PIX 버전 5.2 이상을 통해 사용자 인증, 권한 부여 및 계정 관리 수행

목차

소개

RADIUS 및 TACACS+ 인증은 Cisco Secure PIX Firewall을 통해 FTP, 텔넷 및 HTTP 연결에 대해 수행할 수 있습니다. 일반적으로 다른 덜 일반적인 프로토콜에 대한 인증은 작동합니다. TACACS+ 권한 부여가 지원됩니다. RADIUS 권한 부여는 지원되지 않습니다. 이전 버전에 대한 PIX 5.2 인증, 권한 부여 및 계정 관리(AAA)의 변경 사항에는 인증된 사용자와 사용자가 액세스하는 리소스를 제어하는 AAA 액세스 목록 지원이 포함됩니다. PIX 5.3 이상에서는 RADIUS 포트를 구성할 수 있다는 점이 이전 버전의 코드에 비해 AAA(Authentication, Authorization, and Accounting)가 변경됩니다.

참고: PIX 6.x는 통과 트래픽에 대해 어카운팅을 수행할 수 있지만 PIX로 디스테이트된 트래픽에 대해서는 어카운팅을 수행할 수 없습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Secure PIX Firewall Software 버전 5.2.0.205 및 5.2.0.207

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

참고: PIX/ASA 소프트웨어 버전 7.x 이상을 실행하는 경우 AAA 서버 및 로컬 데이터베이스 구성을 참조하십시오.

표기 규칙

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

인증, 권한 부여 및 계정 관리(AAA)

다음은 인증, 권한 부여 및 어카운팅에 대한 설명입니다.

- 인증은 사용자의 이름입니다.
- 권한 부여는 사용자가 수행하는 작업입니다.
- 권한 부여 없이 인증이 유효합니다.
- 인증 없이는 권한 부여가 유효하지 않습니다.
- 어카운팅은 사용자가 한 것입니다.

인증/권한 부여를 통해 사용자에게 표시되는 내용

사용자가 인증/권한 부여를 사용하여 내부에서 외부로(또는 그 반대로) 이동하려고 할 때:

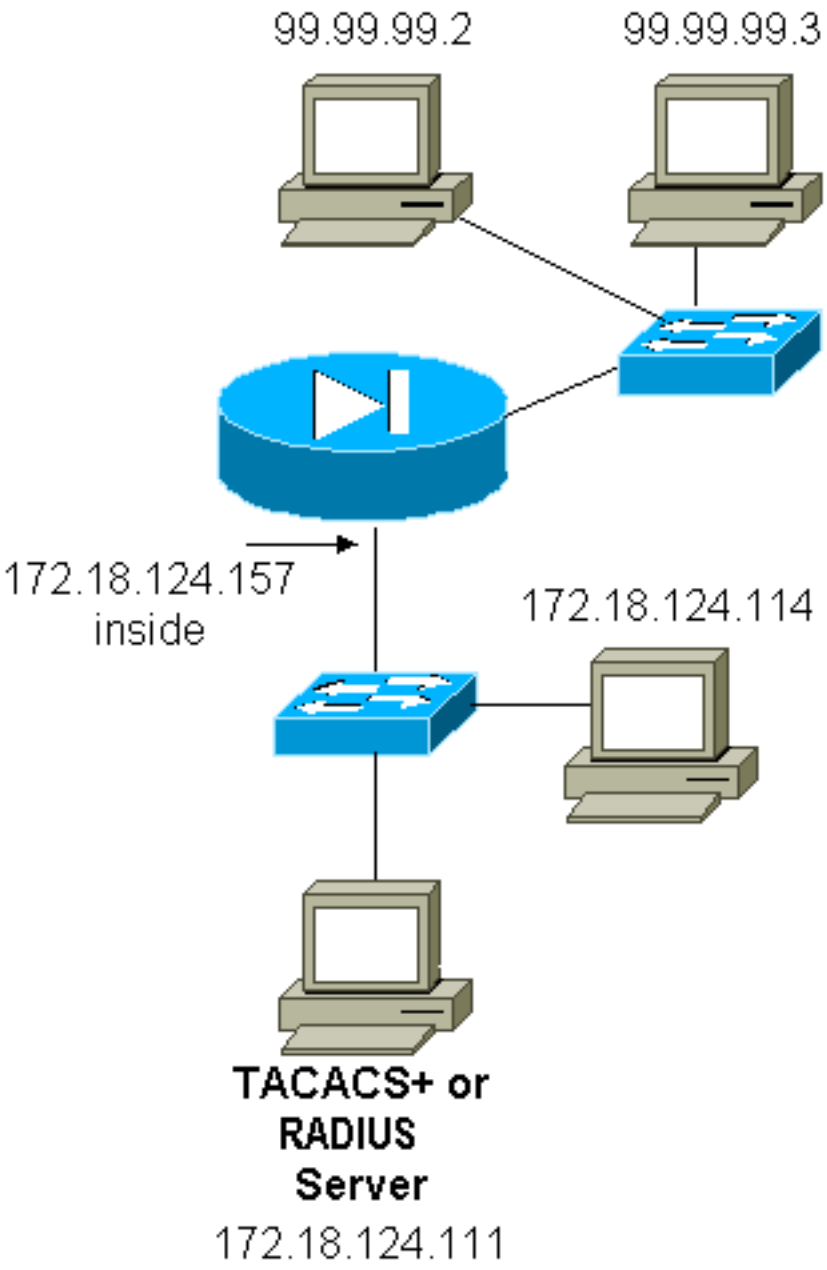
- **Telnet**—사용자 이름 프롬프트가 나타난 다음 비밀번호 요청이 표시됩니다. PIX/Server에서 인증(및 권한 부여)이 성공적으로 수행되면 그 이후의 대상 호스트에서 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.
- **FTP** - 사용자 이름 프롬프트가 나타납니다. 사용자는 사용자 이름에 "local_username@remote_username"을 입력하고 비밀번호에 "local_password@remote_password"을 입력해야 합니다. PIX는 로컬 보안 서버에 "local_username" 및 "local_password"를 보냅니다. PIX/서버에서 인증(및 권한 부여)이 성공하면 "remote_username" 및 "remote_password"가 대상 FTP 서버에 전달됩니다.
- **HTTP** - 사용자 이름과 비밀번호를 요청하는 창이 브라우저에 표시됩니다. 인증(및 권한 부여)에 성공하면 사용자가 대상 웹 사이트에 도착합니다. *브라우저에서 사용자 이름과 암호를 캐시한다는 점에 유의하십시오.* PIX가 HTTP 연결을 시간 초과해야 하지만 시간 초과하지는 않는 것으로 나타나면 브라우저가 PIX에 캐시된 사용자 이름과 비밀번호를 "슈팅"할 때 재인증이 발생할 가능성이 높습니다. PIX는 이를 인증 서버로 전달합니다. PIX syslog 및/또는 서버 디버그는 이 현상을 표시합니다. 텔넷과 FTP가 "정상적으로" 작동하는 것처럼 보이지만 HTTP 연결이 작동하지 않는 경우, 이러한 이유가 됩니다.

디버깅 단계

- AAA 인증 및 권한 부여를 추가하기 전에 PIX 컨피그레이션이 작동하는지 확인합니다. 인증 및 권한 부여를 시작하기 전에 트래픽을 전달할 수 없는 경우, 나중에 트래픽을 전달할 수 없습니다.
- PIX에서 어떤 종류의 로깅을 활성화합니다.logging **console debug** 명령을 실행하여 로깅 콘솔 디버깅을 활성화합니다.**참고:** 로드가 많은 시스템에서는 로깅 콘솔 디버깅을 사용하지 마십시오.텔넷 세션을 **로깅하려면 logging monitor debug** 명령을 사용합니다.로깅 버퍼된 디버깅을 사용한 다음 **show logging** 명령을 실행할 수 있습니다.로깅은 syslog 서버로 전송되어 여기에서 검사할 수도 있습니다.
- TACACS+ 또는 RADIUS 서버에서 디버깅을 설정합니다.

