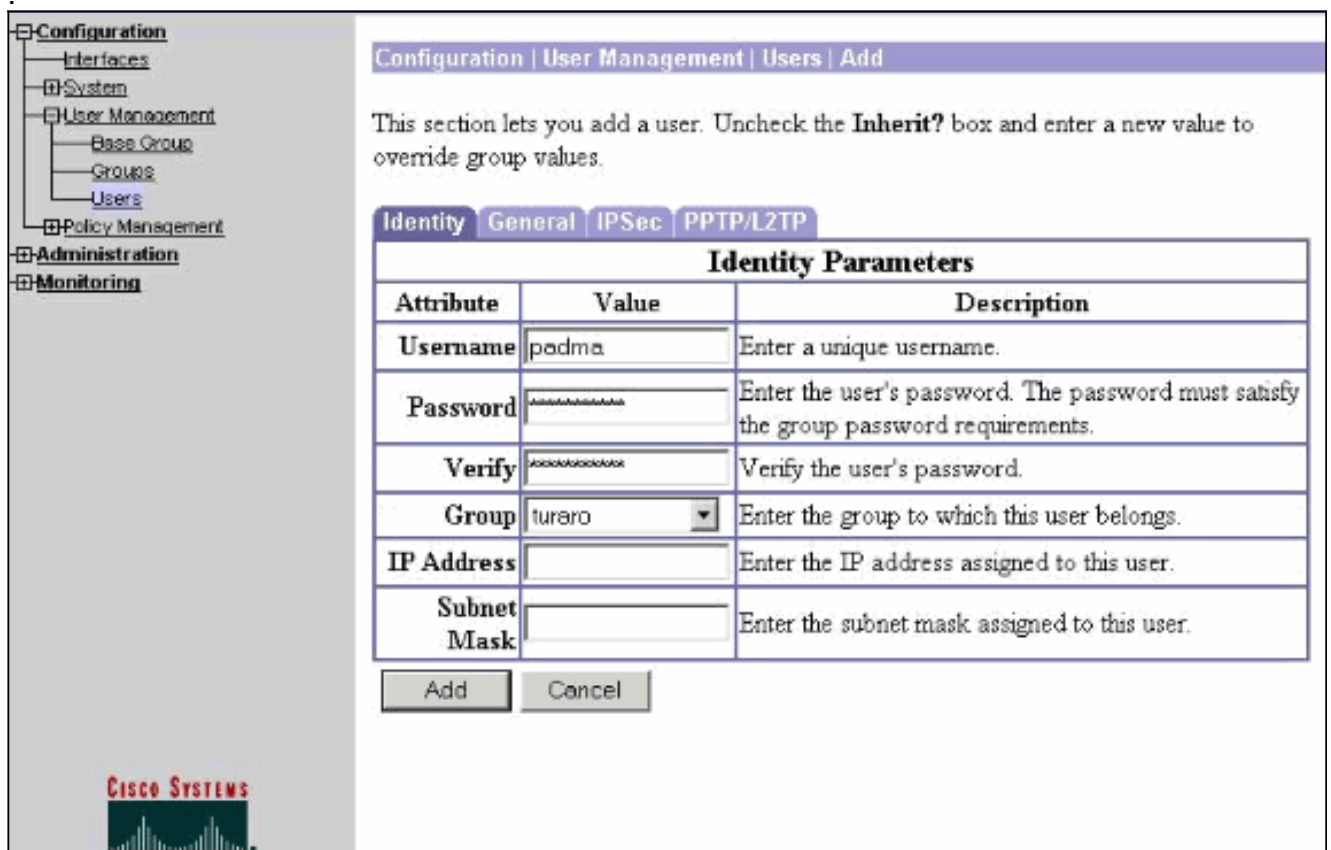
Configuration Policy Management Traffic Management Security Associations Modify		
Modify a configured Security Association.		
SA Name	<input type="text" value="ESP-3DES-MD5"/>	Specify the name of this Security Association (S
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec ke
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
IKE Peer	<input type="text" value="0.0.0.0"/>	Specify the IKE Peer for a LAN-to-LAN IPSec
Negotiation Mode	<input type="text" value="Aggressive"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the
IKE Proposal	<input type="text" value="CiscoVPNClient-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

참고: 사전 정의된 SA를 선택하려는 경우 이 단계와 다음 단계는 선택 사항입니다. 클라이언트에 동적으로 할당된 IP 주소가 있는 경우 IKE 피어 텍스트 상자에서 0.0.0.0을 사용합니다. 이 예와 같이 IKE Proposal(IKE 제안)이 CiscoVPNClient-3DES-MD5로 설정되어 있는지 확인합니다.

