사전 공유 키 구성 사용 Windows 2000/XP PC와 PIX/ASA 7.2 간 L2TP Over IPsec

목차

소개

이 문서에서는 사용자 인증을 위해 Microsoft Windows 2003 IAS(Internet Authentication Service) RADIUS Server와 사전 공유 키를 사용하여 원격 Microsoft Windows 2000/2003 및 XP 클라이언트에서 PIX Security Appliance로 IPsec(Layer 2 Tunneling Protocol)를 구성하는 방법에 대해 설명합니다.Microsoft - 체크리스트를 참조하십시오.IAS에 대한 추가 정보를 위해 전화 접속 및 VPN 액세스를 위한 IAS 구성

원격 액세스 시나리오에서 L2TP를 IPsec으로 구성하는 주요 이점은 원격 사용자가 게이트웨이 또는 전용 회선 없이 공용 IP 네트워크를 통해 VPN에 액세스할 수 있다는 것입니다.따라서 POTS를 사용하는 거의 모든 장소에서 원격 액세스가 가능합니다.또 다른 이점은 VPN 액세스를 위한 유일한 클라이언트 요구 사항은 Windows 2000과 Microsoft DUN(Dial-Up Networking)을 사용하는 것입니다. Cisco VPN Client 소프트웨어와 같은 추가 클라이언트 소프트웨어는 필요하지 않습니다.

이 문서에서는 L2TP over IPsec용 PIX 500 Series Security Appliance를 구성하기 위해 Cisco ASDM(Adaptive Security Device Manager)을 사용하는 방법에 대해서도 설명합니다.

참고: L2TP(Layer 2 Tunneling Protocol) over IPsec은 Cisco Secure PIX Firewall Software Release 6.x 이상에서 지원됩니다.

PIX 6.x와 Windows 2000 간에 L2TP Over IPsec을 구성하려면 인증서를 사용하여 PIX 방화벽과 Windows 2000 PC 간 L2TP Over IPsec 구성을 참조하십시오.

암호화된 방법을 사용하여 원격 Microsoft Windows 2000 및 XP 클라이언트에서 기업 사이트로 L2TP over IPsec을 구성하려면 사전 공유 키를 사용하여 Windows 2000 또는 XP 클라이언트에서 Cisco VPN 3000 Series Concentrator로 L2TP over IPsec 구성을 참조하십시오.

사전 요구 사항

요구 사항

보안 터널을 설정하기 전에 피어 간에 IP 연결이 있어야 합니다.

UDP 포트 1701이 연결 경로를 따라 어느 곳에서도 차단되지 않는지 확인합니다.

Cisco PIX/ASA에서 기본 터널 그룹 및 기본 그룹 정책만 사용합니다.사용자 정의 정책 및 그룹이 작동하지 않습니다.

참고: Cisco VPN Client 3.x 또는 Cisco VPN 3000 Client 2.5가 설치된 경우 보안 어플라이언스는 Windows 2000과 함께 L2TP/IPsec 터널을 설정하지 않습니다.Windows 2000의 서비스 패널에서 Cisco VPN Client 3.x용 Cisco VPN 서비스 또는 Cisco VPN 3000 Client 2.5용 ANETIKE 서비스를 비활성화합니다.이렇게 하려면 **시작 > 프로그램 > 관리 도구 > 서비스**를 선택하고 서비스 패널에서 IPsec 정책 에이전트 서비스를 다시 시작하고 시스템을 재부팅합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX Security Appliance 515E(소프트웨어 버전 7.2(1) 이상)
- Adaptive Security Device Manager 5.2(1) 이상
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional(SP2 포함)
- Windows 2003 Server(IAS 포함)

참고: PIX 6.3을 버전 7.x로 업그레이드하는 경우 Windows XP(L2TP 클라이언트)에 SP2를 설치했는지 확인하십시오.

참고: 문서의 정보도 ASA 보안 어플라이언스에 유효합니다.

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.

관련 제품

이 컨피그레이션은 Cisco ASA 5500 Series Security Appliance 7.2(1) 이상에서도 사용할 수 있습니다.

표기 규칙

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

배경 정보

L2TP over IPsec을 구성하려면 다음 단계를 완료하십시오.

1. L2TP를 사용하여 IPsec을 활성화하려면 IPsec 전송 모드를 구성합니다.Windows 2000 L2TP/IPsec 클라이언트는 IPsec 전송 모드를 사용합니다. - IP 페이로드만 암호화되며 원래 IP 헤더는 그대로 유지됩니다.이 모드의 장점은 각 패킷에 몇 바이트만 추가하고 공용 네트워크의 디바이스에서 패킷의 최종 소스 및 대상을 볼 수 있도록 허용한다는 것입니다.따라서 Windows 2000 L2TP/IPsec 클라이언트가 보안 어플라이언스에 연결하려면 변환을 위한 IPsec 전송 모드를 구성해야 합니다(ASDM 컨피그레이션의 2단계 참조). 이 기능(전송)을 사용하면 IP 헤더의 정보를 기반으로 중간 네트워크에서 특수 처리(예: QoS)를 활성화할 수 있습니다.그러나 레이어 4 헤더는 암호화되어 패킷 검사를 제한합니다.안타깝게도 IP 헤더를 일반 텍스트 전송, 전송 모드에서 전송하면 공격자가 일부 트래픽 분석을 수행할 수 있습니다.
2. VPDN(virtual private dial-up network) 그룹으로 L2TP를 구성합니다.

L2TP with IPsec의 컨피그레이션은 사전 공유 키 또는 RSA 서명 방법을 사용하는 인증서 및 동적(정적 대신) 암호화 맵의 사용을 지원합니다.사전 공유 키는 L2TP over IPsec 터널을 설정하는 인증으로 사용됩니다.

구성

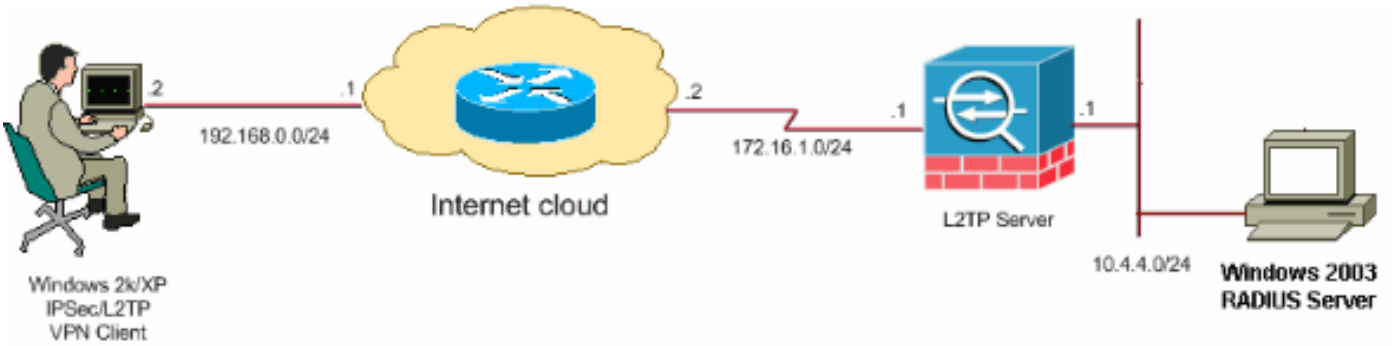
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

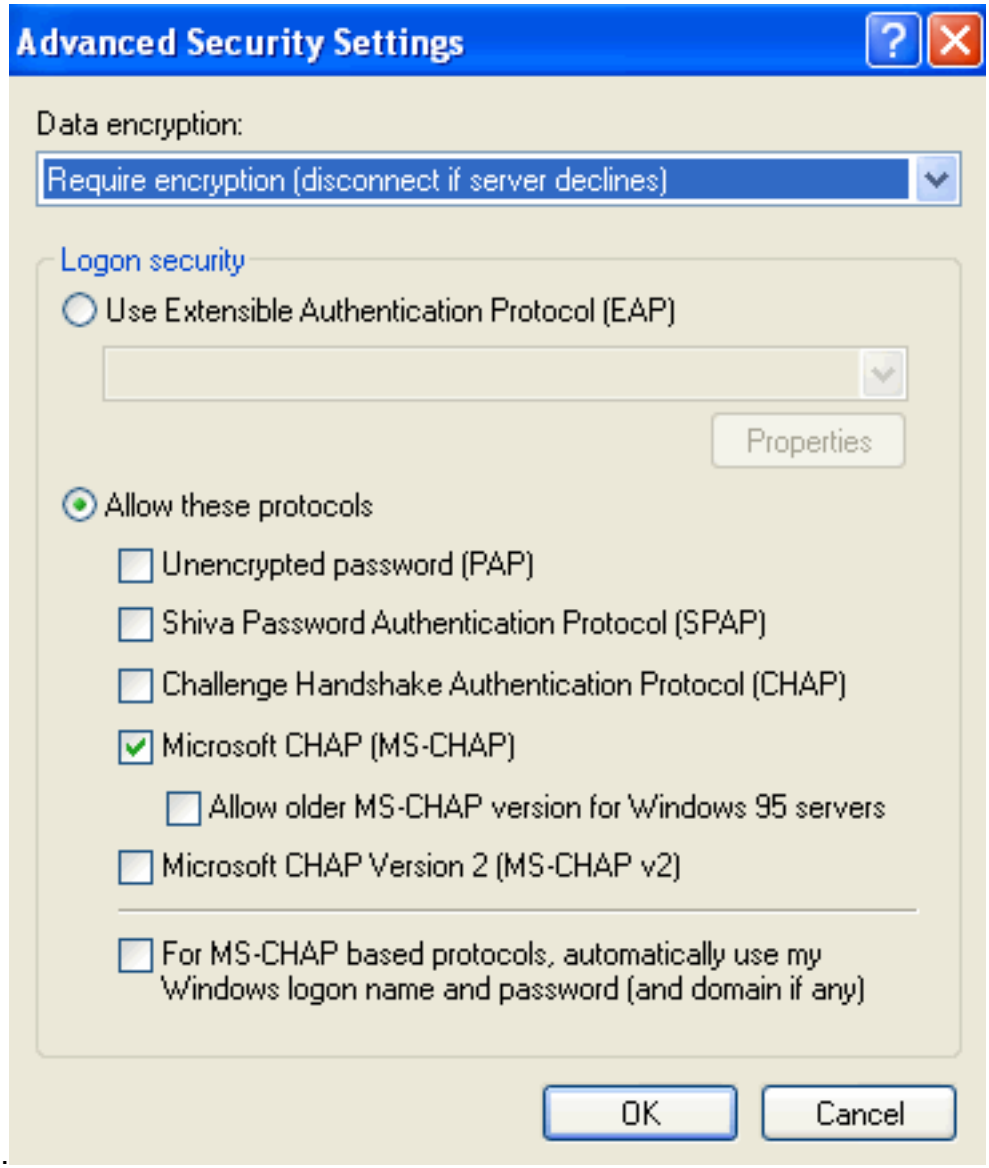
이 문서에서는 다음 구성을 사용합니다.