인증만

네트워크 다이어그램



서버 설정 - 인증만

Cisco Secure UNIX TACACS 서버 컨피그레이션

```
User = cse {
password = clear "cse"
default service = permit
}
```

Cisco Secure UNIX RADIUS 서버 구성

참고: 고급 GUI의 도움을 받아 PIX IP 주소 및 키를 NAS(Network Access Server) 목록에 추가합니다.

```
user=bill {
radius=Cisco {
check_items= {
```

```
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure Windows RADIUS

Cisco Secure Windows RADIUS 서버를 설정하려면 다음 단계를 수행합니다.

1. **User Setup** 섹션에서 비밀번호를 가져옵니다.
2. **Group Setup(그룹 설정)** 섹션에서 특성 6(Service-Type)을 **Login** 또는 **Administrative**로 **설정합니다**.
3. GUI의 **NAS Configuration(NAS 컨피그레이션)** 섹션에서 PIX IP 주소를 추가합니다.

Cisco Secure Windows TACACS+

사용자는 **User Setup** 섹션에서 비밀번호를 가져옵니다.

Livingston RADIUS 서버 구성

참고: PIX IP 주소 및 키를 *클라이언트* 파일에 추가합니다.

- bill password="foo" user-service-type = 셸 사용자

Merit RADIUS 서버 구성

참고: PIX IP 주소 및 키를 *클라이언트* 파일에 추가합니다.

- bill password="foo" Service-Type = Shell-User

TACACS+ 프리웨어 서버 컨피그레이션

```
key = "cisco"
user = cse {
login = cleartext "cse"
default service = permit
}
```

PIX 초기 컨피그레이션 - 인증만

PIX 초기 컨피그레이션 - 인증만

```
PIX Version 5.2(0)205
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
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
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
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 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
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 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 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
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
```

```
cisco timeout 5
!
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

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 다른 것으로 변경할 수 있습니다.

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

PIX 인증 디버그 예

디버깅을 설정하는 방법에 대한 자세한 내용은 디버깅 단계를 참조하십시오. 다음은 내부 172.18.124.114(99.99.99.99)으로 트래픽을 시작하는 99.99.99.2의 사용자의 예입니다. 인바운드 트래픽은 TACACS에서 인증되고 아웃바운드는 RADIUS에서 인증됩니다.

인증 성공 - TACACS+(인바운드)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

잘못된 사용자 이름/암호로 인해 인증에 실패했습니다. - TACACS+(인바운드). 사용자에게 "오류: 최대 시도 횟수를 초과했습니다."

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

서버가 PIX와 통신하지 않음 - TACACS+(인바운드). 사용자는 사용자 이름을 한 번 확인하고 PIX는 비밀번호를 묻지 않습니다(텔넷에 있음). 사용자에게 "오류: 최대 시도 횟수를 초과했습니다."

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

정상 인증 - RADIUS(아웃바운드)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

잘못된 인증(사용자 이름 또는 비밀번호) - RADIUS(아웃바운드). 사용자 이름, 비밀번호 순으로 요청을 확인한 다음 세 가지 기회가 있습니다. 이 값을 입력할 수 없으면 "오류: 최대 시도 횟수를 초과했습니다."

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

서버 ping이 가능하지만 데몬 다운, 서버 ping이 불가능하거나 키/클라이언트 불일치 - PIX - RADIUS(아웃바운드)와 통신하지 않습니다. 사용자 이름, 비밀번호, "RADIUS 서버 실패"를 확인한 다음 "오류: 최대 시도 횟수를 초과했습니다."

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
```

```
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Authentication Plus 권한 부여

인증된 모든 사용자가 PIX를 통해 모든 작업(HTTP, FTP 및 텔넷)을 수행하도록 허용하려면 인증이 충분하며 권한 부여가 필요하지 않습니다. 그러나 특정 사용자에게 일부 서비스의 하위 집합을 허용하거나 사용자가 특정 사이트로 이동하는 것을 제한하려면 권한 부여가 필요합니다. PIX를 통한 트래픽에 대해 RADIUS 권한 부여가 유효하지 않습니다. 이 경우 TACACS+ 권한 부여가 유효합니다.

인증이 전달되고 권한 부여가 설정된 경우 PIX는 사용자가 서버에서 수행하는 명령을 전송합니다. 예: "http 1.2.3.4" PIX 버전 5.2에서는 TACACS+ 권한 부여가 액세스 목록과 함께 사용되어 사용자가 이동하는 위치를 제어합니다.

HTTP(방문한 웹 사이트)에 대한 권한 부여를 구현하려면 단일 웹 사이트에 연결된 많은 수의 IP 주소가 있을 수 있으므로 Websense와 같은 소프트웨어를 사용합니다.

서버 설정 - 인증 + 권한 부여

Cisco Secure UNIX TACACS 서버 컨피그레이션

```
user = can_only_do_telnet {
password = clear "***********"
service = shell {
cmd = telnet {
permit .*
}
}
}

user = can_only_do_ftp {
password = clear "********"
service = shell {
cmd = ftp {
permit .*
}
}
}

user = httponly {
password = clear "*********"
service = shell {
cmd = http {
permit .*
}
}
}
```

Cisco Secure Windows TACACS+

Cisco Secure Windows TACACS+ 서버를 설정하려면 다음 단계를 완료하십시오.

1. Group **Setup(그룹 설정)** 하단의 Deny unmatched IOS **commands(일치하지 않는 IOS 명령 거**

부)를 클릭합니다.

2. Add/**Edit New Command (FTP, HTTP, Telnet)를 클릭합니다**.예를 들어, 특정 사이트("telnet 1.2.3.4")에 텔넷을 허용하려면 명령이 **텔넷입니다**. 인수는 *1.2.3.4입니다.* "command=**telnet"**을 입력한 후 인수 사각형의 "permit" IP 주소를 입력합니다(예: "permit 1.2.3.4"). 모든 텔넷이 허용되어야 하는 경우 명령어는 **텔넷이지만**, **목록에 없는 모든 인수 허용 을** 클릭합니다. 그런 다음 **편집 완료 명령을** 클릭합니다.
3. 허용되는 각 명령(예: 텔넷, HTTP, FTP)에 대해 2단계를 수행합니다.
4. GUI의 도움을 받아 NAS Configuration(NAS 컨피그레이션) 섹션에서 PIX IP 주소를 추가합니다.

TACACS+ 프리웨어 서버 컨피그레이션

```
user = can_only_do_telnet {
   login = cleartext "telnetonly"
   cmd = telnet {
   permit .*
   }
   }

 user = httponly {
   login = cleartext "httponly"
   cmd = http {
   permit .*
   }
   }

 user = can_only_do_ftp {
   login = cleartext "ftponly"
   cmd = ftp {
   permit .*
   }
   }
```

PIX 컨피그레이션 - 권한 부여 추가

권한 부여가 필요한 명령을 추가합니다.

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

새로운 5.2 기능을 사용하면 이전에 정의한 액세스 목록 101과 함께 이 문을 사용하여 이전 세 문을 대체할 수 있습니다. 낡은 것과 새로운 것은 섞여서는 안 된다.

```
aaa authorization match 101 outside AuthInbound
```

PIX 인증 및 권한 부여 디버그 예

올바른 인증 및 권한 부여가 성공함 - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

인증이 올바르지만 권한 부여가 실패합니다. - TACACS+. 사용자는 "오류: 권한 부여가 거부되었습니다."

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

새 액세스 목록 기능

PIX 소프트웨어 릴리스 5.2 이상에서는 PIX에서 액세스 목록을 정의합니다. 서버의 사용자 프로필에 따라 사용자별로 적용합니다. TACACS+에는 인증 및 권한 부여가 필요합니다. RADIUS에는 인증만 필요합니다. 이 예에서는 TACACS+에 대한 아웃바운드 인증 및 권한 부여가 변경됩니다. PIX의 액세스 목록이 설정됩니다.

참고: PIX 버전 6.0.1 이상에서 RADIUS를 사용하는 경우 표준 IETF RADIUS 특성 11(Filter-Id) [CSCdt50422]에 목록을 입력하여 액세스 목록이 구현됩니다. 이 예에서 특성 11은 공급업체별 "acl=115" 버전 대신 115로 설정됩니다.

PIX 컨피그레이션

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

서버 프로파일

참고: 2.1 버전의 TACACS+ 프리웨어는 "acl" 버전을 인식하지 않습니다.