6. 목록의 네트워크가 터널을 우회하도록 허용을 클릭하지 않아야 합니다. 따라서 스플릿 터널링이 지원되지만 EzVPN 클라이언트 기능에서는 바이패스 기능이 지원되지 않습니다



7. 사용자를 추가하려면 **Configuration > User Management > Users**를 선택합니다. 사용자 이름과 암호를 정의하고 그룹에 할당한 다음 **Add(추가)**를 클릭합니다



8. 관리 > 관리 세션을 선택하고 사용자가 연결되어 있는지 확인합니다. NEM에서 VPN Concentrator는 풀에서 IP 주소를 할당하지 않습니다.참고: 사전 정의된 SA를 선택하려는 경우 이 단계는 선택 사항입니다

LAN-to-LAN Sessions									[Remote Access Sessions Management Sessions]
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions	
No LAN-to-LAN Sessions									
Remote Access Sessions									[LAN-to-LAN Sessions Management Sessions]
Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions		
Cisco_MAE	192.168.253.0 172.16.172.46	turaro	IPSec 3DES-168	Mar 31 18:32:23 0:02:50	N/A N/A	301320 301320	[Logout Ping]		
Management Sessions									[LAN-to-LAN Sessions Remote Access Sessions]
Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions			
adman	171.69.89.5	HTTP	None	Mar 31 18:35:01	0:00:12	[Logout Ping]			

9. 구성을 저장하려면 **Save Needed** 또는 **Save** 아이콘을 클릭합니다.

라우터 컨피그레이션

show version 출력

show version

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-M), Version 12.2(8)YJ,
EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

```
1721-1(ADSL) uptime is 4 days, 5 hours, 33 minutes
System returned to ROM by reload
System image file is "flash:c1700-bk9no3r2sy7-mz.122-8.YJ.bin"
cisco 1721 (MPC860P) processor (revision 0x100) with 88474K/9830K bytes
16384K bytes of processor board System flash (Read/Write)
```

1721-1

```
1721-1(ADSL)#show run
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1721-1(ADSL)
!
!--- Specify the configuration name !--- to be assigned
to the interface. crypto ipsec client ezvpn SJVPN
!--- Tunnel control; automatic is the default. connect
auto
!--- The group name and password should be the same as
given in the VPN Concentrator. group turaro key tululo
!--- The mode that is chosen as the network extension.
mode network-extension
!--- The tunnel peer end (VPN Concentrator public
interface IP address). peer 172.16.172.41
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.0
!--- Configure the Loopback interface !--- as the inside
interface. ip nat inside
!--- Specifies the Cisco EzVPN Remote configuration name
!--- to be assigned to the inside interface.
```



```

crypto ipsec client ezvpn SJVPN inside
!
interface Loopback1
 ip address 192.168.253.1 255.255.255.0
 ip nat inside
 crypto ipsec client ezvpn SJVPN inside
!
interface FastEthernet0
 ip address 172.16.172.46 255.255.255.240
 !--- Configure the FastEthernet interface !--- as the
 outside interface. ip nat outside
 !--- Specifies the Cisco EzVPN Remote configuration name
 !--- to be assigned to the first outside interface,
 because !--- outside is not specified for the interface.
 !--- The default is outside.

 crypto ipsec client ezvpn SJVPN
!
 !--- Specify the overload option with the ip nat command
 !--- in global configuration mode in order to enable !--
 - Network Address Translation (NAT) of the inside source
 address !--- so that multiple PCs can use the single IP
 address.

 ip nat inside source route-map EZVPN interface
 FastEthernet0 overload
 ip classless
 ip route 0.0.0.0 0.0.0.0 172.16.172.41
!
 access-list 177 deny ip 192.168.254.0 0.0.0.255
 192.168.2.0 0.0.0.255
 access-list 177 deny ip 192.168.253.0 0.0.0.255
 192.168.2.0 0.0.0.255
 access-list 177 permit ip 192.168.253.0 0.0.0.255 any
 access-list 177 permit ip 192.168.254.0 0.0.0.255 any
!
 route-map EZVPN permit 10
 match ip address 177
!
!
 line con 0
 line aux 0
 line vty 0 4
 password cisco
 login
!
 no scheduler allocate
end

```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

두 디바이스를 모두 구성하면 Cisco 3640 라우터는 피어 IP 주소를 사용하여 VPN Concentrator에 자동으로 연결하여 VPN 터널을 설정하려고 시도합니다. 초기 ISAKMP 매개변수가 교환되면 라우터에 다음 메시지가 표시됩니다.

