PIX IPSec 5.2 이상에 AAA 인증(Xauth)을 추가하는 방법

목차

소개

RADIUS 및 TACACS+ 인증 및 어카운팅, 그리고 어느 정도 권한 부여는 PIX에서 종료되는 Cisco Secure VPN Client 1.1 및 Cisco VPN 3000 2.5 하드웨어 클라이언트 터널에 대해 수행됩니다.인증, 권한 부여 및 계정 관리(AAA) 액세스 목록 지원이 포함된 이전 버전의 PIX 5.2 이상 확장 인증(Xauth)에 대한 변경 사항을 통해 인증된 사용자가 Cisco VPN 3000 Client 2.5 Xauth 종료를 액세스하고 지원할 수 있는 항목을 제어합니다.vpn **group split-tunneling** 명령을 사용하면 VPN 3000 Client가 PIX 내부 네트워크와 기타 네트워크(예: 인터넷)에 동시에 연결할 수 있습니다.PIX 5.3 이상에서는 이전 버전의 코드에 대한 AAA 변경 사항이 RADIUS 포트를 구성할 수 있다는 것입니다 .PIX 6.0에서는 VPN Client 3.x 지원이 추가됩니다.이를 위해서는 Diffie-Hellman 그룹 2가 필요합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 소프트웨어 릴리스 5.2.1
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 2.5 클라이언트 또는 VPN 클라이언트 3.x**참고:** Cisco VPN Client 릴리스 3.0.x는 6.0 이전 버전의 PIX에서 작동하지 않습니다. 자세한 내용은 IPsec/PPTP/L2TP를 지원하는 Cisco 하드웨어 및 VPN 클라이언트를 참조하십시오.

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.

표기 규칙

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

배경 정보

PIX Firewall 소프트웨어 릴리스 6.2에서는 ACS(Access Control Server)에서 PIX 방화벽에 대한 ACL(Access Control List)을 다운로드할 수 있습니다. 이렇게 하면 AAA 서버에서 사용자별 ACL을 구성하여 사용자별 ACL 권한을 제공할 수 있습니다.그런 다음 ACS를 통해 PIX 방화벽에 다운로드할 수 있습니다.이 기능은 RADIUS 서버에서만 지원됩니다.TACACS+ 서버에서는 지원되지 않습니다.

디버그 단계

다음 디버그 단계를 완료합니다.

1. AAA 인증을 추가하기 전에 PIX Xauth 컨피그레이션이 작동하는지 확인합니다.AAA를 구현하기 전에 트래픽을 전달할 수 없는 경우 나중에 트래픽을 전달할 수 없습니다.
2. PIX에서 어떤 종류의 로깅을 활성화합니다.로드가 많은 시스템에서 **logging console 디버깅** 명령을 실행하지 마십시오.logging buffered **디버깅** 명령을 실행할 수 있습니다.그런 다음 **show logging** 명령을 실행합니다.로깅은 시스템 메시지 로그(syslog) 서버로 전송하고 검사할 수도 있습니다.
3. TACACS+ 또는 RADIUS 서버에서 디버깅을 설정합니다.모든 서버에 이 옵션이 있습니다.

PIX의 디버그 명령

- **debug crypto ipsec sa** - 이 debug 명령은 IPsec 이벤트를 표시합니다.
- **debug crypto isakmp sa** - 이 debug 명령은 IKE(Internet Key Exchange) 이벤트에 대한 메시지를 표시합니다.
- **debug crypto isakmp engine** — 이 debug 명령은 IKE 이벤트에 대한 메시지를 표시합니다.

클라이언트측 디버그

Cisco Secure 1.1 또는 VPN 3000 Client 2.5의 클라이언트측 디버그를 로그 뷰어에서 볼 수 있도록 합니다.

AAA 서버 프로파일

Cisco Secure UNIX TACACS+

```
user = noacl{
password = clear "********"
service=shell {
}
}
user = pixb{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
user = 3000full{
  password = clear "********"
  service=shell {
  }
  }
user = 3000partial{
  password = clear "********"
  service=shell {
  }
  }
```

Windows TACACS+용 Cisco Secure ACS

noacl, 3000full 및 3000partial 사용자는 Windows용 Cisco Secure ACS에서 사용자 이름과 비밀번호만 필요합니다.pixb 사용자는 사용자 이름, 비밀번호, 체크 인된 셸/exec 그룹, ACL이 선택되고 상자에 115가 필요합니다.

Cisco Secure UNIX RADIUS

```
user = noacl{
password = clear "********"
}
user = pixb{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
user = 3000full{
  password = clear "********"
  }
user = 3000partial{
  password = clear "********"
  }
```

Windows RADIUS용 Cisco Secure ACS

RADIUS/Cisco는 디바이스 유형입니다.noacl, 3000full 및 3000partial 사용자는 Windows용 Cisco Secure ACS에서 사용자 이름과 비밀번호만 필요합니다.Pixb 사용자는 Cisco/RADIUS 사각형 상자에 009\001 AV-Pair(공급업체별)라고 표시된 사용자 이름, 비밀번호, 체크 및 acl=115가 필요합니다 .

참고: ACL에 대한 공급업체 특성이 필요합니다.특성 11, filter-id가 잘못되었습니다.이 문제에는 Cisco 버그 ID CSCdt50422가 할당됩니다(등록된 고객만 해당). PIX 소프트웨어 릴리스 6.0.1에서 수정되었습니다.

Merit RADIUS(Cisco AV 쌍 지원)