Cisco Secure UNIX TACACS+ 서버 컨피그레이션

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Cisco Secure Windows TACACS+

PIX에 권한 부여를 추가하여 사용자가 액세스 목록과 함께 이동하는 위치를 제어하려면 **shell/exec**을 선택하고 **Access control list**(액세스 제어 목록) 상자를 선택한 다음 번호를 입력합니다(PIX의 액세스 목록 번호와 일치).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Cisco Secure Windows RADIUS

RADIUS/Cisco는 디바이스 유형입니다. "pixa" 사용자는 Cisco/RADIUS 사각형 상자에 009\001 AV-Pair(벤더별)라는 사용자 이름, 비밀번호, 체크 및 "acl=115"가 필요합니다.

출력

프로필에서 "acl=115"를 사용하는 아웃바운드 사용자 "pixa"가 인증되고 인증됩니다. 서버가 acl=115를 PIX로 전달하면 PIX에 다음과 같은 내용이 표시됩니다.

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
   access-list 115
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

사용자 "pixa"가 99.99.99.3(또는 암시적 거부가 있으므로 99.99.99.2을 제외한 모든 IP 주소)로 이동하려고 시도하면 사용자는 다음과 같이 표시됩니다.

```
Error: acl authorization denied
```

버전 6.2의 새로운 사용자별 다운로드 가능 액세스 목록

PIX 방화벽의 소프트웨어 릴리스 6.2 이상에서는 인증 후 PIX로 다운로드하기 위해 액세스 목록이

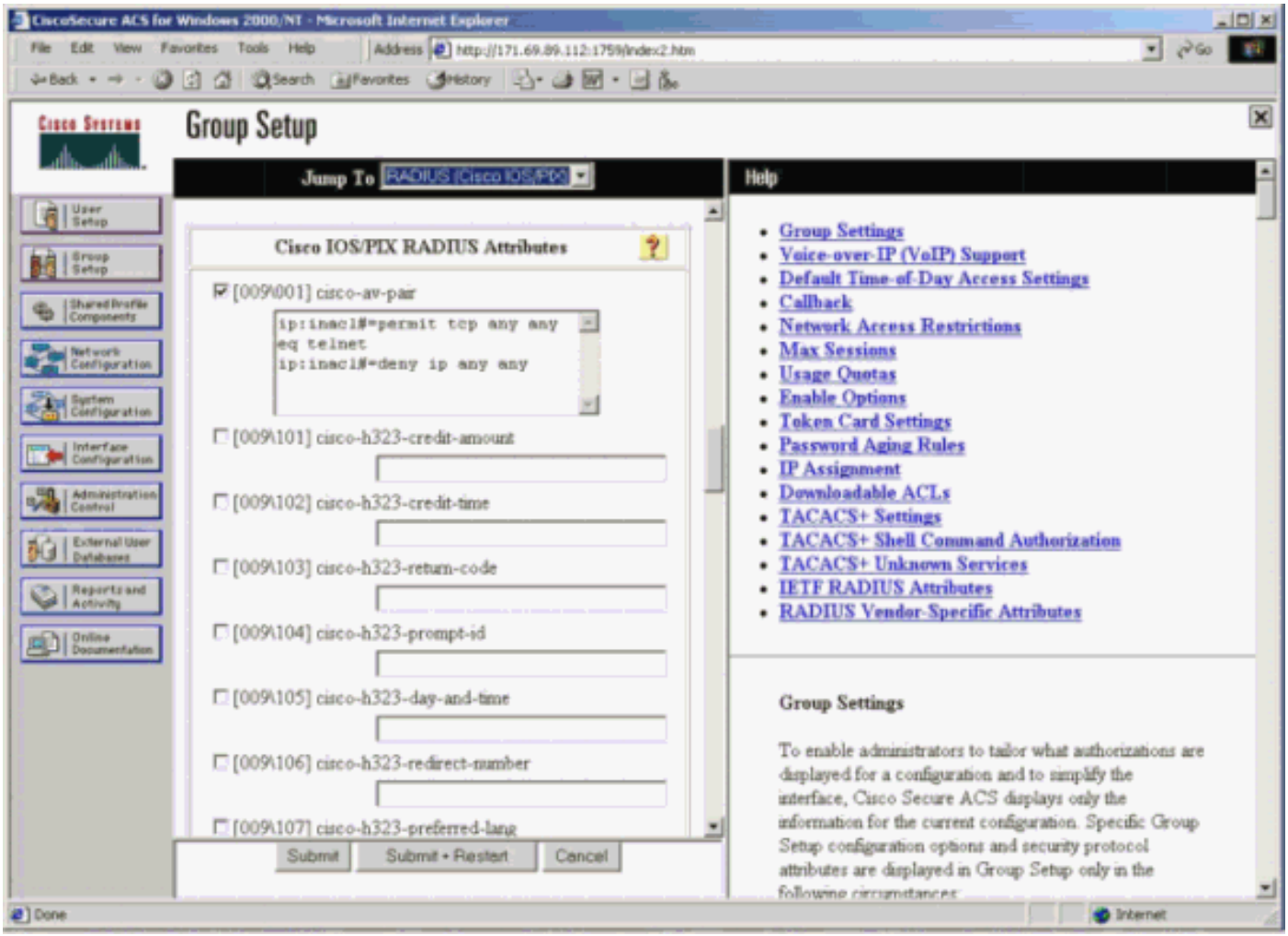
ACS(액세스 제어 서버)에 정의됩니다. 이는 RADIUS 프로토콜에서만 작동합니다. PIX 자체에서 액세스 목록을 구성할 필요가 없습니다. 그룹 템플릿은 여러 사용자에게 적용됩니다.

이전 버전에서는 액세스 목록이 PIX에 정의되어 있습니다. 인증 시 ACS는 액세스 목록 이름을 PIX로 푸시했습니다. 새 버전을 사용하면 ACS가 액세스 목록을 PIX에 직접 푸시할 수 있습니다.

참고: 장애 조치가 발생하면 uauth 테이블이 복사되지 않습니다. 사용자가 다시 인증됩니다. 액세스 목록이 다시 다운로드됩니다.

ACS 설정

Group **Setup(그룹 설정)**을 클릭하고 **RADIUS(Cisco IOS/PIX)** 디바이스 유형을 선택하여 사용자 계정을 설정합니다. 사용자에 대한 사용자 이름("cse", 이 예에서는) 및 비밀번호를 할당합니다. Attributes(특성) 목록에서 **[009\001]** ***vendor-av*-pair를** 구성하는 옵션**을 선택합니다**. 다음 예에 설명된 대로 액세스 목록을 정의합니다.



PIX 디버그: 유효한 인증 및 다운로드한 액세스 목록

- 텔넷만 허용하고 다른 트래픽을 거부합니다.

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
```

```
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

show uauth 명령의 **출력입니다**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

show access-list 명령의 출력입니다.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- 텔넷만 거부하고 다른 트래픽을 허용합니다.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

show uauth 명령의 **출력입니다**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

show access-list 명령의 출력입니다.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

ACS 3.0을 사용한 사용자별 새로운 다운로드 가능 액세스 목록

ACS 버전 3.0에서 공유 프로필 구성 요소를 사용하면 사용자가 액세스 목록 템플릿을 생성하고 특정 사용자 또는 그룹에 템플릿 이름을 정의할 수 있습니다. 템플릿 이름은 필요한 만큼 많은 사용자 또는 그룹과 함께 사용할 수 있습니다. 따라서 각 사용자에 대해 동일한 액세스 목록을 구성할 필요가 없습니다.