Pending XAuth Request, Please enter the following command: **crypto ipsec client ezvpn xauth**

사용자 이름 및 비밀번호를 입력하라는 메시지를 표시하는 **crypto ipsec client ezvpn xauth** 명령을 입력해야 합니다. 이는 VPN Concentrator(7단계)에 구성된 사용자 이름과 비밀번호와 일치해야 합니다. 사용자 이름과 비밀번호가 두 피어에서 모두 동의하면 나머지 매개변수가 동의되고 IPsec VPN 터널이 나타납니다.

EZVPN(SJVPN): Pending XAuth Request, Please enter the following command:

EZVPN: crypto ipsec client ezvpn xauth

!--- Enter the crypto ipsec client ezvpn xauth command.

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show** 명령은 [출력 인터프리터](#) 틀에서 지원되는데(등록된 고객만), 이 틀을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

참고: 디버그 명령을 [실행하기](#) 전에 [디버그 명령](#)에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec client ezvpn** - EzVPN 클라이언트 기능의 컨피그레이션 및 구현을 보여 주는 정보를 표시합니다.
- **debug crypto ipsec** - IPsec 연결에 대한 디버그 정보를 표시합니다.
- **debug crypto isakmp** - IPsec 연결에 대한 디버그 정보를 표시하고 양쪽 끝에서 비호환성으로 인해 거부된 첫 번째 특성 집합을 표시합니다.
- **show debug** - 각 디버깅 옵션의 상태를 표시합니다.

디버그 명령의 출력

crypto ipsec client ezvpn SJVPN 명령을 입력하면 EzVPN Client가 서버에 연결을 시도합니다. 그룹 컨피그레이션 아래에서 **connect manual** 명령을 변경할 경우 **crypto ipsec client ezvpn connect SJVPN** 명령을 입력하여 서버에 대한 제안 교환을 시작합니다.

```
4d05h: ISAKMP (0:3): beginning Aggressive Mode exchange
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): processing SA payload. message ID = 0
4d05h: ISAKMP (0:3): processing ID payload. message ID = 0
```

4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is Unity
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
4d05h: ISAKMP (0:3): vendor ID is XAUTH
4d05h: ISAKMP (0:3): processing vendor id payload
4d05h: ISAKMP (0:3): vendor ID is DPD
4d05h: ISAKMP (0:3) local preshared key found
4d05h: ISAKMP (0:3) Authentication by xauth preshared
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65527 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65528 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65529 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65530 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65531 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): Hash algorithm offered does not match policy!
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65532 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): **atts are acceptable.** Next payload is 0
4d05h: ISAKMP (0:3): processing KE payload. message ID = 0
4d05h: ISAKMP (0:3): processing NONCE payload. message ID = 0

4d05h: ISAKMP (0:3): SKEYID state generated
4d05h: ISAKMP (0:3): processing HASH payload. message ID = 0
4d05h: ISAKMP (0:3): **SA has been authenticated with 172.16.172.41**
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE

4d05h: IPSEC(key_engine): got a queue event...