- Windows L2TP/IPsec 클라이언트 구성
- PIX 구성의 L2TP 서버
- ASDM 구성을 사용하는 L2TP
- Microsoft Windows 2003 Server(IAS 구성 포함)

Windows L2TP/IPsec 클라이언트 구성

Windows 2000에서 L2TP over IPsec을 구성하려면 다음 단계를 완료하십시오.Windows XP의 경우 1단계와 2단계를 건너뛰고 3단계에서 시작합니다.

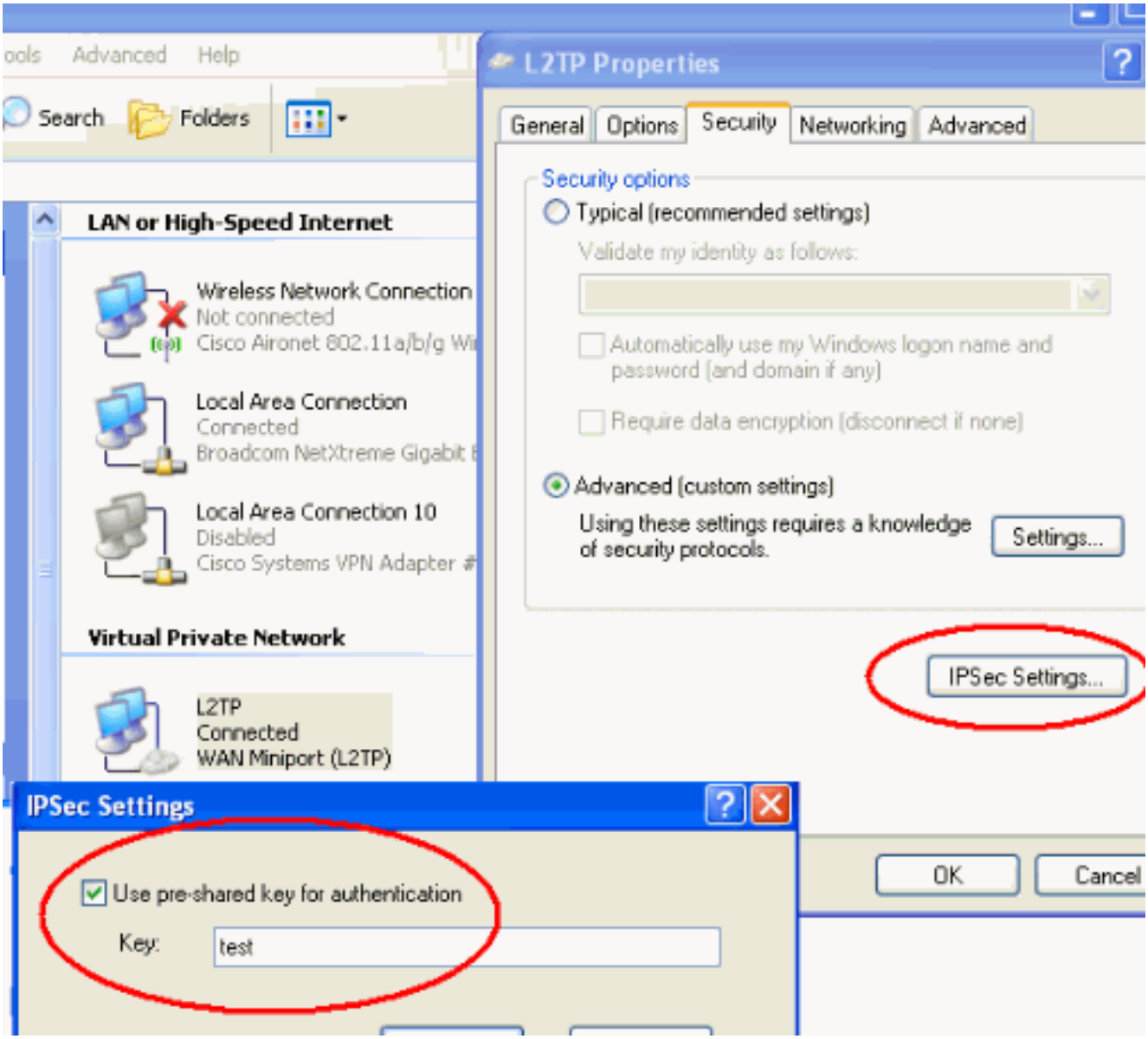
1. Windows 2000 컴퓨터에 이 레지스트리 값을 추가합니다.
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. 이 키에 이 레지스트리 값 추가:
   ```
   Value Name: ProhibitIpSec
   Data Type: REG_DWORD
   Value: 1
   ```
   참고: 경우에 따라 (Windows XP SP2) 이 키가 추가되는 경우도 있습니다**(값:1)** IPsec 연결을 사용하는 L2TP 대신 XP 상자가 L2TP만 협상하므로 연결이 끊어진 것으로 나타납니다.IPsec 정책을 해당 레지스트리 키와 함께 추가해야 합니다.연결을 설정하려고 할 때 `800`이 나타나면 키를 제거합니다(값:1) 작업을 위한 연결**참고:** 변경 사항을 적용하려면 Windows 2000/2003 또는 XP 시스템을 다시 시작해야 합니다.기본적으로 Windows 클라이언트는 CA(Certificate Authority)와 함께 IPsec을 사용하려고 시도합니다. 이 레지스트리 키의 컨피그레이션을 통해 이 문제가 발생하지 않습니다.이제 Windows 스테이션에서 PIX/ASA에서 원하는 매개 변수와 일치하도록 IPsec 정책을 구성할 수 있습니다.Windows IPsec 정책의 단계별 컨피그레이션은 사전 공유 키 인증을 사용하여 L2TP/IPSec 연결 구성 방법(Q240262) 을 참조하십시오.자세한 내용은 Windows XP(Q281555)에서 레이어 2 터널링 프로토콜 연결과 함께 사용할 사전 공유 키 구성\ 을 참조하십시오.
3. 연결을 생성합니다.
4. 네트워크 및 전화 접속 연결에서 연결을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다 .보안 탭으로 이동하여 **고급**을 클릭합니다.이 이미지에 표시된 프로토콜을 선택합니다



.

5. **참고:**이 단계는 Windows XP에만 적용됩니다.IPSec **Settings(IPSec 설정)**를 클릭하고 **Use pre-shared key for authentication(인증에 사전 공유 키 사용)**을 선택하고 사전 공유 키를 입력하여 사전 공유 키를 설정합니다.이 예에서는 테스트가 사전 공유 키로 사용됩니다

.



PIX 구성의 L2TP 서버

PIX 7.2

```
pixfirewall#show run

PIX Version 7.2(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside and inside interfaces.
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat

pager lines 24
```

```
logging console debugging
mtu outside 1500
mtu inside 1500

!--- Creates a pool of addresses from which IP addresses
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

!--- The global and nat command enable !--- the Port
Address Translation (PAT) using an outside interface IP
!--- address for all outgoing traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0


route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify its
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
 key radiuskey

!--- Identifies the group policy as internal. group-
policy DefaultRAGroup internal
!--- Instructs the security appliance to send DNS and !-
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
 wins-server value 10.4.4.99
 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
 default-domain value cisco.com
!--- Configure usernames and passwords on the device !--
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username



          .


username test password DLaUiAX3178qgoB5c7iVNw== nt-
```

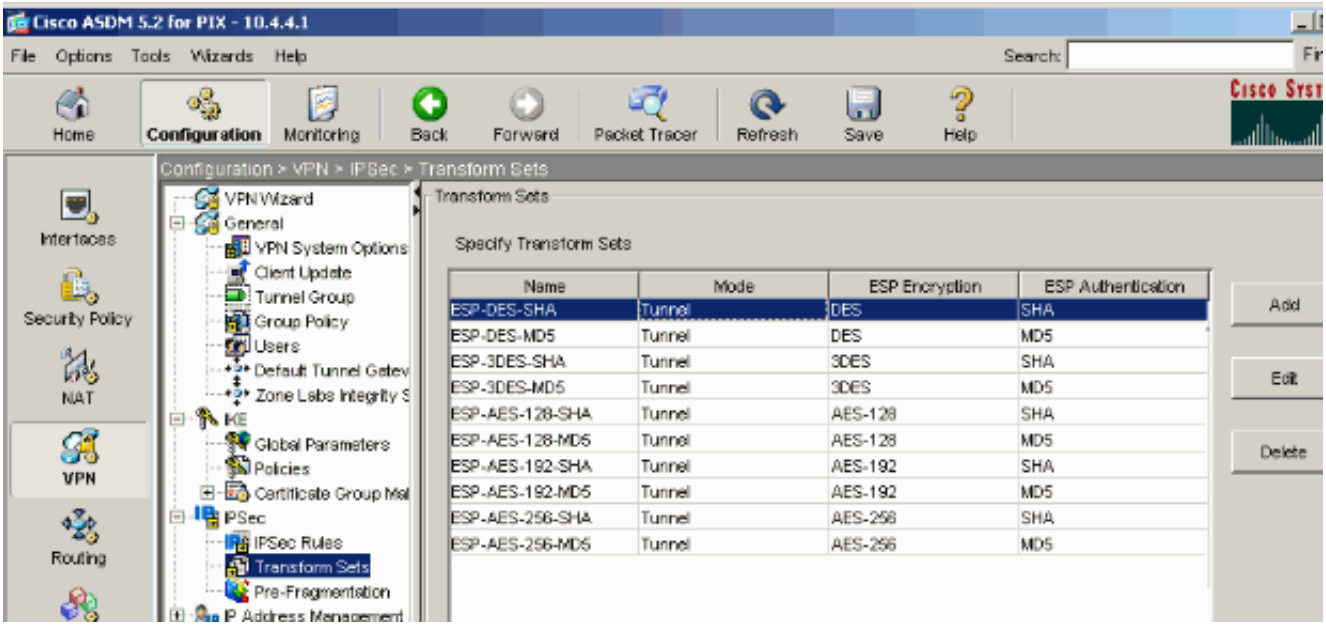
```
encrypted


 vpn-tunnel-protocol l2tp-ipsec

http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

!--- Identifies the IPsec encryption and hash algorithms
!--- to be used by the transform set. crypto ipsec
transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

!--- Since the Windows 2000 L2TP/IPsec client uses IPsec
transport mode, !--- set the mode to transport. !--- The
default is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport




!--- Specifies the transform sets to use in a dynamic
crypto map entry. crypto dynamic-map outside_dyn_map 20
set transform-set TRANS_ESP_3DES_MD5

!--- Requires a given crypto map entry to refer to a
pre-existing !--- dynamic crypto map. crypto map
outside_map 20 ipsec-isakmp dynamic outside_dyn_map

!--- Applies a previously defined crypto map set to an
outside interface. crypto map outside_map interface
outside

crypto isakmp enable outside
crypto isakmp nat-traversal 20

!--- Specifies the IKE Phase I policy parameters. crypto
isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400

!--- Creates a tunnel group with the tunnel-group
command, and specifies the local !--- address pool name
used to allocate the IP address to the client. !---
Associate the AAA server group (VPN) with the tunnel
group.


tunnel-group DefaultRAGroup general-attributes
 address-pool clientVPNpool
 authentication-server-group vpn

!--- Link the name of the group policy to the default
tunnel !--- group from tunnel group general-attributes
mode. default-group-policy DefaultRAGroup

!--- Use the tunnel-group ipsec-attributes command !---
in order to enter the ipsec-attribute configuration
```

```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.


tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *

!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.


tunnel-group DefaultRAGroup ppp-attributes
 no authentication chap
 authentication ms-chap-v2

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd
: end
```