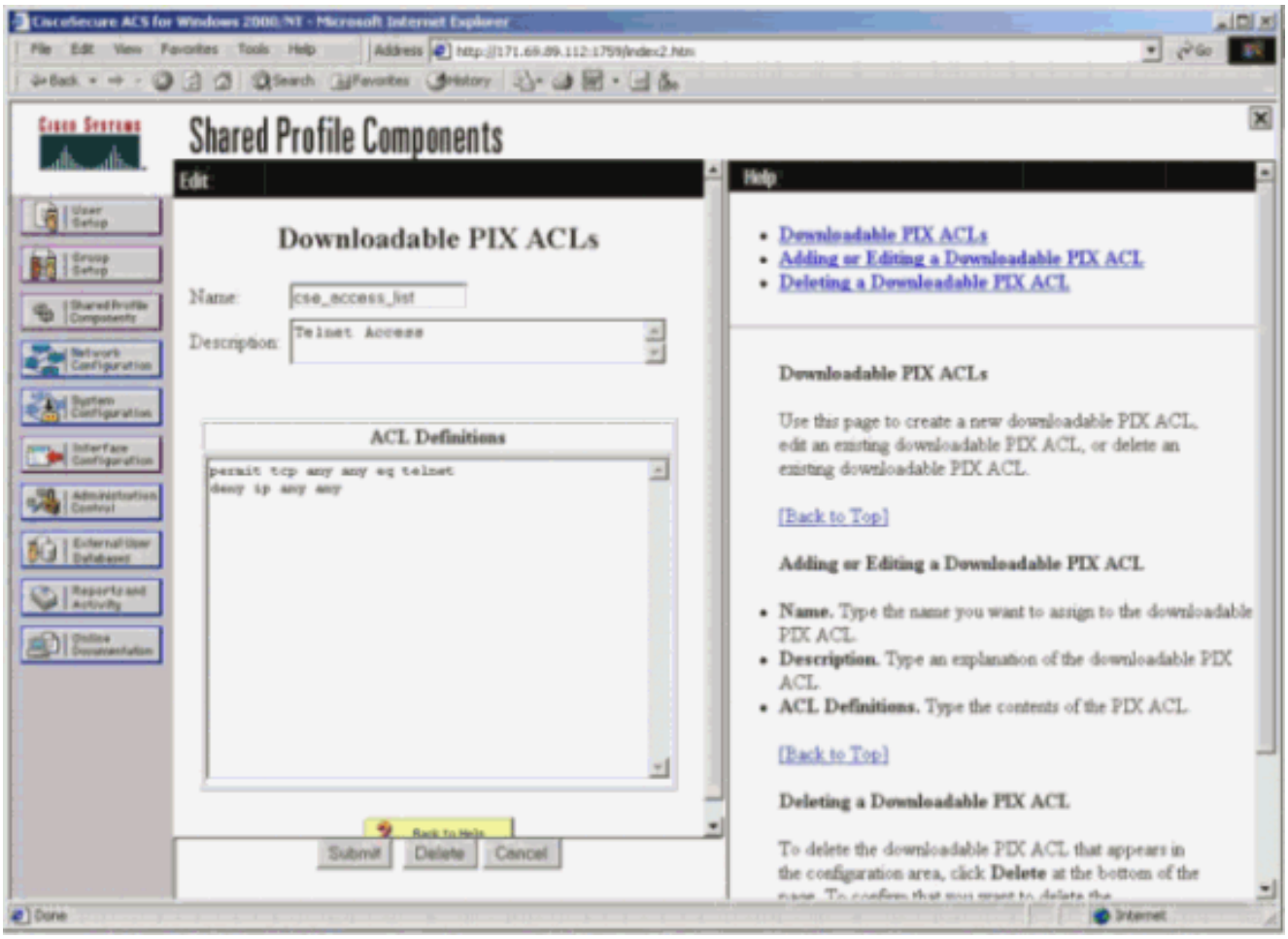
참고: 장애 조치가 발생하면 uauth는 보조 PIX에 복사되지 않습니다. 스테이트풀 장애 조치에서는 세션이 유지됩니다. 그러나 새 연결을 다시 인증하고 액세스 목록을 다시 다운로드해야 합니다.

공유 프로파일 사용

공유 프로파일을 사용할 때 다음 단계를 완료합니다.

1. Interface **Configuration을 클릭합니다**.
2. 사용자 **수준 다운로드 가능한 ACL** 및/또는 **그룹 수준 다운로드 가능한 ACL을 확인합니다**.
3. Shared **Profile Components를 클릭합니다**. User-**Level Downloadable ACLs를 클릭합니다**.
4. 다운로드 가능한 ACL을 정의합니다.
5. Group **Setup을 클릭합니다**. Downloadable ACLs(다운로드 가능한 ACL)에서 앞서 생성한 액세스 목록에 PIX 액세스 목록을 할당합니다

.



PIX 디버그: 공유 프로필을 사용하여 유효한 인증 및 다운로드한 액세스 목록

- 텔넷만 허용하고 다른 트래픽을 거부합니다.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

show uauth 명령의 **출력입니다**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
```

```
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

show access-list 명령의 출력입니다.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- 텔넷만 거부하고 다른 트래픽을 허용합니다.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

show uauth 명령의 **출력입니다**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

show access-list 명령의 출력입니다.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

계정 추가

PIX 컨피그레이션 - 어카운팅 추가

TACACS(AuthInbound=tacacs)

이 명령을 추가합니다.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

또는 5.2의 새 기능을 사용하여 액세스 목록으로 계상할 항목을 정의합니다.

aaa accounting match 101 outside AuthInbound

참고: 액세스 목록 101은 별도로 정의됩니다.

RADIUS(AuthOutbound=radius)

이 명령을 추가합니다.

aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

또는 5.2의 새 기능을 사용하여 액세스 목록으로 계상할 항목을 정의합니다.

aaa accounting match 101 outside AuthOutbound

참고: 액세스 목록 101은 별도로 정의됩니다.

참고: PIX 7.0 코드부터 시작하여 PIX의 관리 세션에 대한 회계 레코드를 생성할 수 있습니다.

회계 예

- 텔넷을 외부99.99.99.2 내부(99.99.99.99)으로 172.18.124.114에 대한 TACACS 계정 예시.

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- 내부172.18.124.114에서 99.99.99.2(텔넷) 및 99.99.99.3 외부(HTTP)로 연결하는 RADIUS 계정 관리 예

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
```

```
            Acct-Input-Octets = 101
            Acct-Output-Octets = 143
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35937
            Vendor-Specific = Destination-IP=99.99.99.2
            Vendor-Specific = Destination-Port=23

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Start
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Username = cse
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Stop
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Acct-Session-Id = 0x0000000a
            Username = cse
            Acct-Session-Time = 0
            Acct-Input-Octets = 1277
            Acct-Output-Octets = 310
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80
```

exclude 명령 사용

이 네트워크에서 특정 소스 또는 목적지에 인증, 권한 부여 또는 어카운팅이 필요하지 않다고 결정할 경우 다음 명령을 실행합니다.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

참고: include 명령이 이미 있습니다.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

또는 5.2의 새 기능을 사용하여 제외할 항목을 정의합니다.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
```

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa accounting match 101 outside AuthInbound
```

참고: 인증에서 상자를 제외하고 권한 부여가 설정된 경우 인증에서도 상자를 제외해야 합니다.

최대 세션 수 및 로그인한 사용자 보기

일부 TACACS+ 및 RADIUS 서버에는 "max-session" 또는 "view logged-in users" 기능이 있습니다. 최대 세션 또는 로그인 사용자를 확인하는 기능은 회계 기록에 따라 달라집니다. 계정 "시작" 레코드가 생성되었지만 "중지" 레코드가 없는 경우 TACACS+ 또는 RADIUS 서버는 사용자가 여전히 로그인되어 있다고 가정합니다(즉, 사용자가 PIX를 통해 세션을 가지고 있음). 이는 연결의 특성 때문에 텔넷 및 FTP 연결에 적합합니다. 그러나 HTTP에서는 이 기능이 제대로 작동하지 않습니다. 이 예에서는 다른 네트워크 컨피그레이션이 사용되지만 개념이 동일합니다.

사용자가 PIX를 통해 전화를 걸어 도중에 인증합니다.