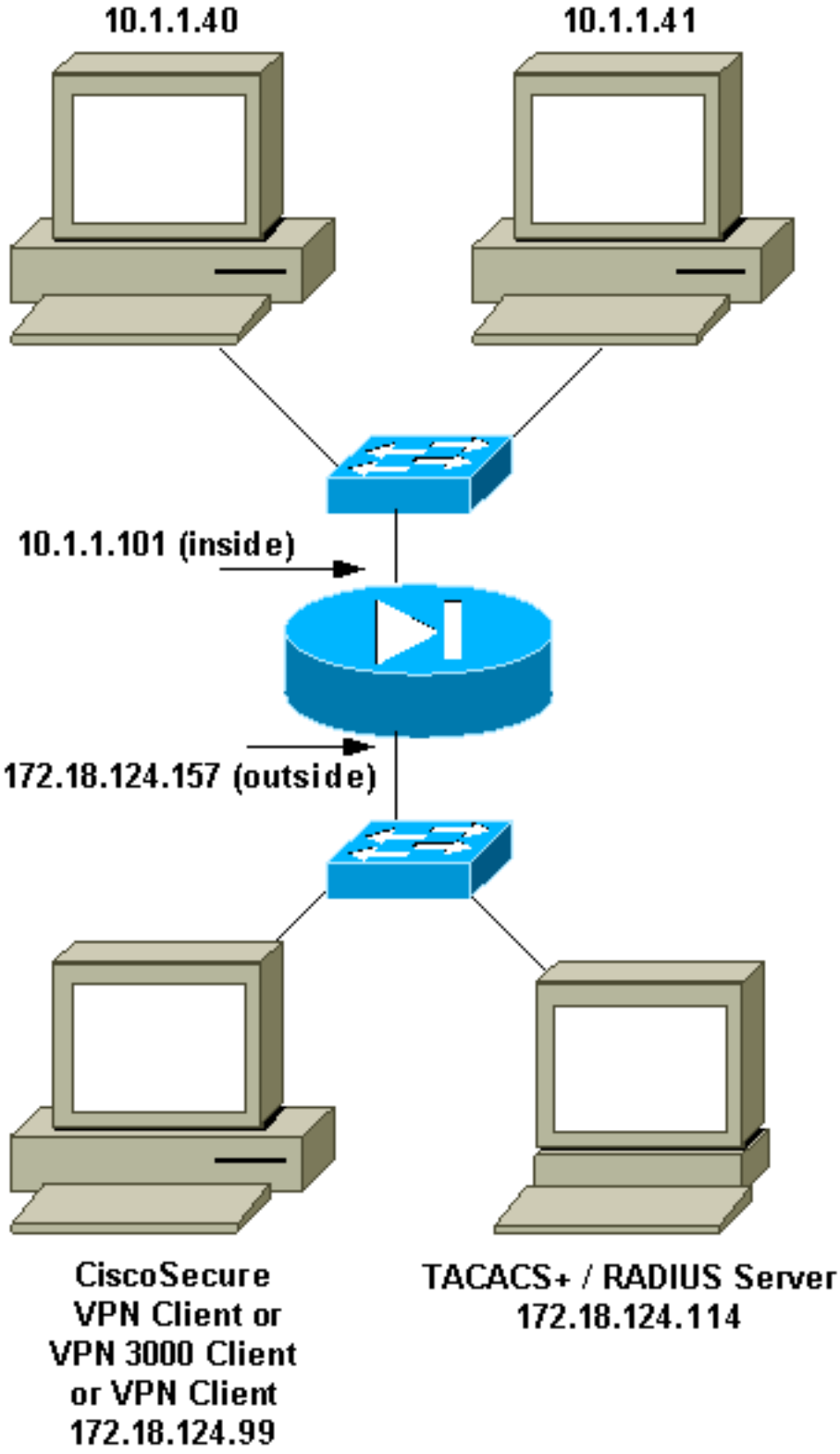
```
noacl Password= "noacl"

pixb Password= "pixb"
cisco-avpair = "acl=115"

3000full Password= "3000full"

3000partial Password= "3000partial"
```

네트워크 다이어그램



구성 가능한 RADIUS 포트(5.3 이상)

일부 RADIUS 서버는 1645/1646 이외의 RADIUS 포트를 사용합니다(일반적으로 1812/1813). PIX 5.3 이상에서는 다음 명령을 사용하여 RADIUS 인증 및 어카운팅 포트를 기본 1645/1646 이외의 포트로 변경할 수 있습니다.

- aaa-server radius-authport #
- aaa-server radius-acctport #

VPN 그룹 없이 Xauth로 인증하는 방법

이 예에서는 3개의 VPN 클라이언트 모두 Xauth를 사용하여 인증됩니다.그러나 스플릿 터널링이 사용되지 않으므로 VPN 클라이언트는 PIX 내부의 네트워크에만 액세스할 수 있습니다.스플릿 터널링에 대한 자세한 내용은 VPN 그룹을 사용하여 Xauth를 인증하는 방법을 참조하십시오.AAA 서버에서 전달된 ACL은 모든 VPN 클라이언트에 적용됩니다.이 예에서 목표는 사용자 noacl을 연결하여 PIX 내의 모든 리소스에 액세스하는 것입니다.사용자 PIXB는 연결되지만 ACL 115는 Xauth 프로세스 동안 AAA 서버에서 전달되므로 사용자는 10.1.1.40에만 액세스할 수 있습니다. 10.1.1.41 및 그 안에 있는 다른 모든 IP 주소에 대한 액세스는 거부됩니다.

참고: VPN Client 3.0을 지원하려면 PIX Software 릴리스 6.0이 필요합니다.

Cisco Secure VPN Client 1.1 설정 - VPN 그룹이 없는 Xauth

```
Name of connection:
Remote party address = IP_Subnet = 10.1.1.0, Mask 255.255.255.0
Connect using Secure Gateway Tunnel to 172.18.124.157
My Identity:
Select certificate = None
ID_Type = ip address, pre-shared key and fill in key
('cisco1234') - matches that of pix in 'isakmp key' command
Security policy = defaults
Proposal 1 (Authen) = DES, MD5
Proposal 2 (Key Exchange) = DES, MD5, Tunnel
```

DoS(서비스 거부) 창을 열고 ping **-t#.#.#.# 명령을** 실행합니다.Xauth(Xauth) 창이 나타나면 AAA 서버의 사용자 이름 및 비밀번호와 일치하는 비밀번호를 입력합니다.

VPN 3000 Client 2.5 또는 VPN Client 3.x Setup - VPN 그룹이 없는 Xauth

다음 단계를 완료하십시오.

1. Options **> Properties > Authentication > Group Name을 선택합니다**.
2. 그룹 이름은 not_care이며 비밀번호는 isakmp **key** 명령의 PIX에 있는 이름과 일치합니다.호스트 이름은 172.18.124.157입니다.
3. **연결을 클릭합니다**.
4. Xauth 창이 나타나면 AAA 서버의 사용자 이름 및 비밀번호와 일치하는 비밀번호를 입력합니다.