4d05h: IPsec: Key engine got KEYENG_IKMP_MORE_SAS message

4d05h: ISAKMP (0:3): Need XAUTH

4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

!--- Phase 1 (ISAKMP) is complete. 4d05h: ISAKMP: received ke message (6/1) 4d05h: ISAKMP: received KEYENG_IKMP_MORE_SAS message 4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH *!--- Initiate extended authentication.* 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): purging node -857862190 4d05h: ISAKMP (0:3): Sending initial contact. 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1898481791 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1898481791 4d05h: ISAKMP: Config payload REQUEST 4d05h: ISAKMP (0:3): checking request: 4d05h: ISAKMP: XAUTH_TYPE_V2 4d05h: ISAKMP: XAUTH_USER_NAME_V2 4d05h: ISAKMP: XAUTH_USER_PASSWORD_V2 4d05h: ISAKMP: XAUTH_MESSAGE_V2 4d05h: ISAKMP (0:3): Xauth process request 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: XAUTH_REQUEST 4d05h: EZVPN(SJVPN): ezvpn_xauth_request 4d05h: EZVPN(SJVPN): ezvpn_parse_xauth_msg 4d05h: EZVPN: Attributes sent in xauth request message: 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): 4d05h: XAUTH_MESSAGE_V2(SJVPN) <Enter Username and Password.> 4d05h: EZVPN(SJVPN): New State: XAUTH_REQ 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Pending XAuth Request, Please enter the following command: 4d05h: EZVPN: **crypto ipsec client ezvpn xauth**

!--- Enter the crypto ipsec client ezvpn xauth command.

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

!--- The router requests your username and password that is !--- configured on the server. 4d05h: EZVPN(SJVPN): Current State: XAUTH_REQ 4d05h: EZVPN(SJVPN): Event: XAUTH_PROMPTING 4d05h: EZVPN(SJVPN): New State: XAUTH_PROMPT 1721-1(ADSL)# 4d05h: EZVPN(SJVPN): Current State: XAUTH_PROMPT 4d05h: EZVPN(SJVPN): Event: XAUTH_REQ_INFO_READY 4d05h: EZVPN(SJVPN): ezvpn_xauth_reply 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): Cisco_MAE 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): <omitted> 4d05h: EZVPN(SJVPN): New State: XAUTH_REPLIED 4d05h: xauth-type: 0 4d05h: username: Cisco_MAE 4d05h: password: <omitted> 4d05h: message <Enter Username and Password.> 4d05h: ISAKMP (0:3): responding to peer config from 172.16.172.41. ID = -1898481791 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1898481791 error FALSE reason "done with xauth request/reply exchange" 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_XAUTH_REPLY_ATTR Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1602220489 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1602220489 4d05h: ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP (0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State =

IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLIED 4d05h: EZVPN(SJVPN): Event: XAUTH_STATUS 4d05h: EZVPN(SJVPN): New State: READY 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP: set new node 486952690 to CONF_ADDR 4d05h: ISAKMP (0:3): initiating peer config to 172.16.172.41. ID = 486952690 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_REQ_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = 486952690 4d05h: ISAKMP: Config payload REPLY 4d05h: ISAKMP(0:3) process config reply 4d05h: ISAKMP (0:3): deleting node 486952690 error FALSE reason "done with transaction" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_CONFIG_MODE_REQ_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: MODE_CONFIG_REPLY 4d05h: EZVPN(SJVPN): ezvpn_mode_config 4d05h: EZVPN(SJVPN): ezvpn_parse_mode_config_msg 4d05h: EZVPN: Attributes sent in message 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 1, new_if 2 4d05h: EZVPN(SJVPN): New State: SS_OPEN 4d05h: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xE6DB9372(3873149810), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x3C77C53D(1014482237), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0x79BB8DF4(2042334708), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x19C3A5B2(432252338), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1494477527 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xB18CF11E(2978803998), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0xA8C469EC(2831444460), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xBC5AD5EE(3160069614), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x8C34C692(2352268946), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1102788797 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MSG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP: set new node 733055375 to QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = 733055375 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 1 spi 0, message ID = 733055375, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (0:3): start processing isakmp responder