```
(pix) 109001: Auth start for user '???' from
         171.68.118.100/1200 to 9.9.9.25 /23
     (pix) 109011: Authen Session Start: user 'cse', Sid 3
     (pix) 109005: Authentication succeeded for user
         'cse' from 171.68.118.100/1200 to 9.9.9.25/23
     (pix) 302001: Built TCP connection 5 for
         faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 laddr
         171.68.118.100/1200 (cse)
     (server start account) Sun Nov 8 16:31:10 1998
         rtp-pinecone.rtp.cisco.com cse
         PIX 171.68.118.100 start task_id=0x3
         foreign_ip=9.9.9.25
         local_ip=171.68.118.100 cmd=telnet
```

서버가 "시작" 레코드를 보았지만 "중지" 레코드가 없기 때문에 이 시점에서 서버는 "텔넷" 사용자가 로그인되어 있음을 표시합니다. 사용자가 인증을 필요로 하는 다른 연결(아마도 다른 PC의 연결)을 시도하고, 이 사용자에 대해 서버에서 max-sessions가 "1"로 설정된 경우(서버가 max-sessions를 지원하는 것으로 가정) 서버에서 연결이 거부됩니다. 사용자는 대상 호스트에서 텔넷 또는 FTP 비즈니스를 수행한 다음 종료합니다(10분 동안).

```
     (pix) 302002: Teardown TCP connection 5 faddr
          9.9.9.25/80 gaddr 9.9.9.10/128 1 laddr
          171.68.118.100/1281 duration 0:00:00 bytes
          1907 (cse)
     (server stop account) Sun Nov 8 16:41:17 1998
          rtp-pinecone.rtp.cisco.com
     cse PIX 171.68.118.100 stop task_id=0x3
          foreign_ip=9.9.9.25 local_ip=171.68.118.100
          cmd=telnet elapsed_time=5 bytes_in=98
          bytes_out=36
```

uauth가 0(즉, 매번 인증) 또는 그 이상(uauth 기간 동안 한 번 인증하고 다시 인증하지 않음)인지 여부에 관계없이 액세스한 모든 사이트에 대해 계정 레코드가 잘립니다.

HTTP는 프로토콜의 특성 때문에 다르게 작동합니다. 다음은 사용자가 PIX를 통해 171.68.118.100에서 9.9.9.25까지 검색하는 HTTP의 예입니다.

```
(pix) 109001: Auth start for user '???' from
    171.68.118.100/1281 to 9.9.9.25 /80
(pix) 109011: Authen Session Start: user 'cse', Sid 5
(pix) 109005: Authentication succeeded for user
    'cse' from 171.68.118.100/12 81 to 9.9.9.25/80
(pix) 302001: Built TCP connection 5 for faddr
    9.9.9.25/80 gaddr 9.9.9.10/12 81 laddr
    171.68.118.100/1281 (cse)
(server start account) Sun Nov 8 16:35:34 1998
    rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 start task_id=0x9
    foreign_ip=9.9.9.25 local_ip=171.68.118.100 cmd=http
(pix) 302002: Teardown TCP connection 5 faddr
    9.9.9.25/80 gaddr 9.9.9.10/128 1
laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35.35 1998
    rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9
    foreign_ip =9.9.9.25 local_ip=171.68.118.100
    cmd=http elapsed_time=0 bytes_ in=1907 bytes_out=223
```

사용자는 다운로드한 웹 페이지를 읽습니다. 시작 레코드는 16:35:34에 게시되고 중지 레코드는 16:35:35에 게시됩니다. 이 다운로드는 1초(즉, 시작 레코드와 중지 레코드 사이에 1초 미만이 소요되었습니다.) 사용자가 웹 사이트에 로그인하지 않았습니다. 사용자가 웹 페이지를 읽을 때 연결이 열리지 않습니다. 최대 세션 또는 로그인한 사용자 보기는 여기서 작동하지 않습니다. HTTP의 연결 시간(HTTP의 "Built" 및 "Teardown" 사이의 시간)이 너무 짧기 때문입니다. "start" 및 "stop" 레코드는 초 미만의 것입니다. "중지" 기록이 없는 "시작" 기록은 거의 동일한 순간에 발생하므로 없습니다. uauth가 0으로 설정되었는지 또는 그 이상으로 설정되었는지에 관계없이 모든 트랜잭션에 대해 서버로 전송된 "시작" 및 "중지" 레코드가 여전히 있습니다. 그러나 HTTP 연결의 특성 때문에 최대 세션 및 로그인 사용자 보기가 작동하지 않습니다.

사용자 인터페이스

프롬프트 사용자 변경 참조

명령이 있는 경우

auth-prompt prompt PIX515B

PIX를 통해 이동하는 사용자는 이 프롬프트를 확인합니다.

PIX515B

메시지 사용자 맞춤화 참조

명령이 있는 경우

auth-prompt accept "GOOD_AUTHENTICATION"
auth-prompt reject "BAD_AUTHENTICATION"

그러면 사용자는 실패/성공 로그인 시 인증 상태에 대한 메시지를 볼 수 있습니다.

```
PIX515B
Username: junk
Password:
"BAD_AUTHENTICATION"

PIX515B
Username: cse
Password:
"GOOD_AUTHENTICATION"
```

사용자별 유휴 및 절대 시간 제한

PIX timeout uauth 명령**은** 재인증이 필요한 빈도를 제어합니다. TACACS+ 인증/권한 부여가 설정된 경우 사용자별로 제어됩니다. 이 사용자 프로필은 시간 초과를 제어하도록 설정됩니다 (TACACS+ 프리웨어 서버에 있으며 시간 초과는 분 단위임).

```
user = cse {
default service = permit
login = cleartext "csecse"
service = exec {
timeout = 2
idletime = 1
}
}
```

인증/권한 부여 후:

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

2분 후:

절대 시간 초과 - 세션이 해제됩니다.

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

가상 HTTP 아웃바운드

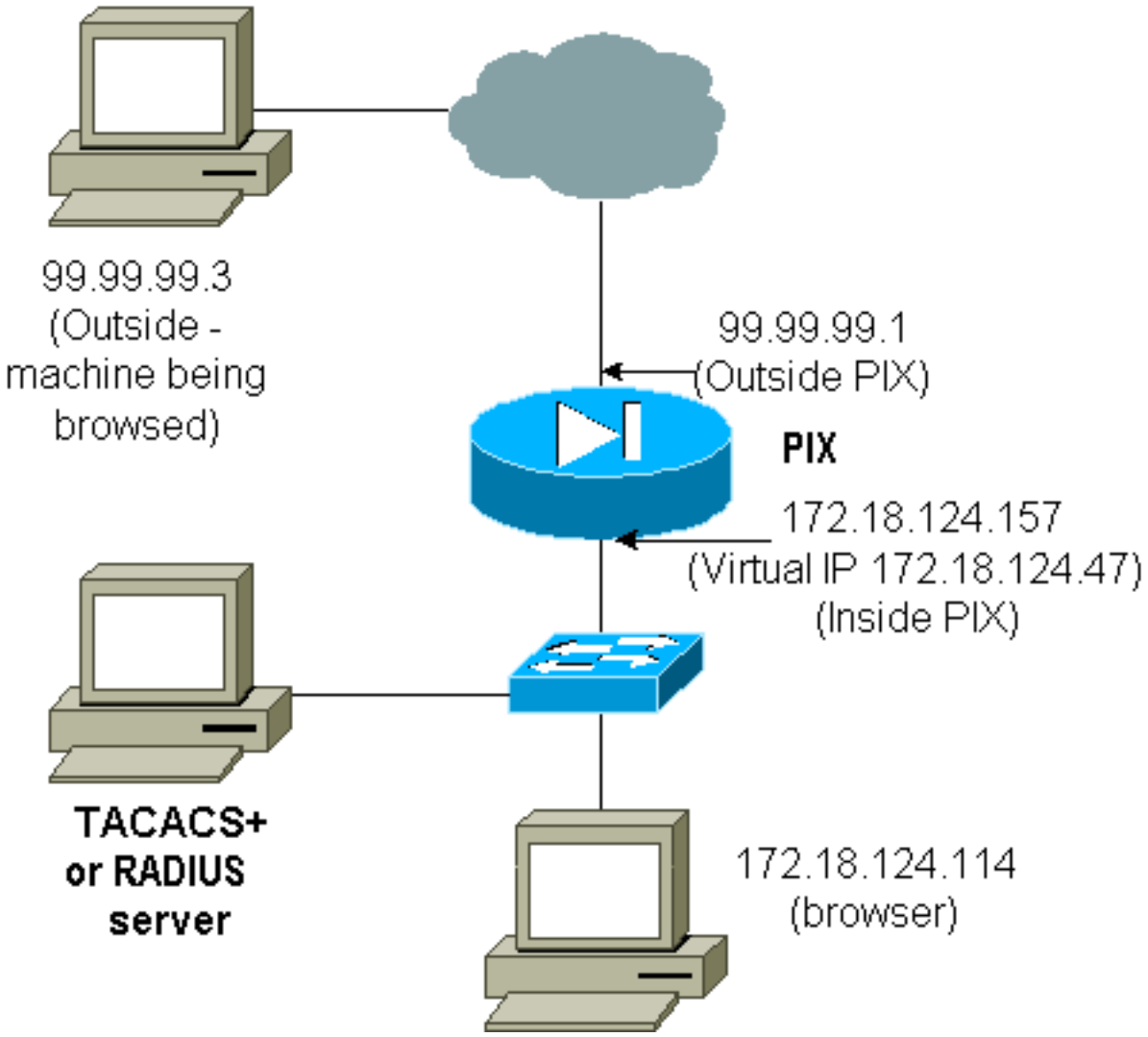
PIX 외부의 사이트와 PIX 자체에서 인증이 필요한 경우 브라우저가 사용자 이름과 비밀번호를 캐시하므로 비정상적인 브라우저 동작이 관찰될 수 있습니다.

이를 방지하려면 PIX 컨피그레이션에 RFC 1918 주소(인터넷에서 라우팅할 수 없지만 PIX 내부 네트워크에 대해 유효하고 고유한 주소)를 추가하여 가상 HTTP를 구현합니다.