VPN 그룹이 없는 Xauth - PIX 설정

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

```
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
access-list 115 deny ip any host 10.1.1.41
access-list 115 permit ip any host 10.1.1.40
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.1.1.101 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.154
nat (inside) 0 access-list 108
Nat (inside) 1 10.1.1.0 255.255.255.0 0 0
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
AAA-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
AAA-server AuthInbound protocol tacacs+
AAA-server AuthInbound (outside) host 172.18.124.114 cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap client authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test outside
!--- Internet Security Association and Key Management Protocol (ISAKMP) !--- Policy for Cisco
VPN Client 2.5 or !--- Cisco Secure VPN Client 1.1. isakmp policy 10 authentication pre-share
```

```
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-H) !--- group 1 policy (PIX default).
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!
!--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
!--- The VPN 3.0 Clients use D-H group 2 policy !--- and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:05c6a2f3a7d187162c4408503b55affa
: end
[OK]
```

VPN 그룹을 사용하여 Xauth를 인증하는 방법

이 예에서는 VPN 3000 Client 2.5 또는 VPN Client 3.0을 Xauth로 인증할 수 있으며 스플릿 터널링이 적용됩니다.VPN 그룹 멤버십을 통해 PIX에서 VPN 3000 클라이언트로 ACL이 전달됩니다.PIX 내부의 네트워크에만 암호화된 터널이 있음을 지정합니다.다른 트래픽(아마도 인터넷으로)은 암호화되지 않습니다.

이 예에서는 AAA 서버에서 사용자 이름이 3000full인 하나의 VPN 클라이언트가 PIX의 그룹 vpn3000-all(PIX)에서 인터넷과 동시에 PIX 내부의 전체 10.1.1.X 네트워크에 액세스합니다.VPN 클라이언트는 wins-server, dns-server 및 domain-name 정보를 수신합니다.그룹 vpn3000-41(PIX의 경우)의 사용자 이름 3000partial(AAA-서버)을 사용하는 다른 VPN 클라이언트는 그룹 프로필을 통해 네트워크 내에서 하나의 IP 주소(10.1.1.40)만 액세스합니다.이 VPN 클라이언트는 wins 및 dns-server 정보를 수신하지 않지만 스플릿 터널링을 수행합니다.

참고: VPN Client 3.0을 지원하려면 PIX Software 릴리스 6.0이 필요합니다.

VPN Client 2.5 또는 3.0 설정 - VPN 그룹이 있는 Xauth

다음 단계를 완료하십시오.

참고: VPN 2.5 또는 3.0 클라이언트 설정은 관련된 사용자에 따라 달라집니다.

1. 옵션 **> 속성 > 인증을 선택합니다**.
2. 그룹 이름과 그룹 비밀번호는 다음과 같이 PIX의 그룹 이름과 일치합니다.vpngroup vpn3000-all 비밀번호 ********** 또는 vpngroup vpn3000-41 비밀번호 *********.호스트 이름은 172.18.124.157입니다.
3. **연결**을 **클릭합니다**.
4. Xauth 창이 나타나면 AAA 서버의 사용자 이름 및 비밀번호와 일치하는 비밀번호를 입력합니다.

이 예에서는 사용자 3000이 인증된 후 vpn3000-all 그룹에서 정보를 선택합니다.사용자 3000partial은 vpn3000-41 그룹에서 정보를 선택합니다.창에 **보안 프로파일 협상**과 **링크가 보안되었습니다**.

사용자 3000full은 group vpn3000-all에 대한 비밀번호를 사용합니다.Access-list 108은 스플릿 터널링을 위해 해당 그룹에 연결됩니다.10.1.1.x 네트워크에 터널이 형성됩니다.트래픽은 access-list 108(예: 인터넷)에 없는 디바이스에 암호화되지 않은 상태로 이동합니다. 스플릿 터널링입니다.

사용자 3000full에 대한 VPN 클라이언트 연결 상태 창의 출력입니다.

```
        Network         Mask
key     10.1.1.0        255.255.255.0
key     172.18.124.157  255.255.255.255
```

사용자 3000partial은 group vpn3000-41에 대한 비밀번호를 사용합니다. Access-list 125는 스플릿 터널링을 위해 해당 그룹에 연결됩니다.터널이 10.1.1.41 디바이스에 형성됩니다.트래픽은 access-list 125(예: 인터넷)에 없는 디바이스에 암호화되지 않은 상태로 이동합니다. 그러나 이 트래픽은 라우팅 불가하므로 10.1.1.40 디바이스으로 트래픽이 전달되지 않습니다.암호화 터널 목록에 지정되지 않았습니다.

사용자 3000partial에 대한 VPN 클라이언트 연결 상태 창의 출력입니다.

```
        Network         Mask
key     10.1.1.41       255.255.255.255
key     172.18.124.157  255.255.255.255
```

VPN 그룹이 있는 Xauth - PIX 설정

참고: Cisco Secure VPN Client 1.1은 ISAKMP(Internet Security Association and Key Management Protocol) 키가 없기 때문에 이 옵션과 함께 작동하지 않습니다.isakmp **키 ******** address 0.0.0.0 netmask 0.0.0.0** 명령을 추가하여 모든 VPN 클라이언트가 작동합니다.

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
access-list 125 permit ip host 10.1.1.41 any
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
```

```
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.154
Nat (inside) 0 access-list 108
Nat (inside) 1 10.1.1.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
AAA-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
AAA-server AuthInbound protocol tacacs+
AAA-server AuthInbound (outside) host 172.18.124.111
cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset ESP-Des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap client authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
isakmp client configuration address-pool local test outside
!--- ISAKMP Policy for Cisco VPN Client 2.5 or !--- Cisco Secure VPN Client 1.1. isakmp policy
10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-H) !--- group 1 policy (PIX default).
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!
!--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
!--- The VPN 3.0 Clients use D-H group 2 policy !--- and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool test
vpngroup vpn3000-all dns-server 10.1.1.40
vpngroup vpn3000-all wins-server 10.1.1.40
vpngroup vpn3000-all default-domain rtp.cisco.com
vpngroup vpn3000-all split-tunnel 108
vpngroup vpn3000-all idle-time 1800
vpngroup vpn3000-all password ********
vpngroup vpn3000-41 address-pool test
vpngroup vpn3000-41 split-tunnel 125
vpngroup vpn3000-41 idle-time 1800
vpngroup vpn3000-41 password ********
```

