PIX 5.1.x 구성:TACACS+ 및 RADIUS

목차

소개

FTP, 텔넷 및 HTTP 연결에 대해 RADIUS 및 TACACS+ 인증을 수행할 수 있습니다.일반적으로 다른 덜 일반적인 프로토콜에 대한 인증은 작동하게 할 수 있습니다.TACACS+ 권한 부여가 지원됩니다.RADIUS 권한 부여가 아닙니다.이전 버전에 대한 PIX 5.1 인증, 권한 부여 및 계정 관리(AAA)의 변경 사항에는 Cisco Secure VPN Client 1.1에서 IPSec 터널의 인증(xauth)이 포함됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

배경 정보

인증 대 권한 부여

- 인증은 사용자의 이름입니다.
- 권한 부여는 사용자가 수행할 수 있는 작업입니다.
- 인증*은 권한* 없이 유효합니다.
- 인증*이* 없으면 권한 부여가 유효하지 않습니다.
- 어카운팅은 사용자가 한 것입니다.

사용자 수가 100명이고 이러한 사용자 중 6명만 네트워크 외부에서 FTP, 텔넷 또는 HTTP를 수행할 수 있도록 하려는 경우를 가정해보겠습니다.PIX에 아웃바운드 트래픽을 인증하도록 지시하고 TACACS+/RADIUS 보안 서버에 있는 6명의 사용자 ID를 모두 제공합니다.간단한 인증으로 이 6명의 사용자는 사용자 이름과 비밀번호를 사용하여 인증한 다음 로그아웃할 수 있습니다.나머지 94명의 사용자는 나갈 수 없었습니다.PIX는 사용자에게 사용자 이름/비밀번호를 묻는 메시지를 표시한 다음 사용자 이름과 비밀번호를 TACACS+/RADIUS 보안 서버에 전달하며, 응답에 따라 연결을 열거나 거부합니다.이 6명의 사용자는 FTP, 텔넷 또는 HTTP를 수행할 수 있습니다.

그러나 *이* 6명의 사용자 중 "Fest"는 신뢰할 수 없다고 가정해 보겠습니다.Festus가 FTP를 수행하도록 허용하되 HTTP 또는 텔넷을 외부에 허용하지 않습니다.이는 *권한 부여*를 추가해야 한다는 것을 의미합니다. 즉 사용자가 인증을 받는 것 외에도 수행할 수 있는 작업을 인증해야 합니다.이는 TACACS+에서만 유효합니다.PIX에 *권한 부여*를 추가하면 PIX는 먼저 Fesus의 사용자 이름과 비밀번호를 보안 서버로 전송한 다음 Festus가 수행하려는 "*명령*"을 보안 서버에 알리는 권한 부여 요

청을 보냅니다.서버가 올바르게 설정되면 Fesus는 "ftp 1.2.3.4"을 허용하지만 HTTP 또는 텔넷 기능이 거부됩니다.

인증/권한 부여를 통해 사용자에게 표시되는 내용

인증/권한 부여를 사용하여 내부에서 외부로(또는 그 반대로) 이동할 때:

- **텔넷** - 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 **비밀번호는 local_password@remote_password**를 입력해야 합니다.PIX는 local_username 및 local_password를 로컬 보안 서버로 전송하고 PIX/서버에서 인증(및 권한 부여)이 성공하면 remote_username 및 remote_password는 그 이후의 대상 FTP 서버로 전달됩니다.
- **HTTP** - 사용자 이름과 비밀번호를 요청하는 창이 브라우저에 표시됩니다.인증(및 권한 부여)에 성공하면 사용자가 대상 웹 사이트에 도착합니다.*브라우저*에서 *사용자 이름과 암호를 캐시한 다는 점에 유의하십시오*.PIX가 HTTP 연결을 시간 초과해야 하지만 시간 초과로 표시되지 않는 경우, 브라우저가 캐시된 사용자 이름 및 비밀번호를 PIX로 전송하면서 재인증이 실제로 수행되고 있는 것으로 보입니다. 그러면 인증 서버에 이 사용자 이름과 비밀번호를 전달합니다.PIX syslog 및/또는 서버 디버그는 이 현상을 표시합니다.텔넷과 FTP가 정상적으로 작동하는 것처럼 보이지만 HTTP 연결이 정상적으로 작동하지 않는 경우, 이러한 이유가 됩니다.
- **Tunnel** - VPN Client 및 xauth를 사용하여 IPSec 트래픽을 네트워크로 터널링하려고 할 때 사용자 이름/비밀번호에 대해 "User Authentication for New Connection(새 연결을 위한 사용자 인증)"에 대한 회색 상자가 표시됩니다.**참고:** 이 인증은 Cisco Secure VPN Client 1.1부터 지원됩니다. **도움말** > **정보** 메뉴**에** 버전 2.1.x 이상이 표시되지 않으면 이는 작동하지 않습니다.