```
virtual http #.#.#.#
```

사용자가 PIX 외부로 나가려고 할 때 인증이 필요합니다. 경고 매개 변수가 있으면 사용자는 리디렉션 메시지를 받습니다. 인증은 uauth의 시간 동안 유효합니다. 설명서에 나와 있는 대로 가상 HTTP를 사용하여 **timeout uauth** 명령 지속 시간을 0초로 설정하지 마십시오. 이렇게 하면 실제 웹 서버에 대한 HTTP 연결이 방지됩니다.

참고: 가상 HTTP 및 가상 텔넷 IP 주소는 aaa **authentication** 문에 포함되어야 합니다. 이 예에서 0.0.0.0을 지정하면 이러한 주소가 포함됩니다.



PIX 컨피그레이션에서 이 명령을 추가합니다.

```
virtual http 172.18.124.47
```

사용자가 브라우저를 99.99.99.3으로 가리킵니다. 이 메시지가 표시됩니다.

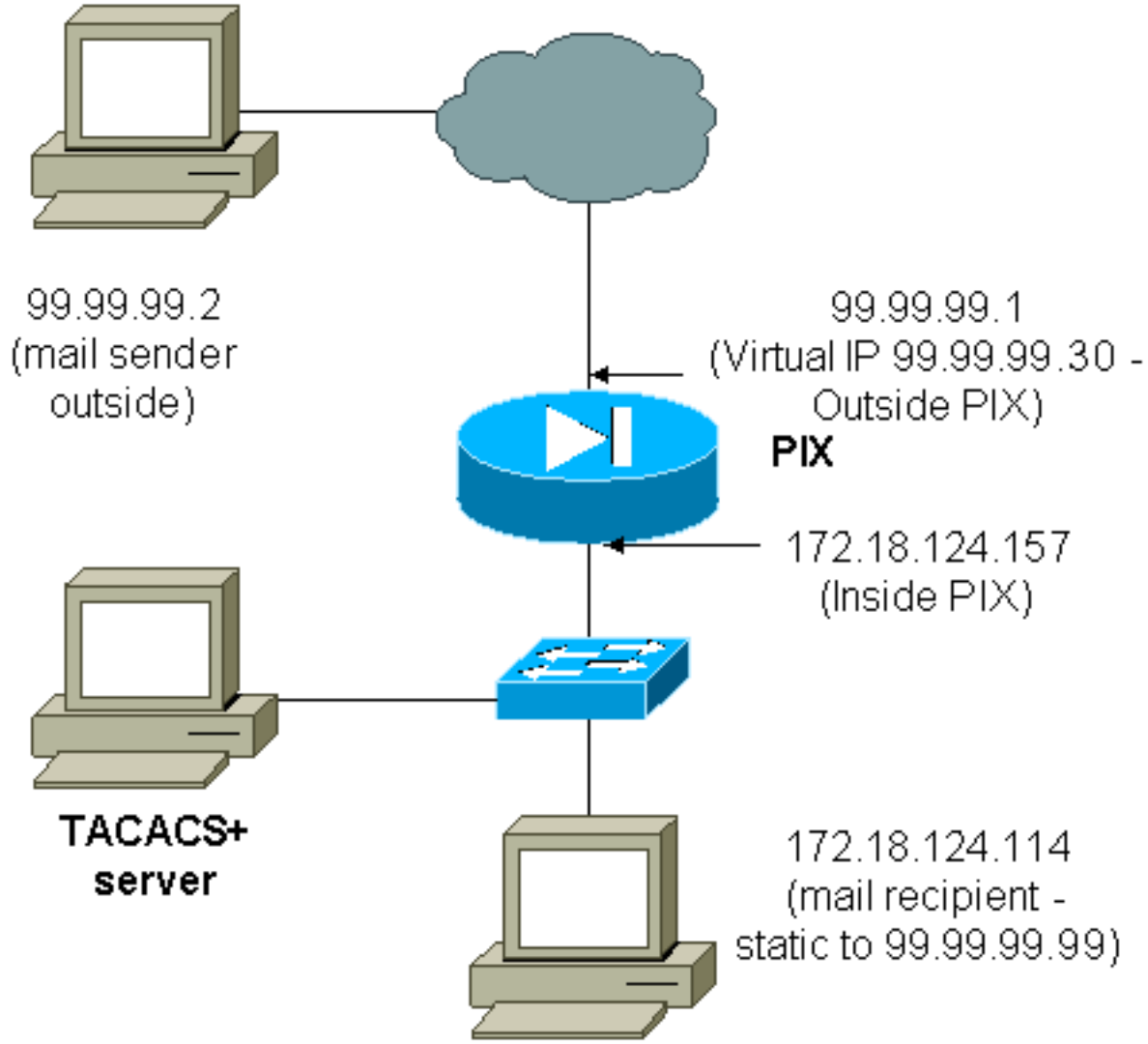
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

인증 후 트래픽은 99.99.99.3으로 리디렉션됩니다.

가상 텔넷

참고: 가상 HTTP 및 가상 텔넷 IP 주소는 aaa **authentication** 문에 포함되어야 합니다. 이 예에서 0.0.0.0을 지정하면 이러한 주소가 포함됩니다.

가상 텔넷 인바운드



인바운드 메일을 보낼 수 있는 창이 표시되지 않으므로 인바운드 메일을 인증하는 것은 좋은 방법이 아닙니다. 대신 **exclude** 명령을 사용합니다. 그러나 설명을 위해 이러한 명령이 추가됩니다.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
```

```
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

사용자(TACACS+ 프리웨어):

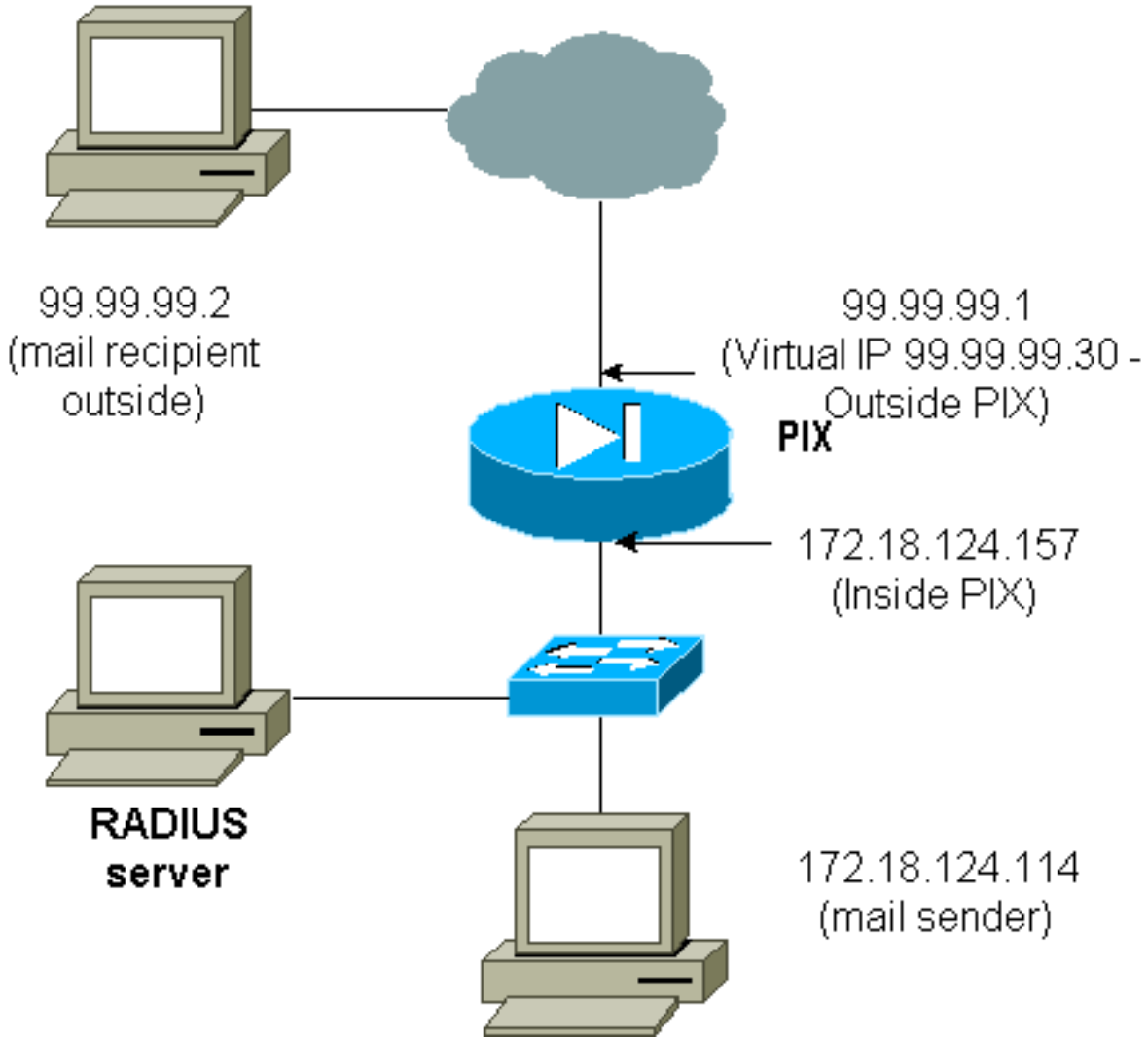
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

인증만 설정된 경우 두 사용자 모두 텔넷에서 IP 주소 99.99.99.30으로 인증한 후 인바운드 메일을 보냅니다. 권한 부여가 활성화된 경우 사용자 "cse"는 99.99.99.30으로 텔넷하고 TACACS+ 사용자 이름/비밀번호를 입력합니다. 텔넷 연결이 끊깁니다. 그런 다음 "cse" 사용자가 99.99.99.99(172.18.124.114)에 메일을 보냅니다. 사용자 "pixuser"에 대한 인증이 성공했습니다. 그러나 PIX가 cmd=tcp/25 및 cmd-arg=172.18.124.114에 대한 권한 부여 요청을 보내면 이 출력에 표시된 대로 요청이 실패합니다.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
```

```
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

가상 텔넷 아웃바운드



인바운드 메일을 보낼 수 있는 창이 표시되지 않으므로 인바운드 메일을 인증하는 것은 좋은 방법이 아닙니다. 대신 **exclude** 명령을 사용합니다. 그러나 설명을 위해 이러한 명령이 추가됩니다.

아웃바운드 메일을 보낼 수 있는 창이 표시되지 않으므로 아웃바운드 메일을 인증하는 것은 좋지 않습니다. 대신 **exclude** 명령을 사용합니다. 그러나 설명을 위해 이러한 명령이 추가됩니다.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

내부에서 외부로 메일을 보내려면 메일 호스트에서 명령 프롬프트를 99.99.99.30으로 표시하고, 이렇게 하면 메일을 통과할 수 있는 구멍이 열립니다. 메일이 172.18.124.114에서 99.99.99.2으로 전송됩니다.