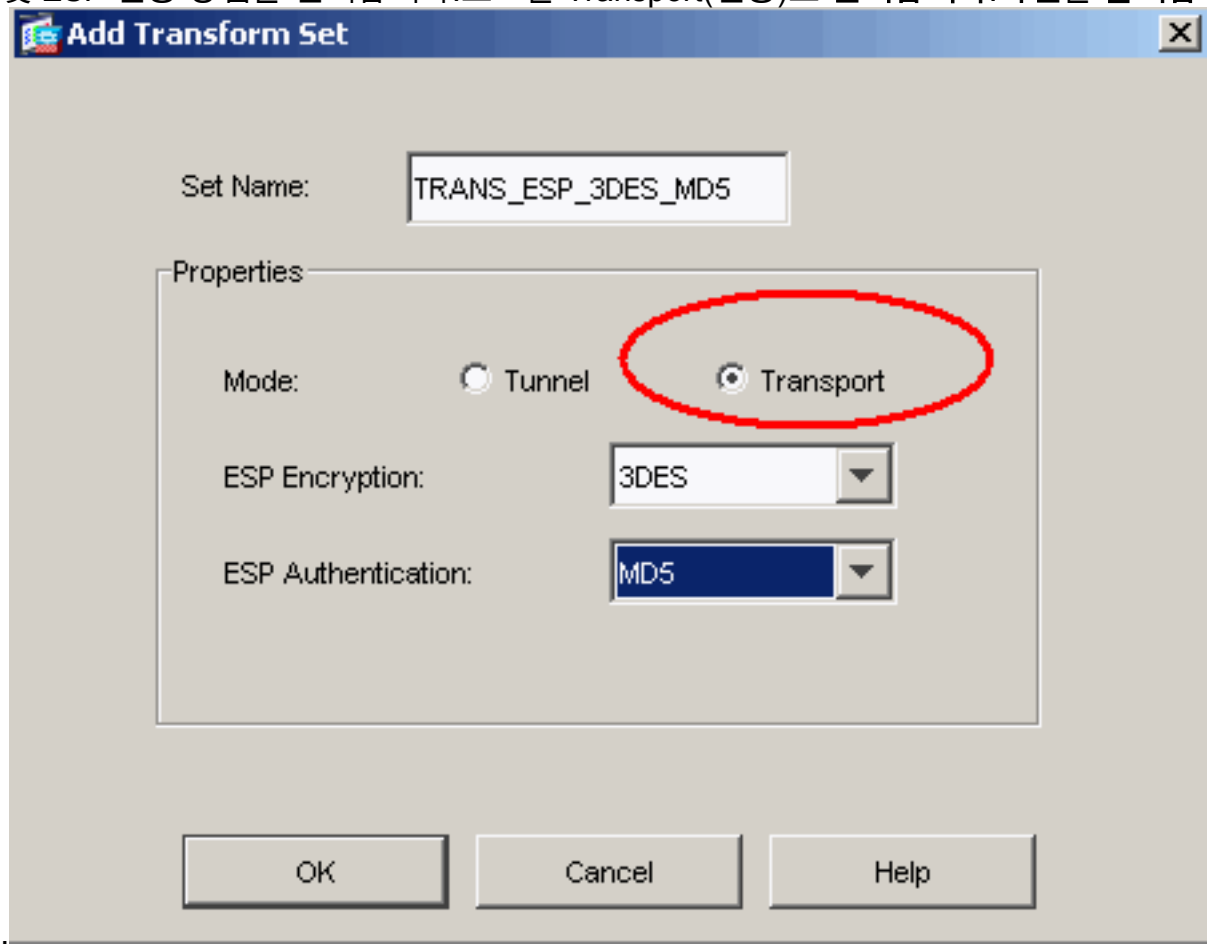
ASDM 구성을 사용하는 L2TP

L2TP over IPsec 연결을 허용하도록 보안 어플라이언스를 구성하려면 다음 단계를 완료합니다.

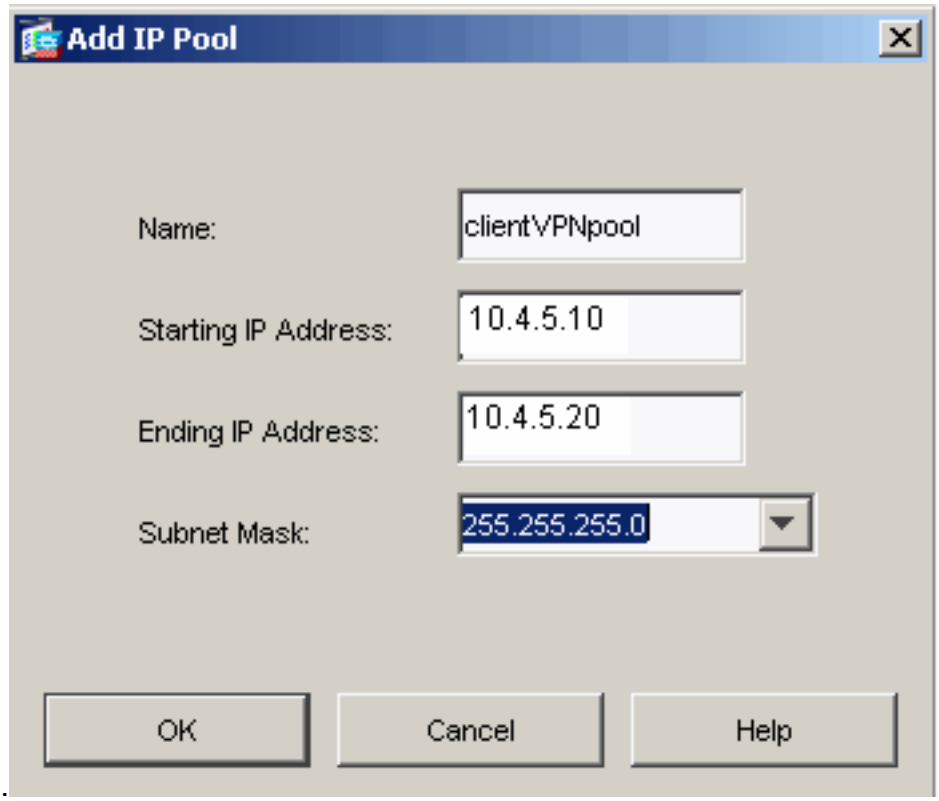
1. IPsec 변형 집합을 추가하고 터널 모드 대신 전송 모드를 사용하도록 IPsec을 지정합니다.이렇게 하려면 Configuration(컨피그레이션) > **VPN > IPSec > Transform Sets(변형 집합)**를 선택하고 **Add(추가)**를 클릭합니다.변형 집합 창이 표시됩니다
   .



2. 변형 집합을 추가하려면 다음 단계를 완료합니다.변형 집합의 이름을 입력합니다.ESP 암호화 및 ESP 인증 방법을 선택합니다.모드를 Transport(전송)로 **선택합니다**.**확인**을 **클릭합니다**



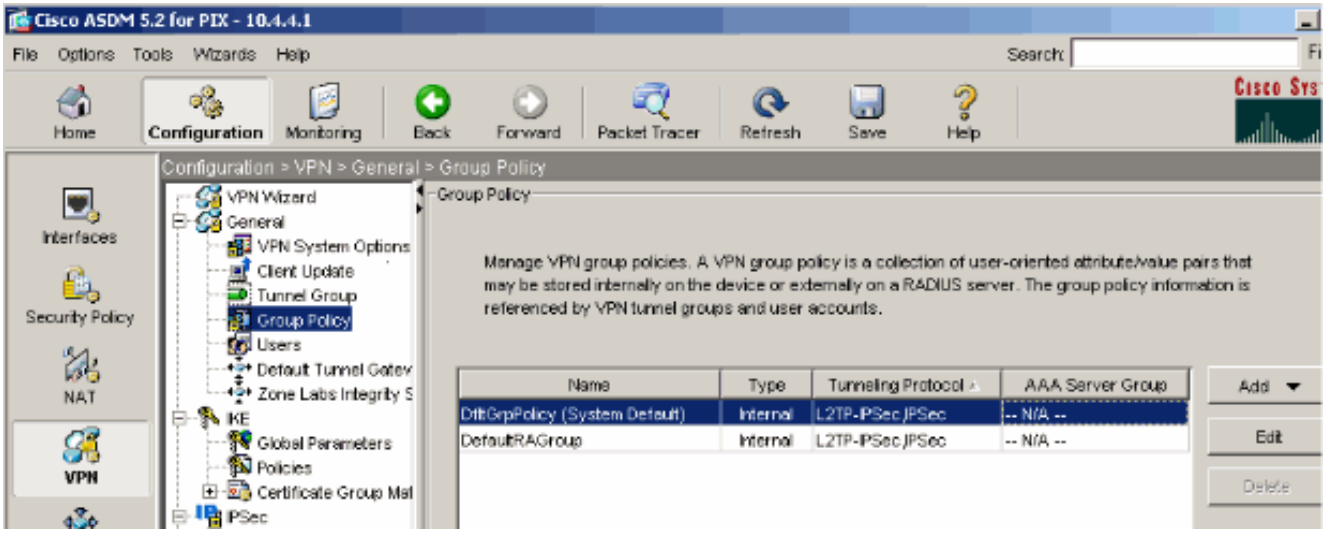
3. 주소 할당 방법을 구성하려면 다음 단계를 완료하십시오.이 예에서는 IP 주소 풀을 사용합니다.Configuration **> VPN > IP Address Management > IP Pools를 선택합니다**.Add(**추가)를 클릭합니다**.Add IP Pool 대화 상자가 나타납니다.새 IP 주소 풀의 이름을 입력합니다.시작 및 종료 IP 주소를 입력합니다.서브넷 마스크를 입력하고 **확인**을 클릭합니다