lifetime 4d05h: ISAKMP (0:3): restart ike sa timer to 86400 secs 4d05h: ISAKMP (0:3): deleting node 733055375 error FALSE reason "informational (in) state 1" 4d05h: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1494477527 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 1344958901, message ID = -1494477527, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.254.0) 4d05h: has spi 0x3C77C53D and conn_id 2000 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.254.0 to 0.0.0.0) 4d05h: has spi 1344958901 and conn_id 2001 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1494477527 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1102788797 4d05h: ISAKMP (0:3): Checking IPsec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 653862918, message ID = -1102788797, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x3C77C53D(1014482237), conn_id= 2000, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= **192.168.254.0**/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x502A71B5(1344958901), conn_id= 2001, keysize= 0, flags= 0x4 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.46, sa_prot= 50, sa_spi= **0x3C77C53D(1014482237)**, *!--- SPI that is used on inbound SA.* sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000 4d05h: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.41, sa_prot= 50, sa_spi= **0x502A71B5(1344958901)**, *!--- SPI that is used on outbound SA.* sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001 4d05h: ISAKMP (0:3): Creating IPsec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.253.0) 4d05h: has spi 0xA8C469EC and conn_id 2002 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.253.0 to 0.0.0.0) 4d05h: has spi 653862918 and conn_id 2003 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting

```

node -1102788797 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1102788797, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
4d05h: ISAKMP: received ke message (4/1) 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for
crypto_ikmp_config_handle_kei_mess, count 3 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h:
EZVPN(SJVPN): Event: MTU_CHANGED 4d05h: EZVPN(SJVPN): No state change 4d05h: IPSEC(key_engine):
got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local=
172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 0kb, spi= 0xA8C469EC(2831444460), conn_id= 2002, keysize= 0, flags= 0x4
4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote=
172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 28800s and 0kb,
    spi= 0x26F92806(653862918), conn_id= 2003, keysize= 0, flags= 0xC
4d05h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.46, sa_prot= 50,
    sa_spi= 0xA8C469EC(2831444460),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
4d05h: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.41, sa_prot= 50,
    sa_spi= 0x26F92806(653862918),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
4d05h: ISAKMP: received ke message (4/1)
4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for
    crypto_ikmp_config_handle_kei_mess, count 4
4d05h: EZVPN(SJVPN): Current State: SS_OPEN
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): New State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: MTU_CHANGED
4d05h: EZVPN(SJVPN): No state change
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): No state change

```

[문제 해결을 위한 관련 Cisco IOS show 명령](#)

```
1721-1(ADSL)#show crypto ipsec client ezvpn
```

```

Tunnel name : SJVPN
Inside interface list: Loopback0, Loopback1,
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP

```

```
1721-1(ADSL)#show crypto isakmp sa
```

dst	src	state	conn-id	slot
172.16.172.41	172.16.172.46	QM_IDLE	3	0

```
1721-1(ADSL)#show crypto ipsec sa
```

```

interface: FastEthernet0
Crypto map tag: FastEthernet0-head-0, local addr. 172.16.172.46
local ident (addr/mask/prot/port): (192.168.253.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

```

```

current_peer: 172.16.172.41
PERMIT, flags={origin_is_acl,}
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest 100

```

#pkts decaps: 100, #pkts **decrypt: 100**, #pkts verify 100
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
path mtu 1500, media mtu 1500
current outbound spi: 26F92806

inbound esp sas:

spi: **0xA8C469EC(2831444460)**
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607848/28656)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: **0x26F92806(653862918)**
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607848/28647)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (**192.168.254.0**/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: **172.16.172.41**

PERMIT, flags={origin_is_acl,}

#pkts encaps: 105, #pkts **encrypt: 105**, #pkts digest 105
#pkts decaps: 105, #pkts **decrypt: 105**, #pkts verify 105
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
path mtu 1500, media mtu 1500
current outbound spi: 502A71B5

inbound esp sas:

spi: **0x3C77C53D(1014482237)**
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x502A71B5(1344958901)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: FastEthernet0-head-0
sa timing: remaining key lifetime (k/sec): (4607847/28644)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