```
   305002: Translation built for gaddr 99.99.99.99
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

가상 텔넷 로그아웃

사용자가 가상 텔넷 IP 주소에 텔넷할 때 **show uauth** 명령은 구멍이 열린 시간을 표시합니다. 세션이 끝난 후(시간이 uauth에 남아 있는 경우) 사용자가 트래픽을 통과하지 못하게 하려면 가상 텔넷 IP 주소에 다시 텔넷해야 합니다. 이렇게 하면 세션이 해제됩니다. 이 예제는 다음과 같습니다.

첫 번째 인증

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

첫 번째 인증 후

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
```

```
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

두 번째 인증

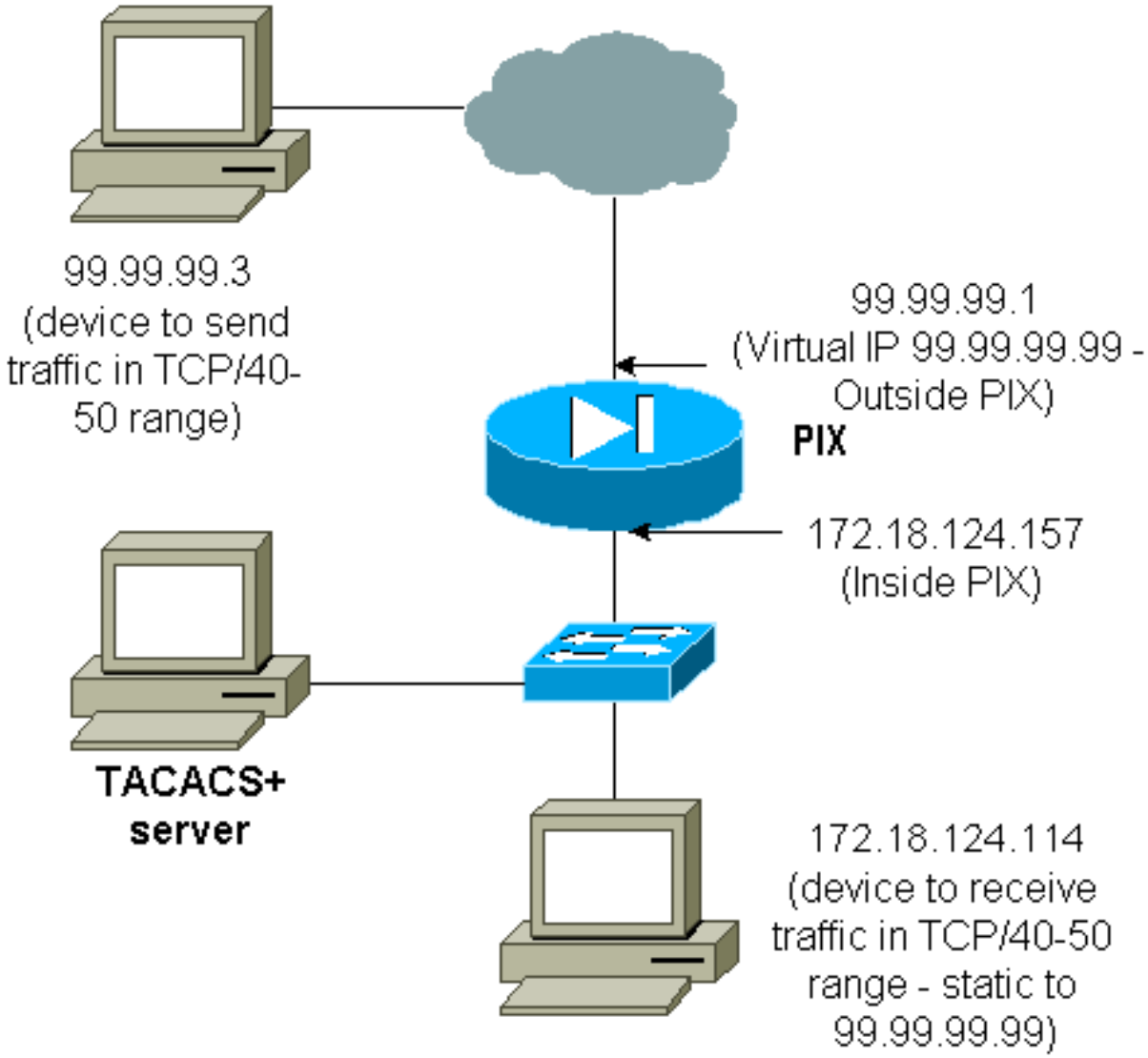
```
   pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

두 번째 인증 후

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

포트 권한 부여

네트워크 다이어그램



포트 범위에 대해 권한 부여가 허용됩니다. PIX에 가상 텔넷이 구성되어 있고 포트 범위에 대한 권

한 부여가 구성된 경우, 사용자는 가상 텔넷으로 구멍을 엽니다. 그런 다음 포트 범위에 대한 권한 부여가 켜져 있고 해당 범위의 트래픽이 PIX에 도달하면 PIX는 권한 부여를 위해 TACACS+ 서버로 명령을 전송합니다. 이 예에서는 포트 범위에 대한 인바운드 인증을 보여줍니다.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

TACACS+ 서버 컨피그레이션 예(프리웨어):