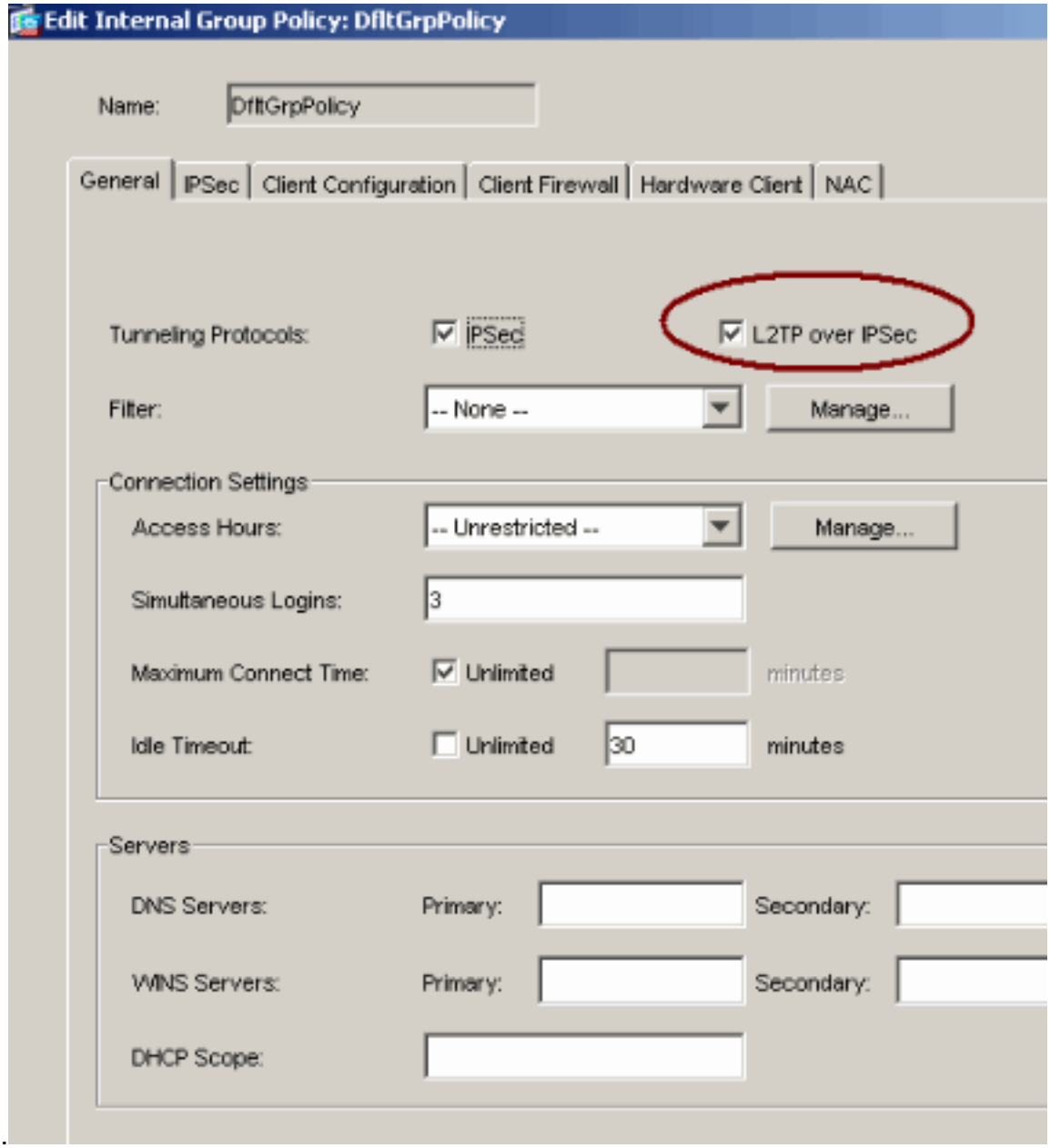
.

4. L2TP over IPsec을 그룹 정책에 대한 유효한 VPN 터널링 프로토콜로 구성하려면 Configuration(컨피그레이션) > VPN > General(일반) > Group Policy(그룹 정책)를 선택합니다.Group Policy 창이 표시됩니다

.



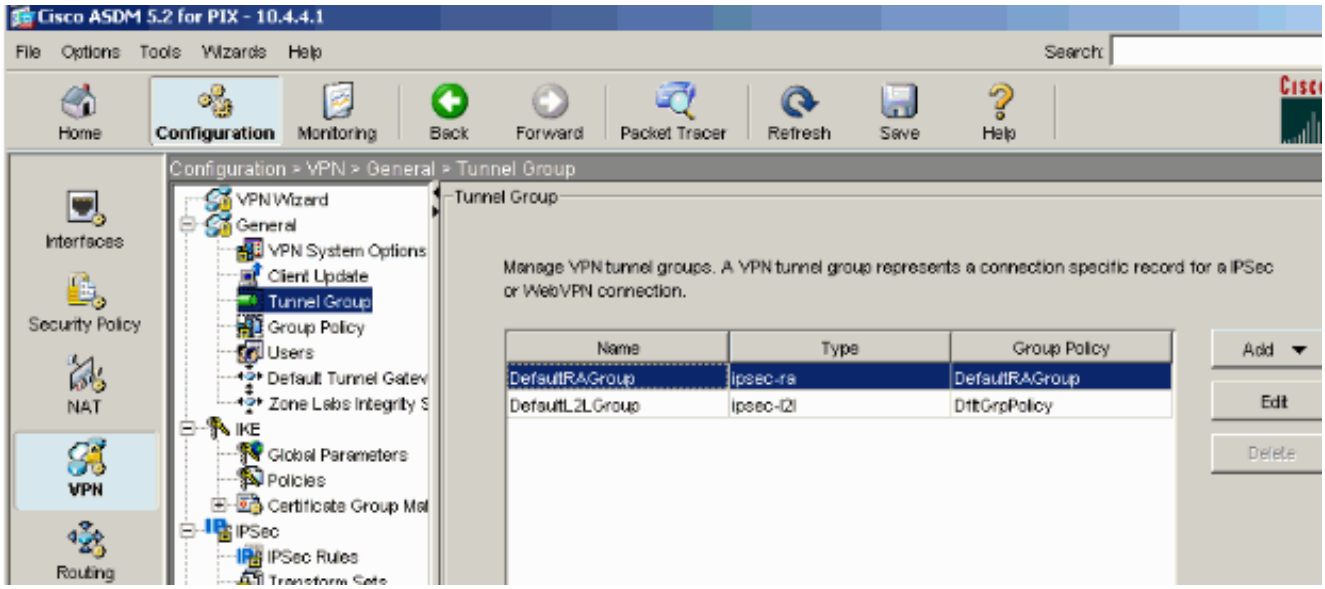
5. 그룹 정책(DiffGrpPolicy)을 선택하고 편집을 **클릭합니다**.Edit Group Policy(그룹 정책 수정) 대화 상자가 표시됩니다.그룹 정책**에** 대한 프로토콜을 활성화하려면 L2TP over IPSec을 선택한 다음 **OK**(확인)를 클릭합니다



.

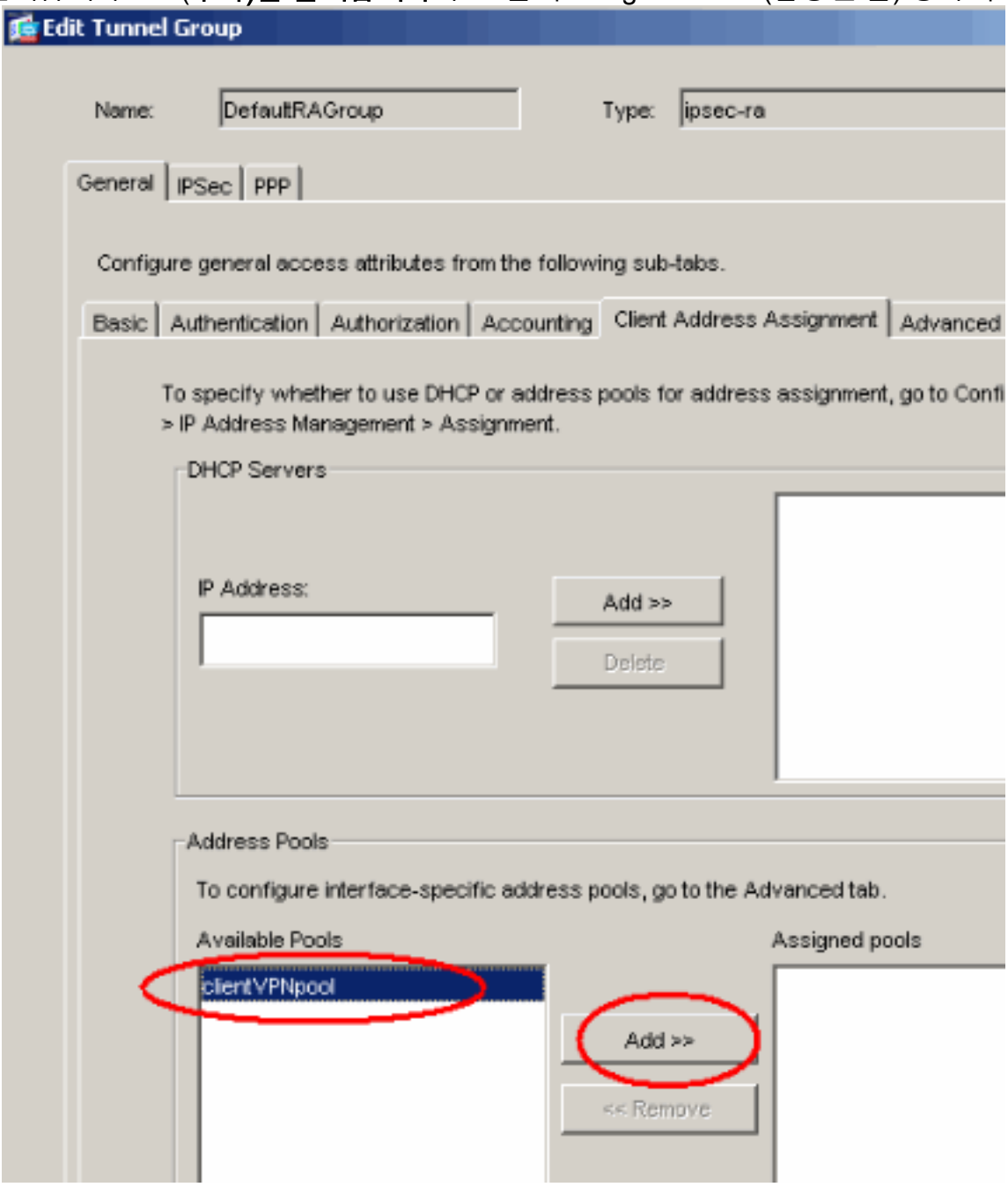
6. 터널 그룹에 IP 주소 풀을 할당하려면 다음 단계를 완료합니다.Configuration **> VPN > General > Tunnel Group을 선택합니다**.Tunnel Group 창이 나타나면 테이블에서 터널 그룹(DefaultRAGroup)을 선택합니다.Edit를 **클릭합니다**

.