활성 터널 지우기

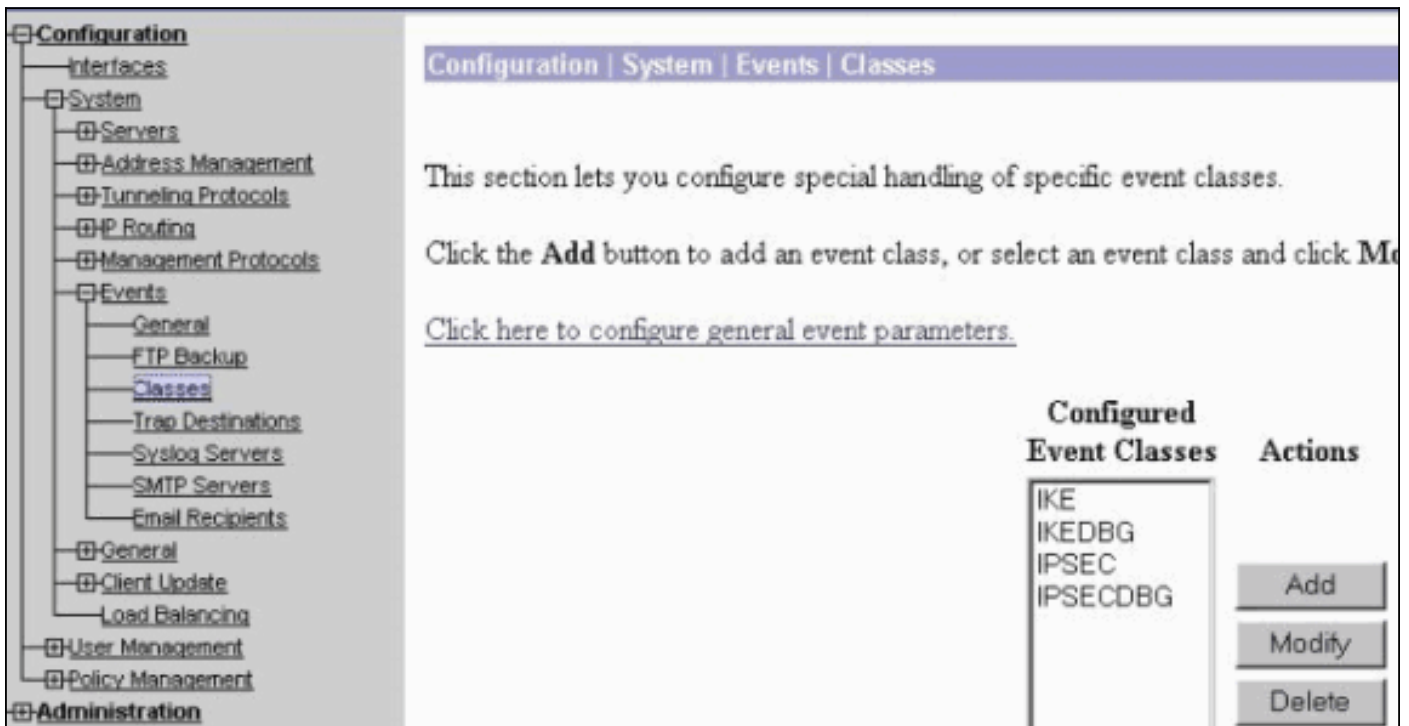
다음 명령을 사용하여 터널을 지울 수 있습니다.

- 암호화 isakmp 지우기
- 암호화 sa 지우기
- crypto ipsec 클라이언트 ezvpn 지우기

참고: VPN Concentrator를 사용하여 Administration(관리) > Admin Sessions(관리 세션)를 선택한 경우 세션에서 로그아웃하고 Remote Access Session(원격 액세스 세션)에서 사용자를 선택한 다음 로그아웃을 클릭합니다.