```
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:429db0e7d20451fc28074f4d6f990d25
: end
```

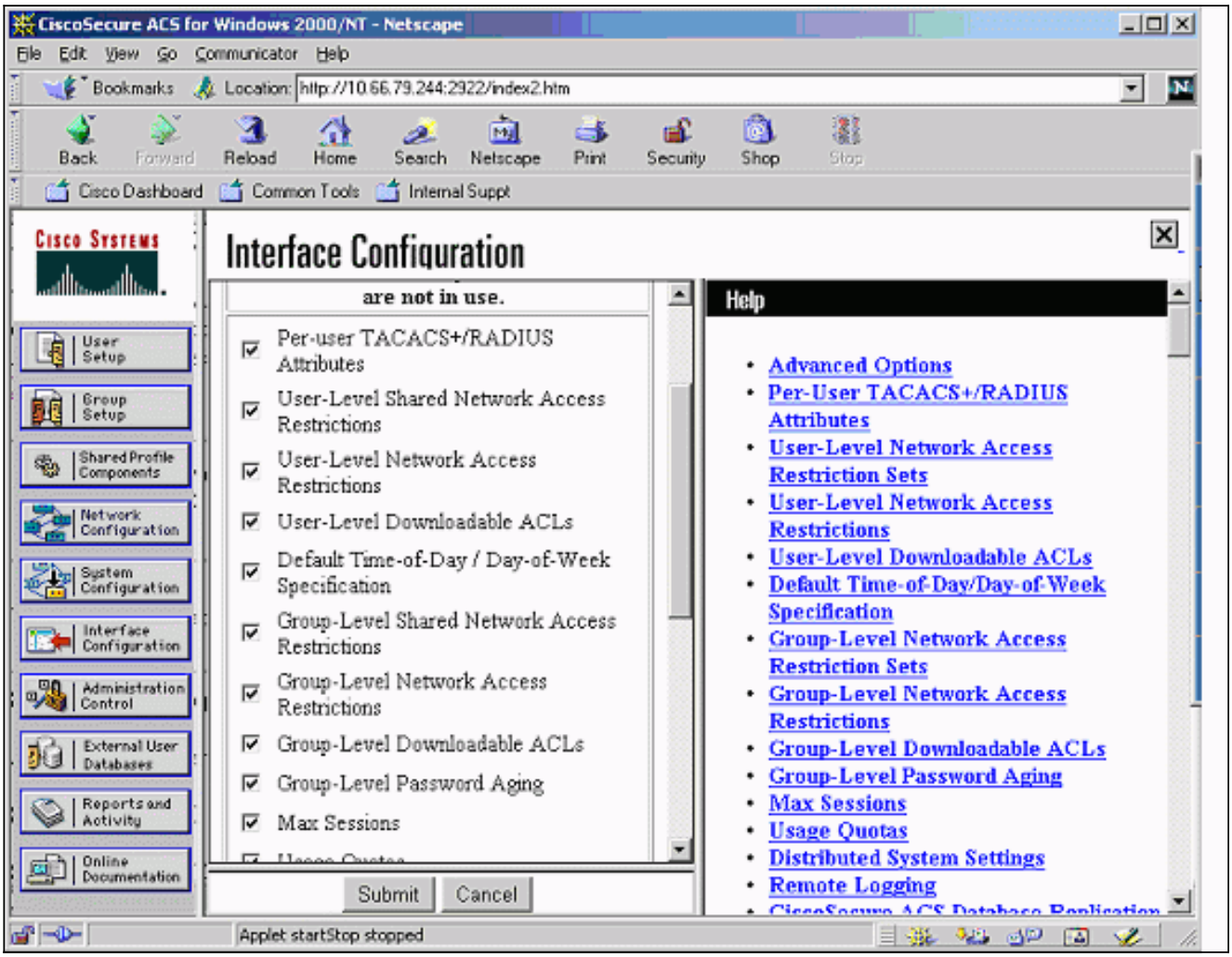
VPN 그룹 및 사용자별 다운로드 가능한 ACL을 사용하는 Xauth - ACS 설정

Cisco Secure ACS 설정

다음 단계를 완료하십시오.

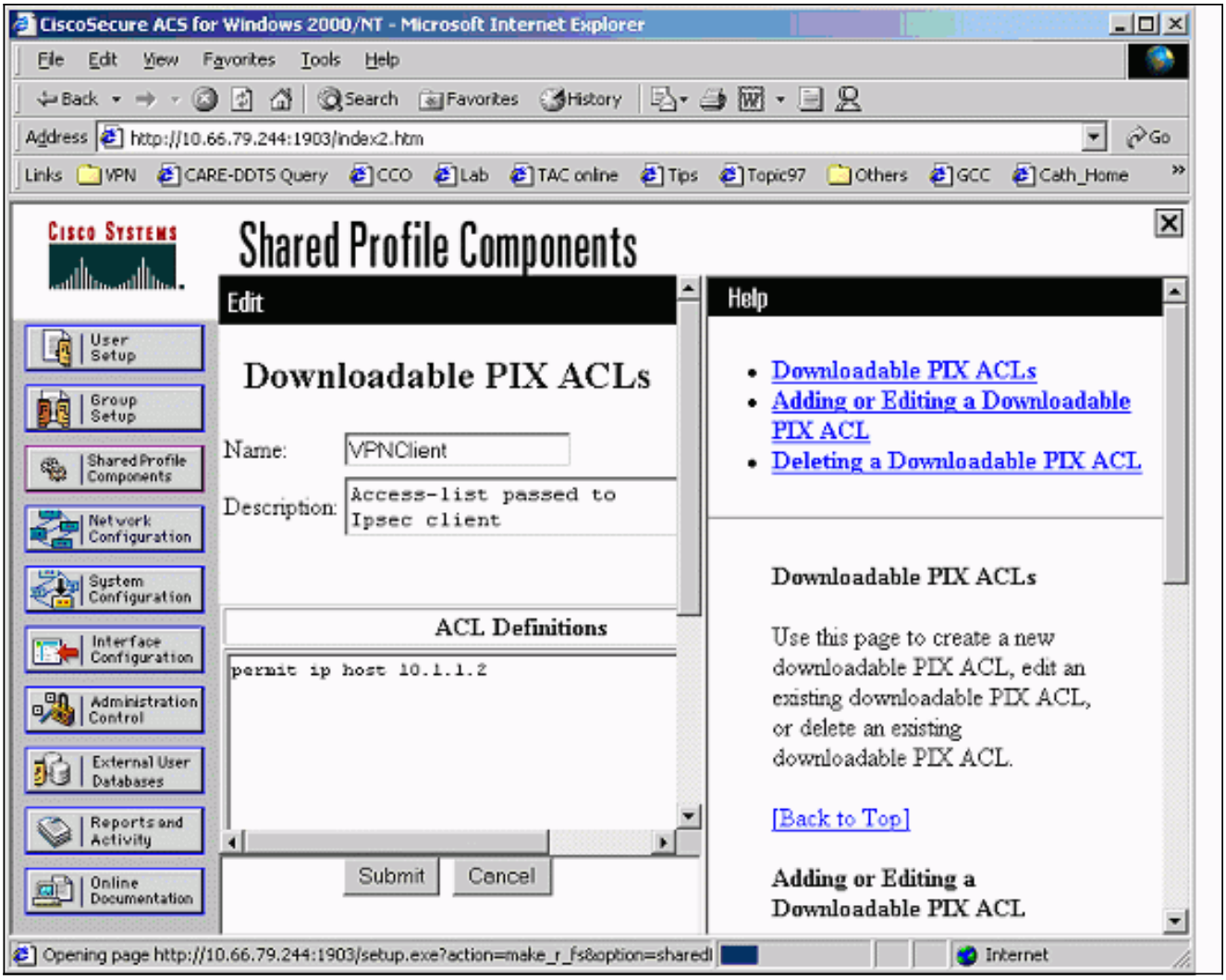
1. Interface **Configuration**(인터페이스 컨피그레이션)을 클릭하고 User-**Level Downloadable ACLs(사용자 레벨 다운로드 가능 ACL)** 옵션을 선택합니다

.