```
  user = cse {
  login = cleartext "numeric"
  cmd = tcp/40-50 {
  permit 172.18.124.114
  }
  }
```

사용자는 먼저 가상 IP 주소 99.99.99.99에 텔넷해야 합니다. 인증 후 사용자가 PIX를 통해 포트 40-50 범위의 TCP 트래픽을 99.99.99.99(172.18.124.114)으로 푸시하려고 할 때 cmd=tcp/40-50은 다음과 같이 cmd-arg=172.18.124.114을 사용하여 TACACS+ 서버로 전송됩니다.

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

HTTP, FTP 및 텔넷 이외의 트래픽에 대한 AAA 어카운팅

가상 텔넷이 네트워크 내부의 호스트에 대한 TCP/40-50 트래픽을 허용하도록 작동하는지 확인한 후 이러한 명령으로 이 트래픽에 대한 어카운팅을 추가합니다.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.
```

```
aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

TACACS+ 어카운팅 레코드의 예

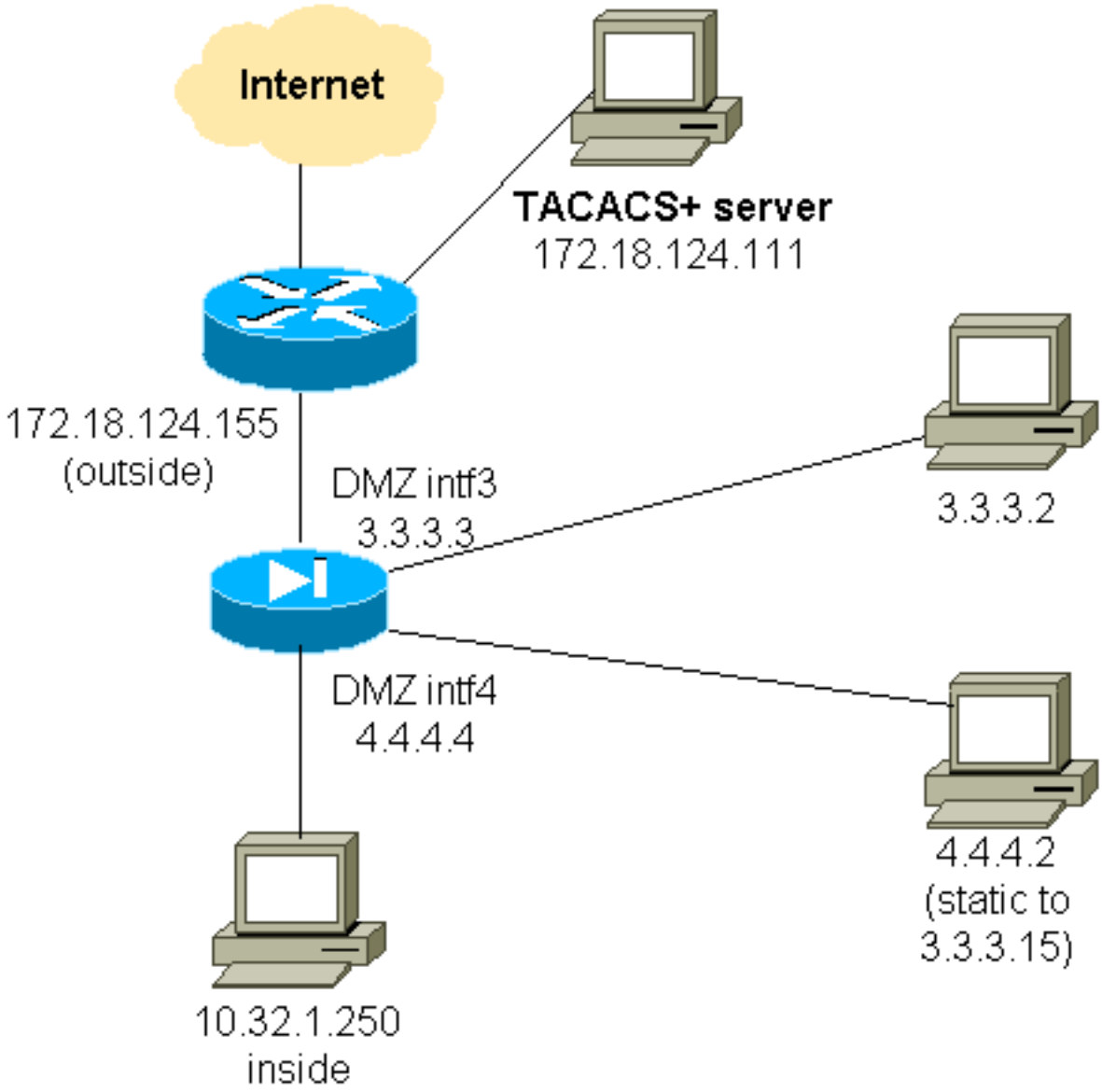
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

DMZ의 인증

한 DMZ 인터페이스에서 다른 인터페이스로 이동하는 사용자를 인증하려면 PIX에 명명된 인터페이스에 대한 트래픽을 인증하도록 지시합니다. PIX에서는 다음과 같은 방식으로 구성됩니다.

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

네트워크 다이어그램



부분 PIX 컨피그레이션

여기서 설명한 대로 pix/intf3 및 pix/intf4 간의 텔넷 트래픽을 인증합니다.

부분 PIX 컨피그레이션

```
  nameif ethernet0 outside security0
  nameif ethernet1 inside security100
  (nameif ethernet2 pix/intf2 security10)
  nameif ethernet3 pix/intf3 security15
  nameif ethernet4 pix/intf4 security20
  (nameif ethernet5 pix/intf5 security25)
  interface ethernet0 auto
  interface ethernet1 auto
  (interface ethernet2 auto shutdown)
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
```

```
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

TAC 케이스를 열 경우 수집할 정보

위의 트러블슈팅 단계를 거친 후에도 지원이 필요한 경우 Cisco TAC에서 케이스를 열려면 PIX 방화벽 트러블슈팅을 위해 이 정보를 포함해야 합니다.

- 문제 설명 및 관련 토폴로지 세부사항
- 케이스를 열기 전에 문제 해결
- **show tech-support** 명령의 출력
- **logging buffered 디버깅** 명령을 사용하여 실행한 후 **show log** 명령 또는 문제를 보여 주는 콘솔 캡처(사용 가능한 경우)의 출력

수집된 데이터를 압축되지 않은 일반 텍스트 형식(.txt)으로 케이스에 첨부합니다. Case Query Tool의 도움을 받아 업로드하여 케이스에 정보를 첨부합니다(등록된 고객만 해당). Case Query Tool에 액세스할 수 없는 경우 이메일 첨부 파일의 정보를 attach@cisco.com으로 전송하고, 케이스 번호는 메시지의 제목 줄에 입력합니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- Windows용 Cisco Secure Access Control Server
- UNIX용 Cisco Secure Access Control Server
- TACACS+(Terminal Access Controller Access Control System)
- 원격 인증 전화 접속 사용자 서비스(RADIUS)
- 기술 지원 및 문서 – Cisco Systems