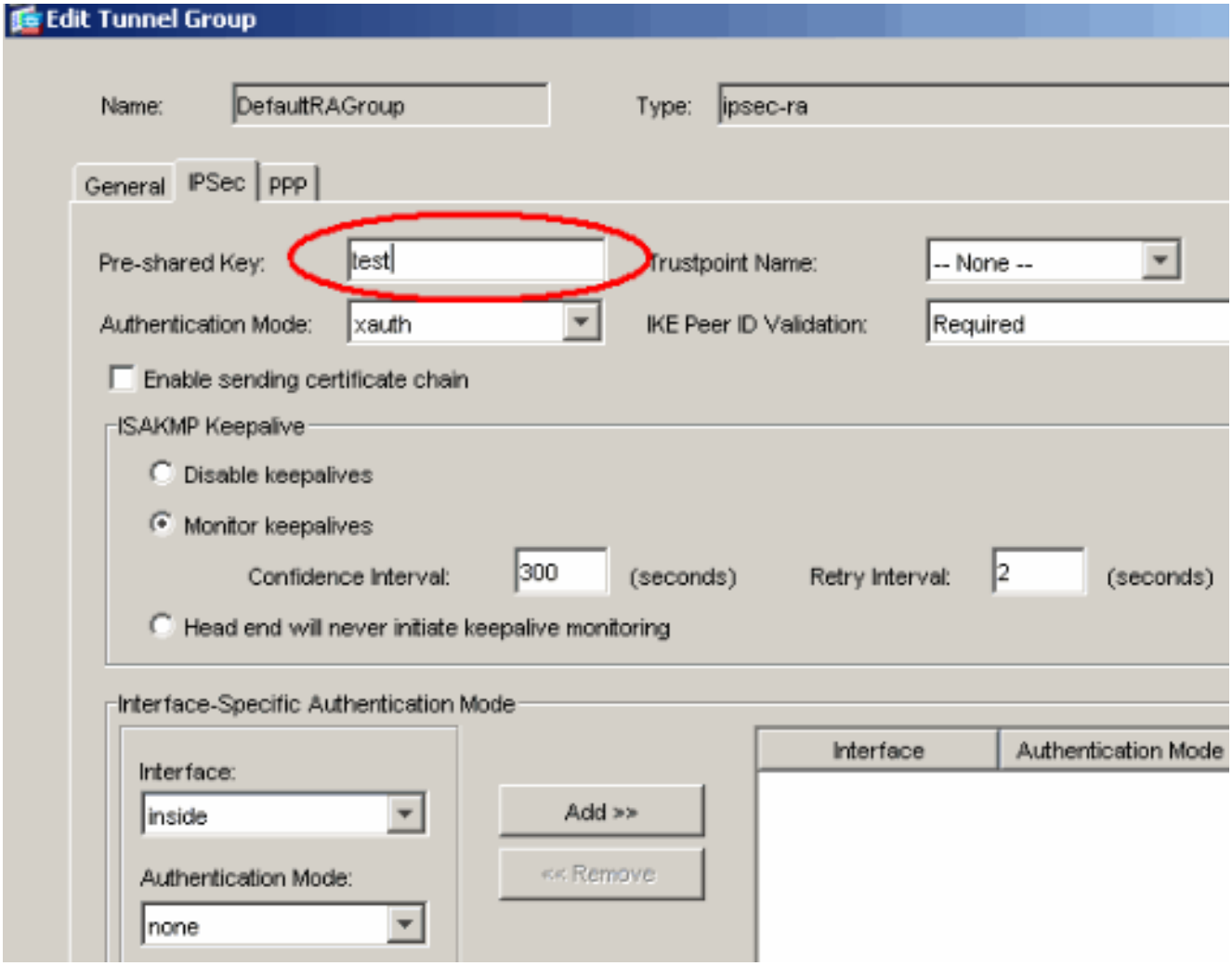
7. Edit Tunnel Group(터널 그룹 수정) 창이 나타나면 다음 단계를 완료합니다.일반 탭에서 클라

이언트 주소 할당 탭으로 이동합니다.Address Pools(주소 풀) 영역에서 터널 그룹에 할당할 주소 풀을 선택합니다.Add(**추가)를 클릭합니다**.주소 풀이 Assigned Pools(할당된 풀) 상자에 나타납니다.

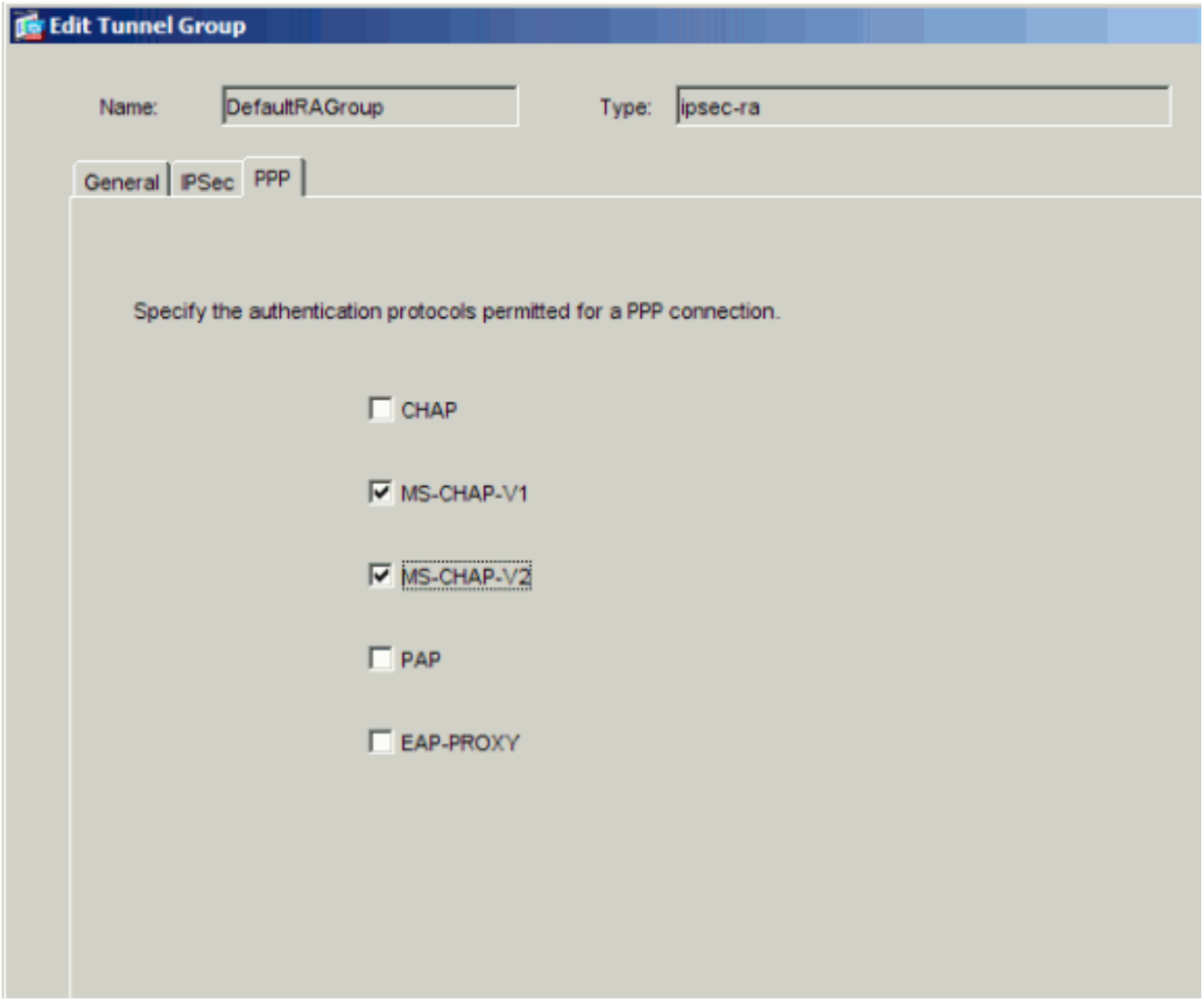


8. 사전 공유 키를 설정하려면 IPSec 탭으로 이동하여 **사전 공유 키**를 입력하고 **확인**을 클릭합니다

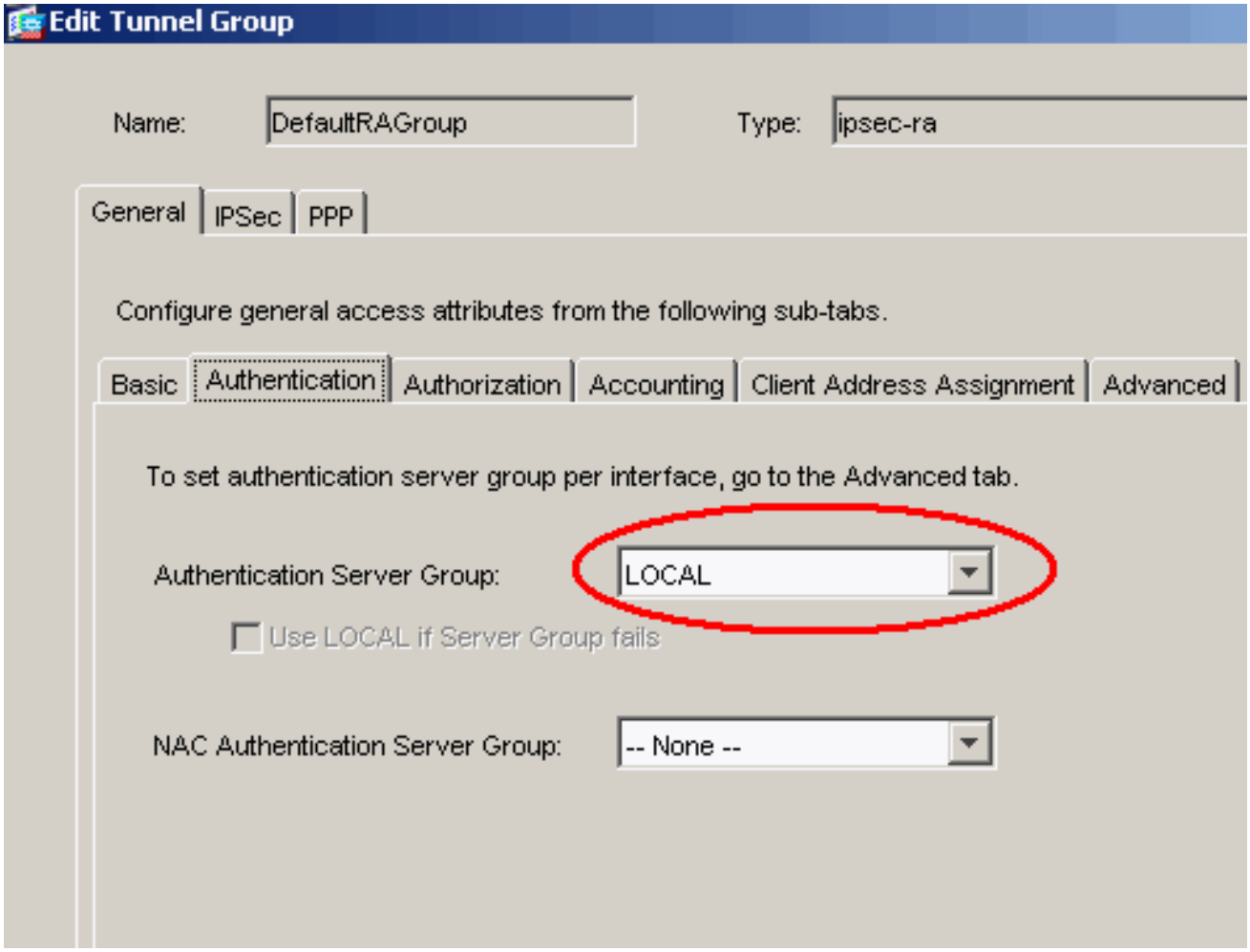
.