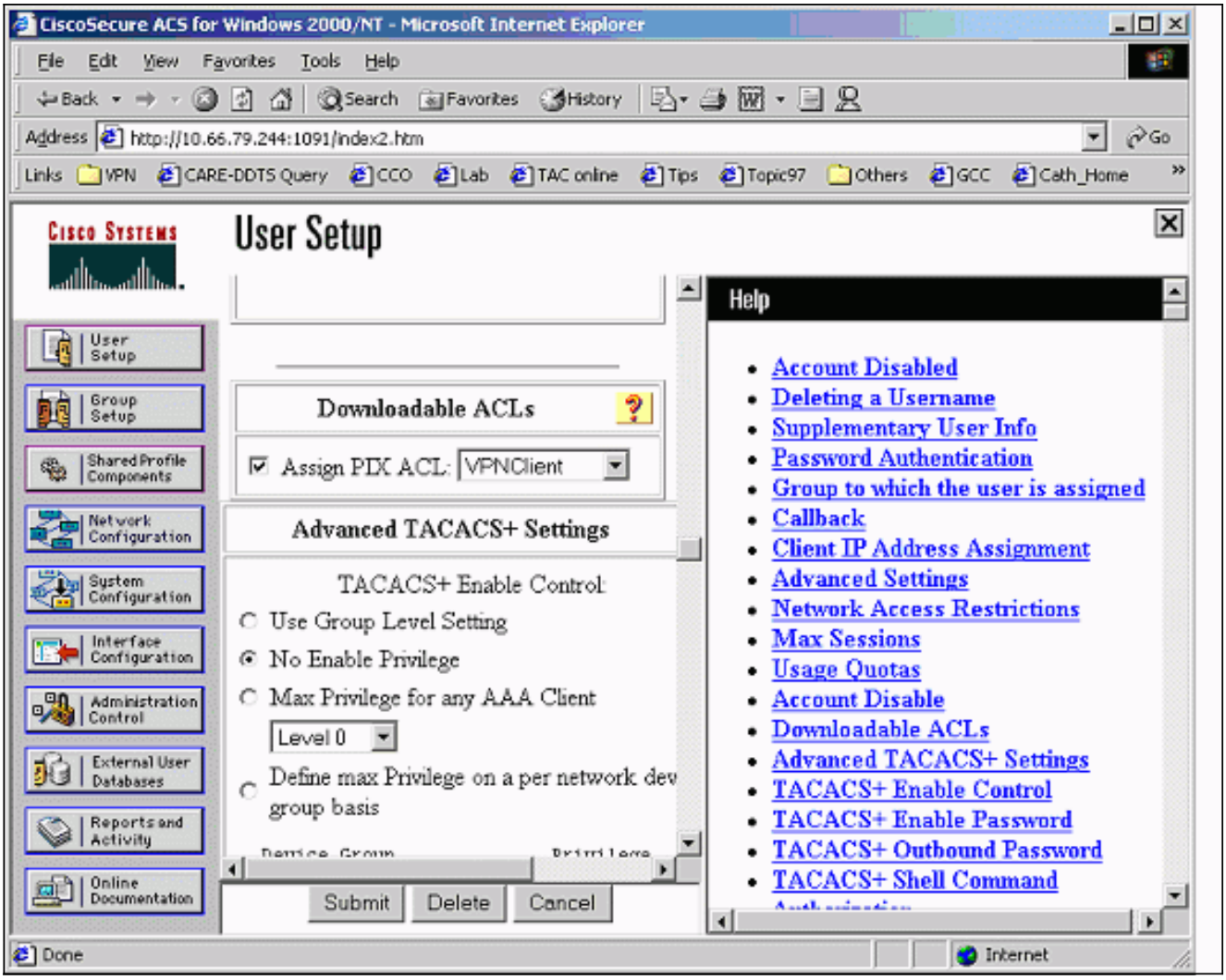
2. Shared **Profile Components(공유 프로파일 구성 요소)를** 클릭하고 다운로드 가능한 ACL을 정의합니다

.



3. User **Setup을 클릭합니다**.Assign PIX **ACL(PIX ACL 할당) 옵션을 선택합니다**.풀다운 목록에서 올바른 ACL을 선택합니다

.



VPN 그룹 및 사용자별 다운로드 가능한 ACL을 사용하는 Xauth - PIX 6.x 설정

권한 부여를 위해 사용자당 다운로드 가능한 ACL을 수행하려면 PIX Firewall 소프트웨어 버전 6.2(2)를 사용합니다. Cisco 버그 ID CSCdx47975(등록된 고객만 해당)를 참조하십시오.