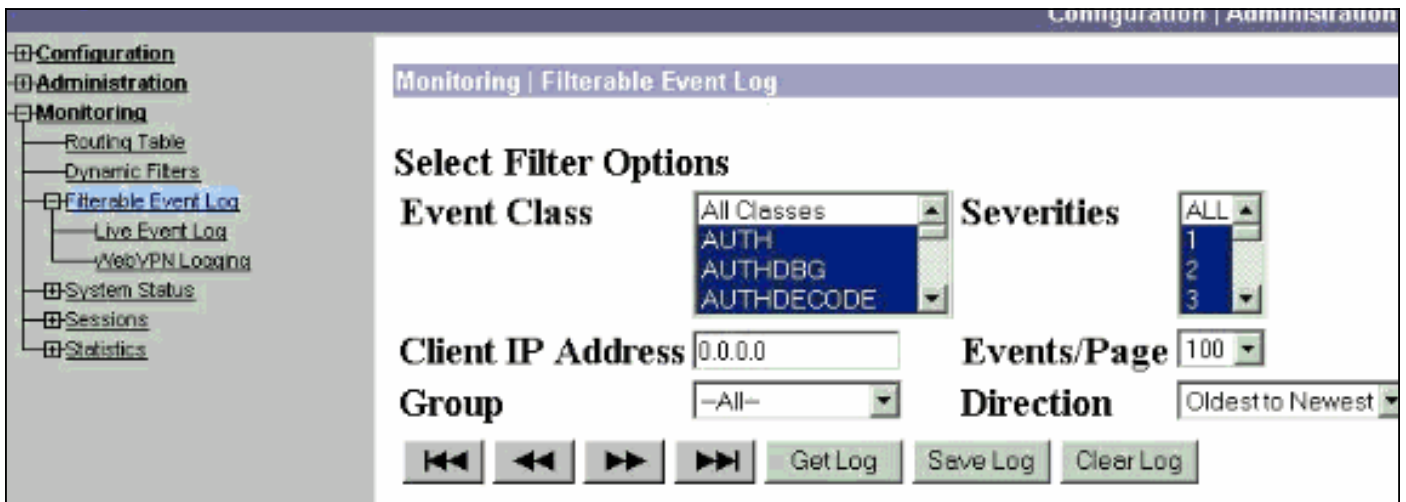
VPN 3000 Concentrator 디버그

이벤트 연결 오류가 있는 경우 이 디버그를 활성화하려면 Configuration > System > Events > Classes를 선택합니다. 표시된 클래스가 문제를 식별하는 데 도움이 되지 않으면 언제든지 클래스를 추가할 수 있습니다.



현재 이벤트 로그 인 메모리, 이벤트 클래스, 심각도, IP 주소 등을 기준으로 필터링할 수 있도록

Monitoring(모니터링) > Filterable Event log(필터링 가능한 이벤트 로그)를 선택합니다.



IPsec 프로토콜의 통계를 보려면 Monitoring(모니터링) > Statistics(통계) > IPsec을 선택합니다. 이 창은 VPN Concentrator가 마지막으로 부팅되거나 재설정된 이후 현재 IPsec 터널을 포함하여 IPsec 활동에 대한 통계를 표시합니다. 이러한 통계는 IPsec Flow Monitoring MIB에 대한 IETF 초안을 따릅니다. Monitoring > Sessions > Detail 창에는 IPsec 데이터도 표시됩니다.

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	2
Total Tunnels	122	Total Tunnels	362
Received Bytes	2057442	Received Bytes	0
Sent Bytes	332256	Sent Bytes	1400
Received Packets	3041	Received Packets	0
Sent Packets	2128	Sent Packets	5
Received Packets Dropped	1334	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	15	Sent Packets Dropped	0
Sent Notifies	254	Inbound Authentications	0
Received Phase-2 Exchanges	362		

문제가 될 수 있는 부분

- Cisco IOS 라우터가 AG_INIT_EXCH 상태로 고정됩니다. 문제를 해결하는 동안 다음 명령을 사용하여 IPsec 및 ISAKMP 디버그를 켜십시오. 디버그 암호화 ipsec디버그 암호화 isakmp디버그 암호화 ezvpnCisco IOS 라우터에서 다음을 확인할 수 있습니다.

```

5d16h: ISAKMP (0:9): beginning Aggressive Mode exchange
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
    
```

```
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH...
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
```

VPN 3000 Concentrator에서 Xauth가 필요합니다. 그러나 선택한 제안은 Xauth를 지원하지 않습니다. Xauth에 대한 내부 인증이 지정되었는지 확인합니다. 내부 인증을 활성화하고 IKE 제안의 인증 모드가 이전 [스크린샷과](#) 같이 Xauth(Preshared Keys)로 설정되어 있는지 [확인합니다](#). 제안을 편집하려면 수정을 클릭합니다.

- 암호가 잘못되었습니다. Cisco IOS 라우터에 Invalid Password 메시지가 표시되지 않습니다. VPN Concentrator에서 상태 AM_TM_INIT_XAUTH에 Received 여기치 않은 이벤트 EV_ACTIVATE_NEW_SA가 표시될 수 있습니다. 암호가 올바른지 확인하십시오.
- 사용자 이름이 잘못되었습니다. Cisco IOS 라우터에서 잘못된 비밀번호가 있는 경우 이와 유사한 디버그가 표시됩니다. VPN Concentrator에서 Authentication rejected(인증 거부)가 표시됩니다. 이유 = 사용자를 찾을 수 없습니다.

[관련 정보](#)

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [Cisco Easy VPN Remote Phase II](#)
- [Cisco VPN 3000 Series 클라이언트 지원 페이지](#)
- [IPsec 협상/IKE 프로토콜 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)