9. L2TP over IPsec은 PPP 인증 프로토콜을 사용합니다.터널 그룹의 PPP 탭에서 PPP 연결에 허용된 프로토콜을 지정합니다.인증을 위해 **MS-CHAP-V1** 프로토콜을 선택합니다
.



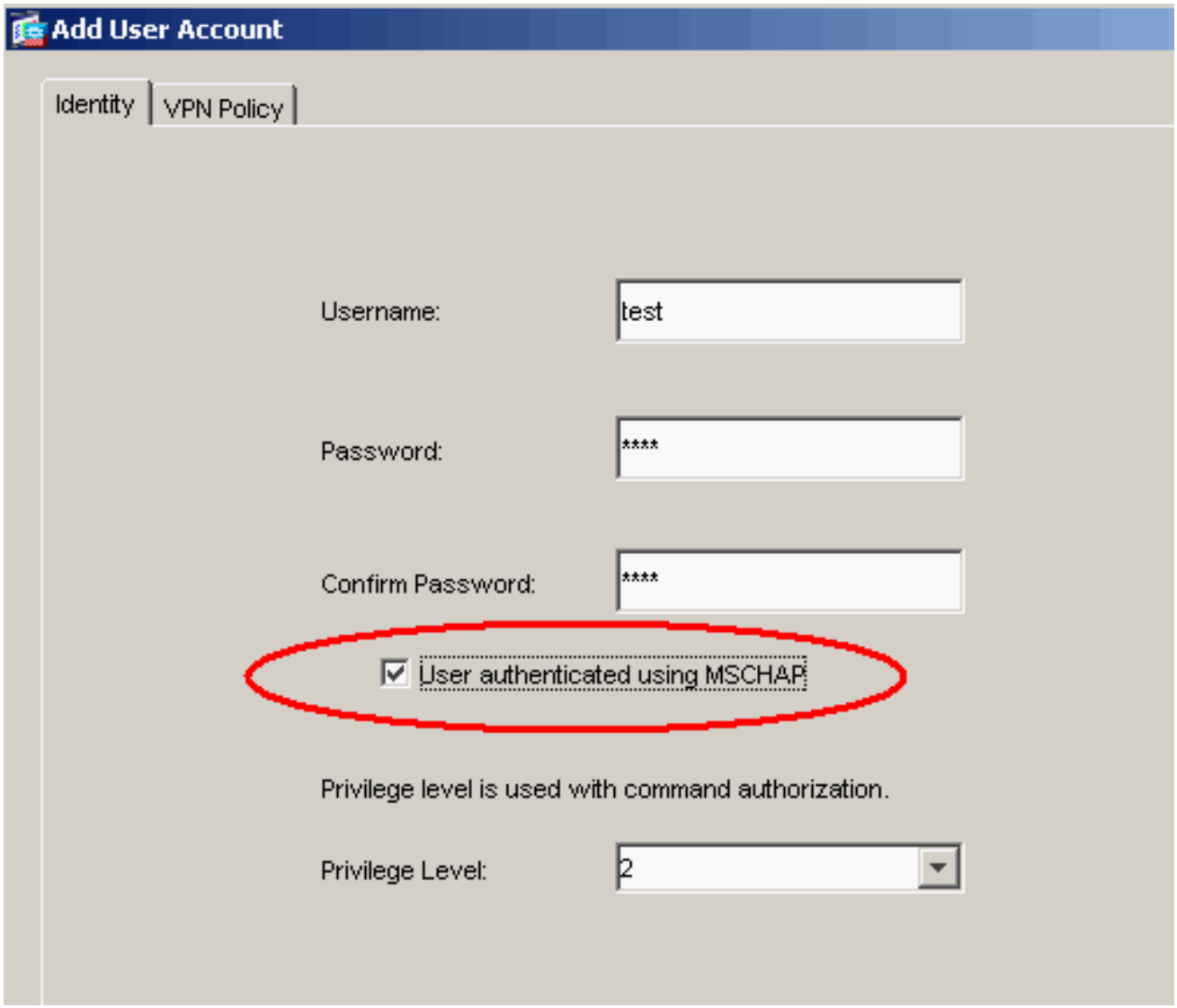
10. L2TP over IPsec 연결을 시도하는 사용자를 인증하는 방법을 지정합니다.인증 서버 또는 자체 로컬 데이터베이스를 사용하도록 보안 어플라이언스를 구성할 수 있습니다.이렇게 하려면 터널 그룹의 Authentication(인증) 탭으로 이동합니다.기본적으로 보안 어플라이언스는 로컬 데이터베이스를 사용합니다.Authentication Server Group(인증 서버 그룹) 드롭다운 목록에 LOCAL(로컬)이 표시됩니다.인증 서버를 사용하려면 목록에서 하나를 선택합니다.**참고:** 보안 어플라이언스는 로컬 데이터베이스에서 PPP 인증 PAP 및 Microsoft CHAP 버전 1 및 2만 지원합니다.EAP 및 CHAP는 프록시 인증 서버에 의해 수행됩니다.따라서 원격 사용자가 EAP 또는 CHAP로 구성된 터널 그룹에 속하고 보안 어플라이언스가 로컬 데이터베이스를 사용하도록 구성된 경우 해당 사용자는 연결할 수 없습니다
.



참고: 터널 그룹 정책**을** 터널 그룹에 연결하고 터널 그룹 전환을 활성화할 수 있도록 터널 그룹 컨피그레이션으로 돌아가려면 Configuration(컨피그레이션) > **VPN > General(일반) > Tunnel Group(터널 그룹)**을 선택합니다(선택 사항). Tunnel Group 창이 나타나면 터널 그룹을 선택하고 Edit를 **클릭합니다.참고:** Tunnel Group Switching을 사용하면 보안 어플라이언스에서 L2TP over IPsec 연결을 설정하는 다른 사용자를 다른 터널 그룹과 연결할 수 있습니다.각 터널 그룹에는 고유한 AAA 서버 그룹 및 IP 주소 풀이 있으므로 사용자는 해당 터널 그룹에 특정한 방법을 통해 인증할 수 있습니다.이 기능을 사용하면 사용자 이름만 보내는 대신 사용자 이름과 그룹 이름을 username@group_name 형식으로 보냅니다. 여기서 "@"는 구성할 수 있는 구분 기호를 나타내고 그룹 이름은 보안 어플라이언스에 구성된 터널 그룹의 이름입니다.**참고:** Tunnel Group Switching(터널 그룹 전환)은 Strip Group(스트립 그룹) 처리에 의해 활성화되며, 보안 어플라이언스는 VPN 클라이언트에서 제공하는 사용자 이름에서 그룹 이름을 가져와서 사용자 연결에 대한 터널 그룹을 선택할 수 있습니다.그러면 보안 어플라이언스는 권한 부여 및 인증을 위해 사용자 이름의 사용자 부분만 전송합니다.그렇지 않으면(비활성화된 경우) 보안 어플라이언스는 영역을 포함하여 전체 사용자 이름을 전송합니다 .Tunnel Group Switching을 활성화하려면 **Strip the realm from username before passing it on to the AAA server(AAA 서버에 전달하기 전에 사용자 이름에서 영역 제거**를 선택하고 **Strip the group from username(그룹을 사용자 이름에서 제거한 후 AAA 서버로 전달)을** 선택합니다.그런 다음 **확인**을 클릭합니다.

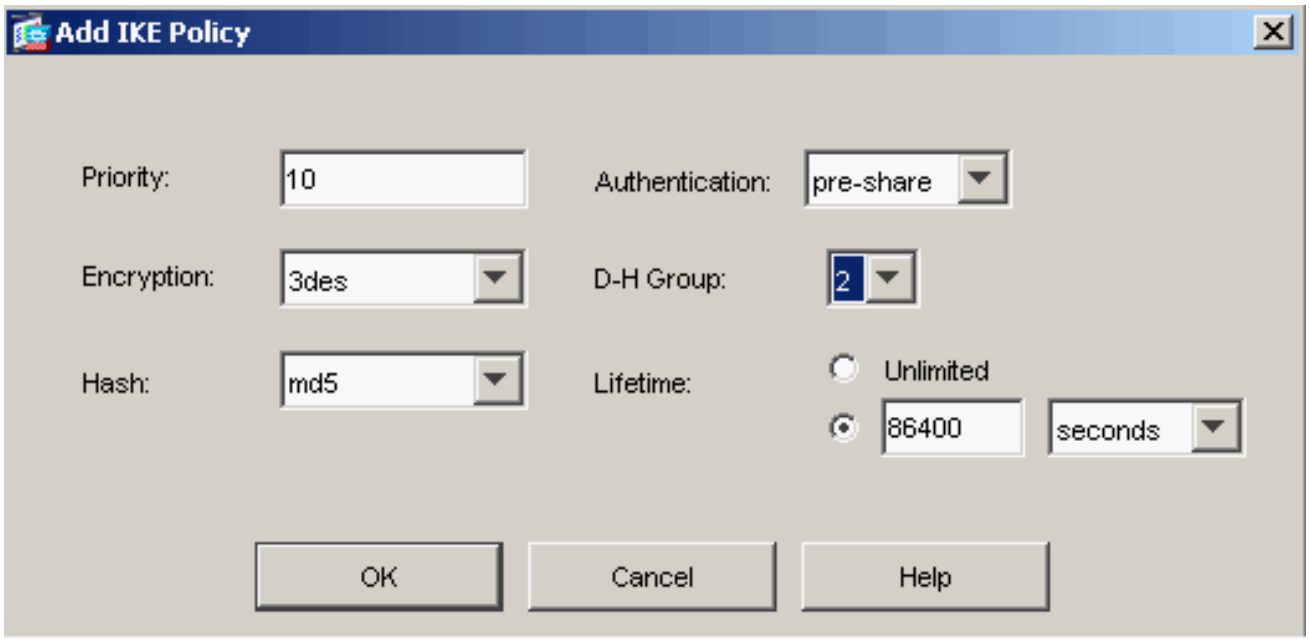
11. 로컬 데이터베이스에서 사용자를 생성하려면 다음 단계를 완료합니다.Configuration > **Properties > Device Administration > User Accounts를 선택합니다**.Add(**추가)를 클릭합니다** .사용자가 Microsoft CHAP 버전 1 또는 2를 사용하는 L2TP 클라이언트이고 보안 어플라이언스가 로컬 데이터베이스에 대해 인증하도록 구성된 경우 MSCHAP를 활성화하려면 **User Authenticated using MSCHAP(MSCHAP를 사용하여 사용자 인증**)를 선택해야 합니다.**확인을 클릭합니다**

.