```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-4
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
pager lines 24
logging buffered debugging
```

```
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 10.66.79.69 255.255.255.224
ip address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 108
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 10.66.79.65 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server AuthInbound protocol radius
aaa-server AuthInbound (outside) host 10.66.79.244 cisco123 timeout 10
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- This commands the router to respond to the VPN 3.x Client. crypto map mymap client
configuration address respond
!--- This tells the router to expect Xauth for the VPN 3.x Client. crypto map mymap client
authentication AuthInbound
crypto map mymap interface outside
isakmp enable outside
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
!
!--- This is the VPN group configuration. vpngroup vpn3000-all address-pool test
vpngroup vpn3000-all default-domain apt.cisco.com
!--- The split-tunnel mode-config is not used, !--- which enforces authorization on a per-user
basis. vpngroup vpn3000-all idle-time 1800
vpngroup vpn3000-all password ********
!
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:7c3d067232f427e7522f4a679e963c58
end:
```

VPN 그룹 및 사용자별 다운로드 가능한 ACL을 사용하는 Xauth - ASA/PIX 7.x 설정

```
PIX Version 7.1(1)
!
```

```
hostname PIX
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.66.79.69 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns domain-lookup inside
dns server-group DefaultDNS
 timeout 30

access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
logging buffer-size 500000
logging console debugging
logging monitor errors
mtu outside 1500
mtu inside 1500
ip local pool test 192.168.1.1-192.168.1.5
no failover
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400

nat (inside) 0 access-list 108
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

aaa-server AuthInbound protocol radius
aaa-server AuthInbound host 10.66.79.244 key cisco123

group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com

username vpn3000 password nPtKy7KDCerzhKeX encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

crypto ipsec transform-set my-set esp-des esp-md5-hmac

crypto dynamic-map dynmap 10 set transform-set my-set

crypto dynamic-map dynmap 10 set reverse-route

crypto map mymap 10 ipsec-isakmp dynamic dynmap
```

```
crypto map mymap interface outside

isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 1000

isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400


tunnel-group DefaultRAGroup general-attributes
 authentication-server-group (outside) vpn

tunnel-group vpn3000 type ipsec-ra

tunnel-group vpn3000 general-attributes
 address-pool test
 authentication-server-group vpn


tunnel-group vpn3000 ipsec-attributes
 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  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
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf
: end
```

VPN 클라이언트 연결을 위한 로컬 Xauth를 구성하는 방법

VPN 클라이언트 연결을 위한 로컬 Xauth를 구성하려면 다음 명령이 필요합니다.

- **aaa-server** *server-tag* **프로토콜** *로컬*
- **암호화 맵** *맵 이름* **클라이언트 인증 aaa-***server-name*

PIX에서 로컬 사용자를 정의하려면 username 명령을 실행합니다.

로컬 PIX Firewall 사용자 인증 데이터베이스를 사용하려면 aaa-**server** 명령에 대한 *server-tag* 매개변수에 대해 **LOCAL**을 입력합니다.aaa-**server** 명령은 **crypto map** 명령과 함께 실행되어 VPN 클라이언트가 PIX 방화벽에 액세스할 때 인증되도록 인증 연결을 설정합니다.

어카운팅 추가 방법

다음은 어카운팅을 추가하기 위한 명령의 구문입니다.

- **aaa accounting** *acctg_service*|inbound|outbound/*if_name local_ip local_mask foreign_ip foreign_mask* **tacacs+|radius;**

또는 (5.2의 새로운 기능:

- **aaa accounting inbound** *acctg_service* **inbound|outbound match server_***tag* ***포함***

PIX 컨피그레이션에서 추가된 명령은 다음과 같습니다.

- **aaa 어카운팅에는 모든 인바운드 0.0.0.0 0.0.0.0 AuthInbound0.0.0.0 포함됩니다**.

또는 (5.2의 새로운 기능:

- **access-list 150 permit ip any aaa accounting match 150 outside AuthInbound**

참고: Xauth 어카운팅이 작동하려면 sysopt ipsec **pl-compatible** 명령이 아닌 sysopt connection permit-ipsec 명령이 필요합니다.Xauth 어카운팅은 sysopt ipsec pl**-compatible** 명령에서만 작동하지 않습니다.Xauth 어카운팅은 TCP 연결에 유효합니다.ICMP(Internet Control Message Protocol) 또는 UDP(User Datagram Protocol)에는 유효하지 않습니다.

TACACS+ 계정 관리 예

```
Fri Sep 8 03:48:40 2000 172.18.124.157
pixc PIX 192.168.1.1 start task_id=0x17 foreign_ip=192.168.1.1
    local_ip=10.1.1.40 cmd=telnet
Fri Sep 8 03:48:44 2000 172.18.124.157 pixc PIX 192.168.1.1
    stop task_id=0x17 foreign_ip=192.168.1.1 local_ip=10.1.1.40
    cmd=telnet elapsed_time=4 bytes_in=42 bytes_out=103
Fri Sep 8 03:49:31 2000 172.18.124.157 pixc PIX 192.168.1.1
    start task_id=0x18
foreign_ip=192.168.1.1 local_ip=10.1.1.40 cmd=http
Fri Sep 8 03:49:35 2000 172.18.124.157 pixc PIX 192.168.1.1
    stop task_id=0x18 foreign_ip=192.168.1.1 local_ip=10.1.1.40
    cmd=http elapsed_time=4 bytes_in=242 bytes_out=338
```

RADIUS 어카운팅 예

```
Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000003
User-Name = noacl
```

```
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1141
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23

Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 80
Acct-Session-Id = 0x00000004
User-Name = noacl
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1168
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=80

Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.41
Login-TCP-Port = 80
Acct-Session-Id = 0x00000008
User-Name = noacl
Acct-Session-Time = 4
Acct-Input-Octets = 242
Acct-Output-Octets = 338
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1182
Vendor-Specific = Destination-IP=10.1.1.41
Vendor-Specific = Destination-Port=80

Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000015
User-Name = noacl
Acct-Session-Time = 33
Acct-Input-Octets = 43
Acct-Output-Octets = 103
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1257
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23
```

디버그 및 표시 - VPN 그룹 없이 Xauth

```
goss-pixb#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
tx Off
rx Off
open Off
cable Off
txdmp Off
rxdmp Off
ifc Off
rxip Off
txip Off
get Off
put Off
```

```
verify Off
switch Off
fail Off
fmsg Off
goss-pixb#terminal monitor
goss-pixb#

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing KE payload. Message ID = 0

ISAKMP (0): processing NONCE payload. Message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_MM exchange
ISAKMP (0): processing ID payload. Message ID = 0
ISAKMP (0): processing HASH payload. Message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99

ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 2218162690 (0x84367a02)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
```

```
Message ID = 2156074032
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS109005: Authentication succeeded
for user 'pixb' from 172.18.124.99/0 to 0.0.0.0/0 on
interface IKE-XAUTH
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 2218162690 (0x84367a02)
109005: Authentication succeeded for user 'pixb' from 172.18.124.157
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
Message ID = 2156497080
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 393799466 (0x1778e72a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
Message ID = 2156156112
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
return status is IKMP_NO_ERROR.99/0 to 0.0.0.0/0 on
interface IKE-XAUTH

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. Message ID = 2323118710

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= ESP-Des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. Message ID = 2323118710

ISAKMP (0): processing ID payload. Message ID = 2323118710
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. Message ID = 2323118710
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0
prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xeeae8930(4004415792) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR4
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2
```

```
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
(proxy 192.168.1.1 to 10.1.1.0)
has spi 4004415792 and conn_id 1 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 10.1.1.0 to 192.168.1.1)
has spi 1281287211 and conn_id 2 and flags 4
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xeeae8930(4004415792), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x4c5ee42b(1281287211), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR02101: decaps: rec'd
IPSEC packet has invalid spi for destaddr=172.18.124.157,
prot=esp, spi=0xeeae8930(0)
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0xeeae8930(4004415792), sa_trans= esp-des esp-md5-hmac,
 sa_conn_id= 1

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0x4c5ee42b(1281287211), sa_trans= esp-des esp-md5-hmac,
 sa_conn_id= 2

109011: Authen Session Start: user 'pixb', sid 5
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside
109015: Authorization denied (acl=115) for user 'pixb' from
192.168.1.1/0 to 10.1.1.40/8 on interface outside

goss-pixb#
goss-pixb#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'pixb' at 192.168.1.1, authenticated
access-list 115
goss-pixb#show access-list
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0
255.255.255.0 (hitcnt=18)
access-list 125 permit ip host 10.1.1.41 any (hitcnt=0)
access-list dynacl4 permit ip 10.1.1.0 255.255.255.0 host
192.168.1.1 (hitcnt=0)
access-list 115 permit ip any host 10.1.1.41 (hitcnt=0)
access-list 115 deny ip any host 10.1.1.42 (hitcnt=0)
```

디버그 및 표시 - VPN 그룹이 있는 Xauth

```
crypto_isakmp_process_block: src 172.18.124.96,
dest 172.18.124.157
goss-pixb#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
tx Off
rx Off
open Off
cable Off
txdmp Off
rxdmp Off
ifc Off
rxip Off
txip Off
get Off
put Off
verify Off
switch Off
fail Off
fmsg Off
goss-pixb#
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a VPN3000 client

ISAKMP (0): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
ISAKMP (0:0): Need XAUTH
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 1396280702 (0x53398d7e)
return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
message ID = 2156608344
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS10
ISAKMP (0:0): initiating peer config to 172.18.124.99.
ID = 1396280702 (0x53398d7e)9
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.99.
message ID = 2156115984
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1697984837

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 172.18.124.157/255.255.255.255/0/0 (type=1),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1697984837

ISAKMP (0): processing ID payload. message ID = 1697984837
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1697984837
ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.157 prot 0 port 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 1697984837
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine):
got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x6a9d3f79(1788690297) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR0
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2

ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
(proxy 192.168.1.1 to 172.18.124.157)
has spi 1788690297 and conn_id 1 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 172.18.124.157 to 192.168.1.1)
has spi 2854452814 and conn_id 2 and flags 4
```

```
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x6a9d3f79(1788690297), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xaa237e4e(2854452814), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR05: Authentication succeeded
for user 'pixc' from 172.18.124.99/0 to 0.0.0.0/0 on interface IKE-XAUTH
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0x6a9d3f79(1788690297), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 1

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0xaa237e4e(2854452814), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2

109011: Authen Session Start: user 'pixc', sid 19

crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3361949217

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 3361949217

ISAKMP (0): processing ID payload. message ID = 3361949217
ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 3361949217
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfec4c3aa(4274308010) for SA
from 172.18.124.99 to 172.18.124.157 for prot 3

return status is IKMP_NO_ERROR4
crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4
```

```
map_alloc_entry: allocating entry 3

ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.99 to 172.18.124.157
(proxy 192.168.1.1 to 10.1.1.0)
has spi 4274308010 and conn_id 4 and flags 4
outbound SA from 172.18.124.157 to 172.18.124.99
(proxy 10.1.1.0 to 192.168.1.1)
has spi 798459812 and conn_id 3 and flags 4
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xfec4c3aa(4274308010), conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x2f9787a4(798459812), conn_id= 3, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR02101: decaps: rec'd IPSEC
packet has invalid spi for destaddr=172.18.124.157, prot=esp,
spi=0xfec4c3aa(0)
602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50,
sa_spi= 0xfec4c3aa(4274308010), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 4

602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50,
sa_spi= 0x2f9787a4(798459812), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 3


goss-pixb#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'pixc' at 192.168.1.1, authenticated
goss-pixb#show crypto ipsec sa


interface: outside
Crypto map tag: mymap, local addr. 172.18.124.157

local ident (addr/mask/prot/port): (172.18.124.157/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 172.18.124.99
dynamic allocated peer ip: 192.168.1.1

PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#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.: 172.18.124.157, remote crypto endpt.: 172.18.124.99
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: aa237e4e
```

```
inbound esp sas:
spi: 0x6a9d3f79(1788690297)
transform: esp-des esp-md5-hmac ,
<--- More ---> in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28519)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0xaa237e4e(2854452814)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28510)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:
<--- More --->

outbound pcp sas:



local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 172.18.124.99
dynamic allocated peer ip: 192.168.1.1

PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#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.: 172.18.124.157, remote crypto
endpt.:172.18.124.99
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 2f9787a4

inbound esp sas:
spi: 0xfec4c3aa(4274308010)
<--- More ---> transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/27820)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:
```

```
inbound pcp sas:


outbound esp sas:
spi: 0x2f9787a4(798459812)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/27820)
IV size: 8 bytes
replay detection support: Y


<--- More ---> outbound ah sas:


outbound pcp sas:
```

디버그 및 표시 - 사용자별 다운로드 가능한 ACL이 포함된 Xauth

```
crypto_isakmp_process_block: src 10.66.79.229,
dest 10.66.79.69
VPN Peer: ISAKMP: Added new peer: ip:10.66.79.229
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:10.66.79.229 Ref cnt incremented to:1
Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
```

```
ISAKMP (0): Checking ISAKMP transform 5 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 10
ISAKMP (0): Total payload length: 14
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0RADIUS_GET_PASS
RADIUS_REQUEST
raidus.c: rad_mkpkt_authen
attribute:
type 1, length 10, content:
80917fb0: 74 65 73 74 75 73 65 72 | testuser
attribute:
type 4, length 6, content:
80917fb0: 0a 42 | .B
80917fc0: 4f 45 | OE
attribute:
type 5, length 6, content:
80917fd0: 00 00 00 01 | ....