12. Configuration(**구성) > VPN > IKE > Policies(정책)를** 선택하고 **Add(추가)**를 클릭하여 Phase I에 대한 IKE 정책을 생성합니다. 계속하려면 **OK(확인)를** 클릭합니다

.



13. (선택 사항) NAT 장치 뒤에 있는 여러 L2TP 클라이언트가 보안 어플라이언스에 대한 L2TP over IPsec 연결을 시도할 것으로 예상하는 경우 ESP 패킷이 하나 이상의 NAT 디바이스를

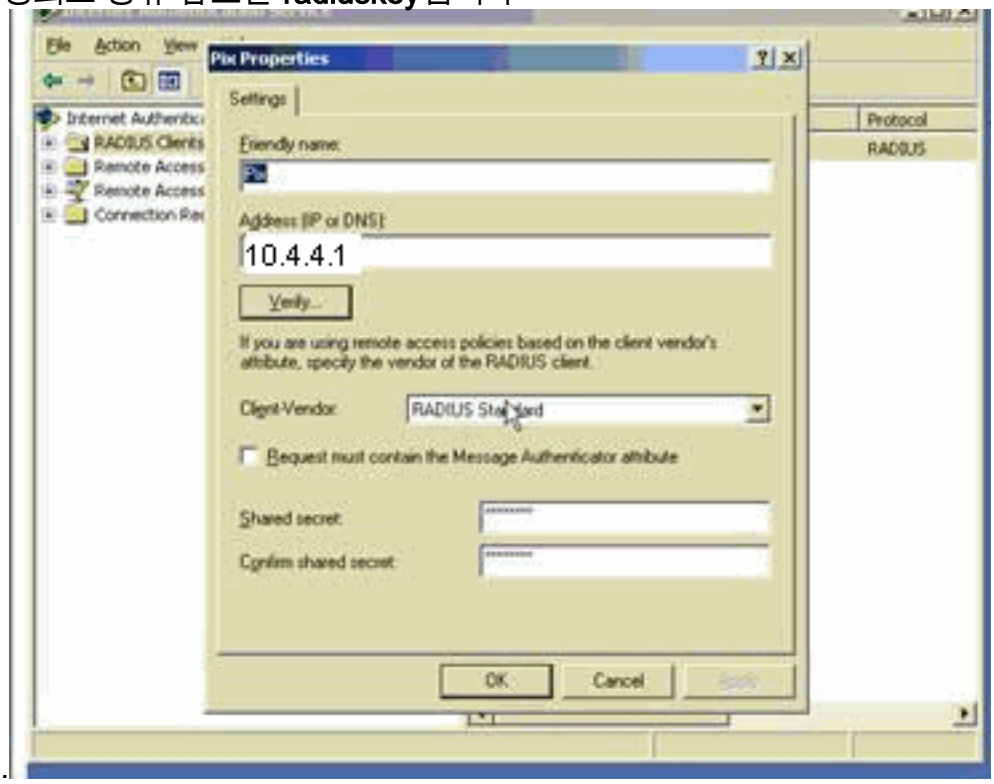
통과할 수 있도록 NAT 통과를 활성화해야 합니다.이 작업을 수행하려면 다음 단계를 완료하십시오.Configuration **> VPN > IKE > Global Parameters를 선택합니다**.인터페이스에서 **ISAKMP**가 활성화되었는지 확인합니다.Enable **IPSec over NAT-T를 선택합니다**.**확인**을 **클릭합니다**.

Microsoft Windows 2003 Server(IAS 구성 포함)

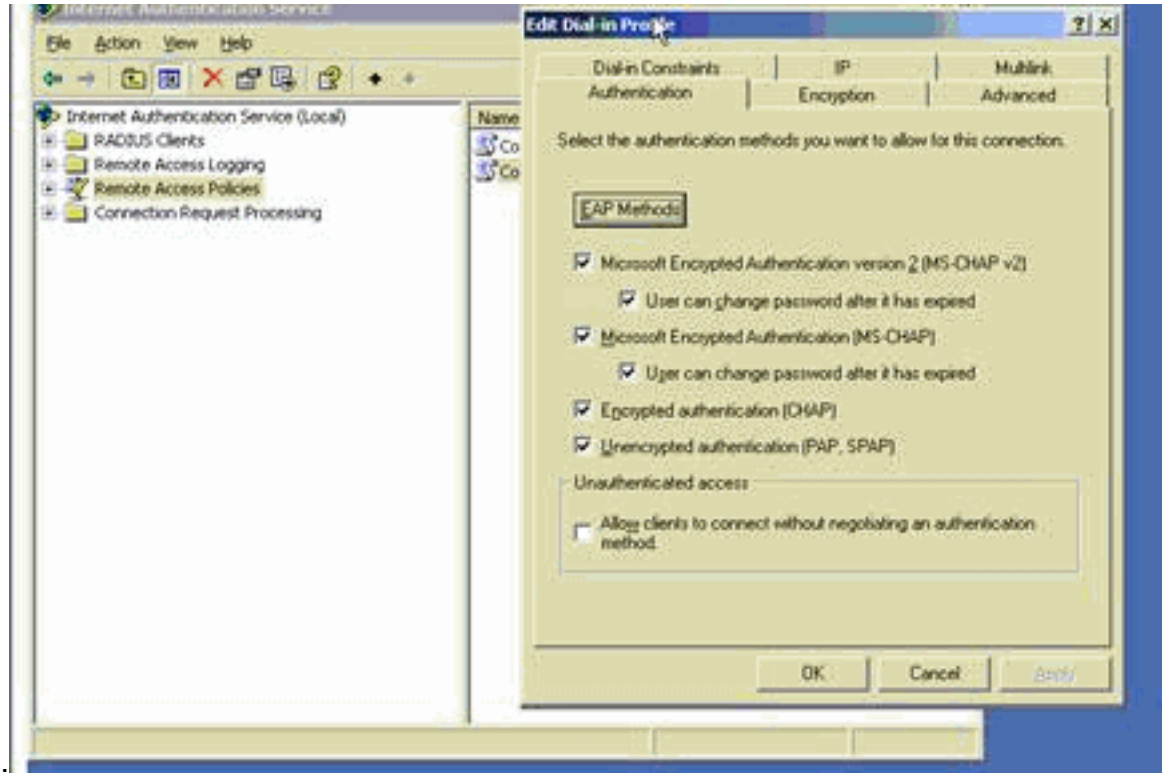
Microsoft Windows 2003 서버를 IAS로 구성하려면 다음 단계를 완료하십시오.

참고: 이 단계에서는 IAS가 로컬 시스템에 이미 설치되어 있다고 가정합니다.그렇지 않은 경우 **제어판 > 프로그램 추가/제거를** 통해 **추가합니다**.

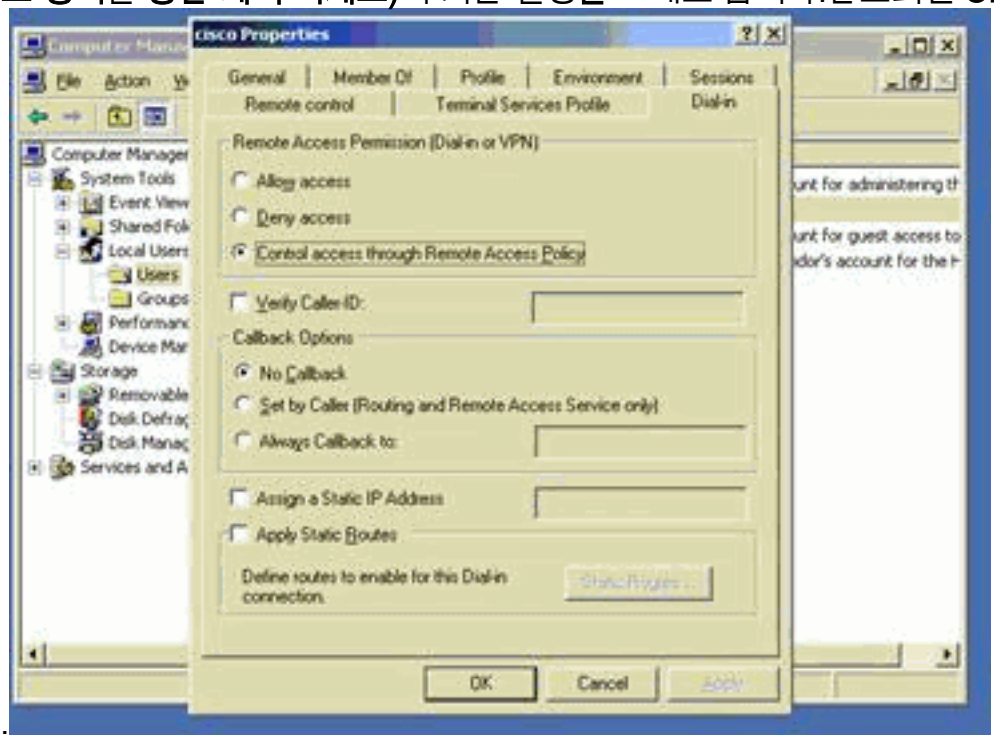
1. Administrative **Tools(관리 툴) > Internet Authentication Service(인터넷 인증 서비스)**를 선택하고 마우스 오른쪽 버튼으로 **RADIUS Client(RADIUS 클라이언트)**를 클릭하여 새 RADIUS 클라이언트를 추가합니다.클라이언트 정보를 입력한 후 **OK**를 클릭합니다.이 예에서는 IP 주소가 10.4.4.1인 "Pix"라는 클라이언트를 보여 줍니다. Client-Vendor는 **RADIUS Standard**로 설정되고 공유 암호는 **radiuskey**입니다



2. Remote **Access Policies(원격 액세스 정책)**를 선택하고 Connections to **Other Access Servers(다른 액세스 서버에 대한 연결)를** 마우스 오른쪽 버튼으로 클릭한 다음 Properties(속성)를 **선택합니다**.
3. 원격 액세스 권한 부여 옵션**이** 선택되었는지 확인합니다.
4. Edit **Profile(프로필 수정)**을 클릭하고 다음 설정을 확인합니다.Authentication(인증) 탭에서 **Unencrypted authentication (PAP, SPAP)을** 선택합니다.Encryption(암호화) 탭에서 No Encryption(암호화 **없음)** 옵션이 선택되었는지 확인합니다.완료되면 **OK**(확인)를 클릭합니다



5. 관리 **도구 > 컴퓨터 관리 > 시스템 도구 > 로컬 사용자 및 그룹을 선택하고 사용자**를 마우스 오른쪽 단추로 클릭한 다음 **새 사용자**를 선택하여 로컬 컴퓨터 계정에 사용자를 추가합니다.
6. Cisco 비밀번호 **password1**을 사용하여 사용자를 추가하고 이 프로파일 정보를 확인합니다 .General(일반) 탭에서 User Must Change Password(사용자가 비밀번호를 변경해야 함) 옵션 대신 **Password Never Expired(비밀번호 만료되지** 않음) 옵션이 선택되어 있는지 확인합니다 .Dial-in 탭에서 Allow access(**액세스 허용**) 옵션을 선택하거나 **Control access access(원격 액세스 정책**을 **통한 제어 액세스)**의 기본 설정**을** 그대로 둡니다.완료되면 **OK**(확인)를 클릭합니다.



Active Directory를 사용하는 L2TP over IPSec에 대한 확장 인증

L2tp 연결에 대한 인증이 Active Directory에서 수행되도록 하려면 ASA에서 이 컨피그레이션을 사용합니다.

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

또한 L2tp 클라이언트에서 **Advanced Security Settings(Custom)로** 이동하여 Unencrypted **Password(PAP)** 옵션만 선택합니다.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

- **show crypto ipsec sa** - 피어에 있는 현재 IKE SA(보안 연결)를 모두 표시합니다.

```
pixfirewall#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1

      access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
      local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0)
      remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701)
      current_peer: 192.168.0.2, username: test
      dynamic allocated peer ip: 10.4.5.15

#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
       #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C16F05B8

    inbound esp sas:
      spi: 0xEC06344D (3959829581)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y

outbound esp sas:
      spi: 0xC16F05B8 (3245278648)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 3, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 3335
         IV size: 8 bytes
         replay detection support: Y
```

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.

```
pixfirewall#show crypto isakmp sa
```

```
   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.0.2
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

- **show vpn-sessiondb** - L2TP over IPsec 연결에 대한 자세한 정보를 보기 위해 사용할 수 있는 프로토콜 필터를 포함합니다.전역 컨피그레이션 모드의 전체 명령은 **show vpn-sessoindb detailed remote filter protocol l2tpOverIpsec입니다**.다음 예에서는 단일 L2TP over IPsec 연결의 세부 정보를 보여줍니다.

```
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

Session Type: Remote Detailed

Username     : test
Index        : 1
Assigned IP  : 10.4.5.15             Public IP    : 192.168.0.2
Protocol     : L2TPOverIPSec         Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 1336                  Bytes Rx     : 14605
Client Type  :                       Client Ver   :
Group Policy : DefaultRAGroup
Tunnel Group : DefaultRAGroup
Login Time   : 18:06:08 UTC Fri Jan 1 1993
Duration     : 0h:04m:25s
Filter Name  :
NAC Result   : N/A
Posture Token:

IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1


IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28536 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 172.16.1.1/255.255.255.255/17/1701
  Remote Addr  : 192.168.0.2/255.255.255.255/17/1701
  Encryption   : 3DES                  Hashing      : MD5
  Encapsulation: Transport
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3333 Seconds
  Idle Time Out: 30 Minutes            Idle TO Left : 30 Minutes
  Bytes Tx     : 1336                  Bytes Rx     : 14922
  Pkts Tx      : 25                    Pkts Rx      : 156


L2TPOverIPSec:
  Session ID   : 3
  Username     : test
  Assigned IP  : 10.4.5.15
  Encryption   : none                  Auth Mode    : msCHAPV1
  Idle Time Out: 30 Minutes            Idle TO Left : 30 Minutes
  Bytes Tx     : 378                   Bytes Rx     : 13431
```

```
      Pkts Tx      : 16                    Pkts Rx      : 146
```

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅을 위한 정보를 제공합니다.샘플 디버그 출력도 표시됩니다.

문제 해결 명령

특정 명령은 Output Interpreter 도구(등록된 고객만 해당)에서 지원되므로 **show** 명령 출력의 분석을 볼 수 있습니다.

참고: debug **명령**을 사용하기 전에 Debug 명령 및 IP 보안 문제 해결 - Understanding and Using debug Commands(디버그 명령 이해 및 사용)에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec 7** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp 7** - 1단계의 ISAKMP 협상을 표시합니다.

샘플 디버그 출력

PIX 방화벽

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
ID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
# 2 acceptable  Matches global IKE entry # 2
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
+ extended capabilities payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
yload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo
ad
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V
```

```
endor ID payload (version: 1.0.0, capabilities: 20000001)
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco
 ASA GW VID
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing keys for Responder...
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (
13) + VENDOR (13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ
ously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting dpd vid payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length :
80

!--- Phase 1 completed succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, PHASE 1 COMPL
ETED
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection:
None
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do
es not support keep-alives (type = None)
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P1 rekey timer: 21600 seconds.
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NONE (0) total length : 164
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo
te Proxy Host data in ID Payload:  Address 192.168.0.2, Protocol 17, Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca
l Proxy Host data in ID Payload:  Address 172.16.1.1, Protocol 17, Port 1701

!--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP
= 192.168.0.2, L2TP/IPSec se
```

ssion detected.
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed
old sa not found by addr
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe
er configured for crypto map: outside_dyn_map
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S
A Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti
ng SPI!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 SPI from key engine: SPI = 0xce9f6e19

!--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, **oakley**
constucting quick mode
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting blank hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting IPSec nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting proxy ID
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi
tting Proxy Id:
  Remote host: 192.168.0.2 Protocol 17 Port 1701
  Local host: 172.16.1.1 Protocol 17 Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting qm hash payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b
84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N
ONE (0) total length : 144
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading
 all IPSEC SAs
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
ing Quick Mode Key!
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego
tiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI
= 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
 a KEY_ADD msg for SA: SPI = 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher
: received KEY_UPDATE, spi 0xce9f6e19
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
g P2 rekey timer: 3059 seconds.

!--- Phase 2 completes succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add
L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto
ipsec 7**
pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09
    Rule ID: 0x028D78D8
IPSEC: Deleted inbound permit rule, SPI 0x71933D09
    Rule ID: 0x02831838
IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
    Rule ID: 0x029134D8

```
IPSEC: Deleted inbound VPN context, SPI 0x71933D09
    VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
    Rule ID: 0x028DAC90
IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
    Rule ID: 0x02912AF8
IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
    VPN handle: 0x0048468C
IPSEC: New embryonic SA created @ 0x01BFCF80,
    SCB: 0x01C262D0,
    Direction: inbound
    SPI      : 0x45C3306F
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
    SCB: 0x028D1B38,
    Direction: outbound
    SPI      : 0x370E8DD1
    Session ID: 0x0000000C
    VPIF num  : 0x00000001
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    Dst mask: 255.255.255.255
    Src ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Dst ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
    Src addr: 172.16.1.1
    Src mask: 255.255.255.255
    Dst addr: 192.168.0.2
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
```

```
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x370E8DD1
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: Completed host IBSA update, SPI 0x45C3306F
IPSEC: Creating inbound VPN context, SPI 0x45C3306F
    Flags: 0x00000206
    SA   : 0x01BFCF80
    SPI  : 0x45C3306F
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x0048C164
    SCB  : 0x01C262D0
    Channel: 0x01693F08
IPSEC: Completed inbound VPN context, SPI 0x45C3306F
    VPN handle: 0x0049107C
IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
    Flags: 0x00000205
    SA   : 0x0283A3A8
    SPI  : 0x370E8DD1
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0049107C
    SCB  : 0x028D1B38
    Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
    VPN handle: 0x0048C164
IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
    Rule ID: 0x02826540
IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
    Rule ID: 0x028D78D8
IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Dst ports
      Upper: 1701
      Lower: 1701
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F
    Rule ID: 0x02831838
IPSEC: New inbound decrypt rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
```

```
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
    Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
    Src addr: 192.168.0.2
    Src mask: 255.255.255.255
    Dst addr: 172.16.1.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x45C3306F
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
    Rule ID: 0x02912E50
```

ASDM을 사용하여 문제 해결

ASDM을 사용하여 로깅을 활성화하고 로그를 볼 수 있습니다.

1. 로깅을 활성화하려면 **Configuration > Properties > Logging > Logging Setup**을 선택하고 **Enable Logging**을 선택한 다음 **Apply**를 클릭합니다.
2. Monitoring(**모니터링**) > **Logging(로깅)** > **Log Buffer(로그 버퍼)** > **On Logging Level(로깅 레벨)**을 선택하고 **Logging Buffer(로깅 버퍼)**를 선택한 다음 View(**보기**)를 클릭하여 로그를 확인합니다.

문제/장애:빈번한 연결 끊기

유휴/세션 시간 초과

유휴 시간 초과가 30분(기본값)으로 설정된 경우, 트래픽이 터널을 통과하지 않은 후 30분 동안 터널을 삭제함을 의미합니다.유휴 시간 제한 설정에 관계없이 30분 후에 VPN 클라이언트의 연결이 끊어지고 PEER_DELETE-IKE_DELETE_UNSPECIFIED 오류 메시지가 나타납니다.

터널이 항상 작동되고 터널이 삭제되지 않도록 하려면 유휴 시간 제한 및 세션 시간 제한을 none으로 구성합니다.

사용자 시간 제한 기간을 **구성하려면** group-policy 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 vpn-idle-timeout 명령을 입력합니다.

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

그룹 정책 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 vpn-session-timeout 명령을 사용하여 VPN 연결에 대한 최대 시간을 구성합니다.

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-session-timeout none
```

Windows Vista 문제 해결

동시 사용자

Windows Vista L2TP/IPsec은 둘 이상의 동시 사용자가 헤드 엔드 PIX/ASA에 연결하지 못하도록 하는 몇 가지 아키텍처 변경 사항을 도입했습니다.이 동작은 Windows 2K/XP에서 발생하지 않습니다.Cisco는 릴리스 7.2(3) 이상에서 이 변경에 대한 해결 방법을 구현했습니다.

Vista PC에서 연결할 수 없음

Windows Vista 컴퓨터가 L2TP 서버에 연결할 수 없는 경우 DefaultRAGroup의 ppp 특성 아래에 ONLY mschap-v2를 구성했는지 확인합니다.

관련 정보

- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- Cisco PIX 500 Series 보안 어플라이언스
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco PIX 방화벽 소프트웨어 제품 지원
- Cisco Secure PIX Firewall 명령 참조
- RADIUS 지원 페이지
- IPSec 협상/IKE 프로토콜 지원 페이지
- RFC(Request for Comments)
- 레이어 2 터널 프로토콜(L2TP)
- 기술 지원 및 문서 – Cisco Systems