ISAKMP (0): processing notify INITIAL_CONTACTrip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
```

```
session_id 0x5d5ba513
request_id 0x2
user 'testuser'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 8, length 6, content:
809186f0: ff ff | ..
80918700: ff ff | ..
RADIUS_RCVD
attribute:
type 26, length 67, content:
Vendor ID 0 0 0 9, type=1, len=61:
80918700: 41 43 53 3a 43 69 | ACS:Ci
80918710: 73 63 6f 53 65 63 75 72 65 2d 44 65 66 69 6e 65
| scoSecure-Define
80918720: 64 2d 41 43 4c 3d 23 41 43 53 41 43 4c 23 2d 50
| d-ACL=#ACSACL#-P
80918730: 49 58 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33
| IX-VPNClient-3d3
80918740: 32 37 38 31 35 | 27815
RADIUS_RCVD
RADIUS_REQUEST
raidus.c: rad_mkpkt_authen
attribute:
type 1, length 33, content:
809186d0: 23 41 43 53 41 43 4c 23 2d 50 49 58 | #ACSACL#-PIX
809186e0: 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33 32 37
| -VPNClient-3d327
809186f0: 38 31 35 | 815
attribute:
type 4, length 6, content:
809186f0: 0a 42 4f 45 | .BOE
attribute:
type 5, length 6, content:
80918700: 00 00 00 | ...
80918710: 02 | .
IPSEC(key_engine): got a queue event...rip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
session_id 0x5d5ba513
request_id 0x3
user '#ACSACL#-PIX-VPNClient-3d327815'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 26, length 46, content:
Vendor ID 0 0 0 9, type=1, len=40:
80918e20: 69 70 3a 69 6e 61 63 6c 23 31 3d 70 | ip:inacl#1=p
80918e30: 65 72 6d 69 74 20 69 70 20 61 6e 79 20 68 6f 73
| ermit ip any hos
80918e40: 74 20 31 30 2e 31 2e 31 2e 32 | t 10.1.1.2
RADIUS_RCVD
RADIUS_RCVD
RADIUS_ACCESS_ACCEPT:normal termination
RADIUS_DELETE
```

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 10.66.79.229

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify
ISAKMP (0): sending NOTIFY message 24576 protocol 1
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 3250273953 (0xc1bb3ea1)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
 message ID = 2167001532
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 1530000247 (0x5b31f377)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1)
ISAKMP: attribute IP4_NETMASK (2)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute ADDRESS_EXPIRY (5)
Unsupported Attr: 5
ISAKMP: attribute APPLICATION_VERSION (7)
Unsupported Attr: 7
ISAKMP: attribute UNKNOWN (28672)
Unsupported Attr: 28672
ISAKMP: attribute UNKNOWN (28673)
Unsupported Attr: 28673
ISAKMP: attribute ALT_DEF_DOMAIN (28674)
ISAKMP: attribute ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute ALT_PFS (28679)
ISAKMP: attribute UNKNOWN (28680)
Unsupported Attr: 28680
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 10.66.79.229.
ID = 2397668523
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2858414843

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
```

```
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (2)
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
```

```
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
ipsec user 'testuser' at 192.168.1.1, authenticated
access-list #ACSACL#-PIX-VPNClient-3d327815
sv2-4(config)#show access-list
access-list 108; 1 elements
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0
255.255.255.0 (hitcnt=38)
access-list #ACSACL#-PIX-VPNClient-3d327815; 1 elements
access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any host
10.1.1.2 (hitcnt=15)
access-list dynacl4; 1 elements
access-list dynacl4 permit ip host 10.66.79.69
host 192.168.1.1 (hitcnt=0)
access-list dynacl5; 1 elements
access-list dynacl5 permit ip any host 192.168.1.1 (hitcnt=15)
sv2-4(config)#show access-list
access-list 108; 1 elements
access-list 108 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 (hitcnt=42)
access-list #ACSACL#-PIX-VPNClient-3d327815; 1 elements
access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any
host 10.1.1.2 (hitcnt=17)
access-list dynacl4; 1 elements
access-list dynacl4 permit ip host 10.66.79.69 host
192.168.1.1 (hitcnt=0)
access-list dynacl5; 1 elements
access-list dynacl5 permit ip any host 192.168.1.1 (hitcnt=17)



sv2-4(config)#show crypto map

Crypto Map: "mymap" interfaces: { outside }
client configuration address respond
client authentication AuthInbound

Crypto Map "mymap" 10 ipsec-isakmp
Dynamic map template tag: dynmap

Crypto Map "mymap" 20 ipsec-isakmp
Peer = 10.66.79.229
access-list dynacl6; 1 elements
access-list dynacl6 permit ip host 10.66.79.69
host 192.168.1.1 (hitcnt=0)
dynamic (created from dynamic map dynmap/10)
Current peer: 10.66.79.229
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset, }

Crypto Map "mymap" 30 ipsec-isakmp
Peer = 10.66.79.229
access-list dynacl7; 1 elements
```

```
access-list dynacl7 permit ip any host 192.168.1.1 (hitcnt=0)
dynamic (created from dynamic map dynmap/10)
Current peer: 10.66.79.229
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ myset, }
sv2-4(config)
```

관련 정보

- PIX 지원 페이지
- PIX 명령 참조
- RFC(Request for Comments)
- UNIX용 Cisco Secure ACS 지원 페이지
- Cisco Secure ACS for Windows 지원 페이지
- TACACS/TACACS+ 지원 페이지
- IOS 설명서의 TACACS+
- RADIUS 지원 페이지
- 기술 지원 및 문서 – Cisco Systems