모든 시나리오에 사용되는 보안 서버 구성

Cisco Secure UNIX TACACS 서버 컨피그레이션

이 섹션에는 보안 서버를 구성하는 정보가 표시됩니다.

CSU.cfg 파일에 PIX IP 주소 또는 정규화된 도메인 이름과 키가 있는지 확인합니다.

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

user = can_only_do_ftp {
password = clear "ftponly"
```

```
service = shell {
cmd = ftp {
permit .*
}
}
}

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

Cisco Secure UNIX RADIUS 서버 구성

GUI를 사용하여 PIX IP 주소 및 키를 Network Access Server (NAS) 목록에 추가합니다.

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
}
```

Windows 2.x RADIUS용 Cisco Secure ACS

다음 단계를 사용하여 Windows 2.x RADIUS용 Cisco Secure ACS를 구성합니다.

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

EasyACS TACACS+

EasyACS 설명서에서는 설정에 대해 설명합니다.

1. 그룹 섹션에서 **Shell exec**을 클릭하여 exec 권한을 부여합니다.
2. PIX에 권한 부여를 추가하려면 그룹 설정 하단의 **Deny unmatched IOS 명령**을 클릭합니다.
3. 허용할 각 명령**에 대해 Add/Edit new 명령**(예: Telnet)을 **선택합니다**.
4. 특정 사이트에 대한 텔네팅을 허용할 경우 인수 섹션의 "permit #.#.#.#" 형식으로 IP 주소를 입력합니다. 그렇지 않으면 텔네팅을 허용하려면 목록에 없는 **모든 인수 허용 을** 클릭합니다.
5. 편집 **완료 명령을 클릭합니다**.
6. 허용되는 각 명령(예: 텔넷, HTTP 또는 FTP)에 대해 1~5단계를 수행합니다.
7. NAS Configuration GUI 섹션에서 PIX IP를 추가합니다.

Cisco Secure 2.x TACACS+

사용자는 User Setup GUI 섹션에서 비밀번호를 얻습니다.

1. 그룹 섹션에서 **Shell exec**을 클릭하여 exec 권한을 부여합니다.
2. PIX에 권한 부여를 추가하려면 그룹 설정 하단에서 Deny unmatched IOS **명령**을 클릭합니다.
3. 허용할 각 명령(예: **텔넷**)에 대해 **Add/Edit new 명령**을 선택합니다.
4. 특정 사이트에 대한 텔네팅을 허용하려면 "permit #.#.#.#" 형식의 인수 섹션에 IP 주소를 입력합니다. 임의의 사이트에 텔네팅을 허용하려면 목록에 없는 **모든 인수 허용 을** 클릭합니다.
5. 편집 **완료 명령을 클릭합니다**.
6. 허용되는 각 명령(예: 텔넷, HTTP 또는 FTP)에 대해 1~5단계를 수행합니다.
7. PIX IP 주소가 NAS Configuration GUI 섹션에 추가되었는지 확인합니다.

Livingston RADIUS 서버 구성

Clients 파일에 PIX IP 주소 및 키를 추가합니다.

```
adminuser Password="all" User-Service-Type = Shell-User
```

Merit RADIUS 서버 구성

Clients 파일에 PIX IP 주소 및 키를 추가합니다.

```
adminuser Password="all" Service-Type = Shell-User
```

TACACS+ 프리웨어 서버 컨피그레이션

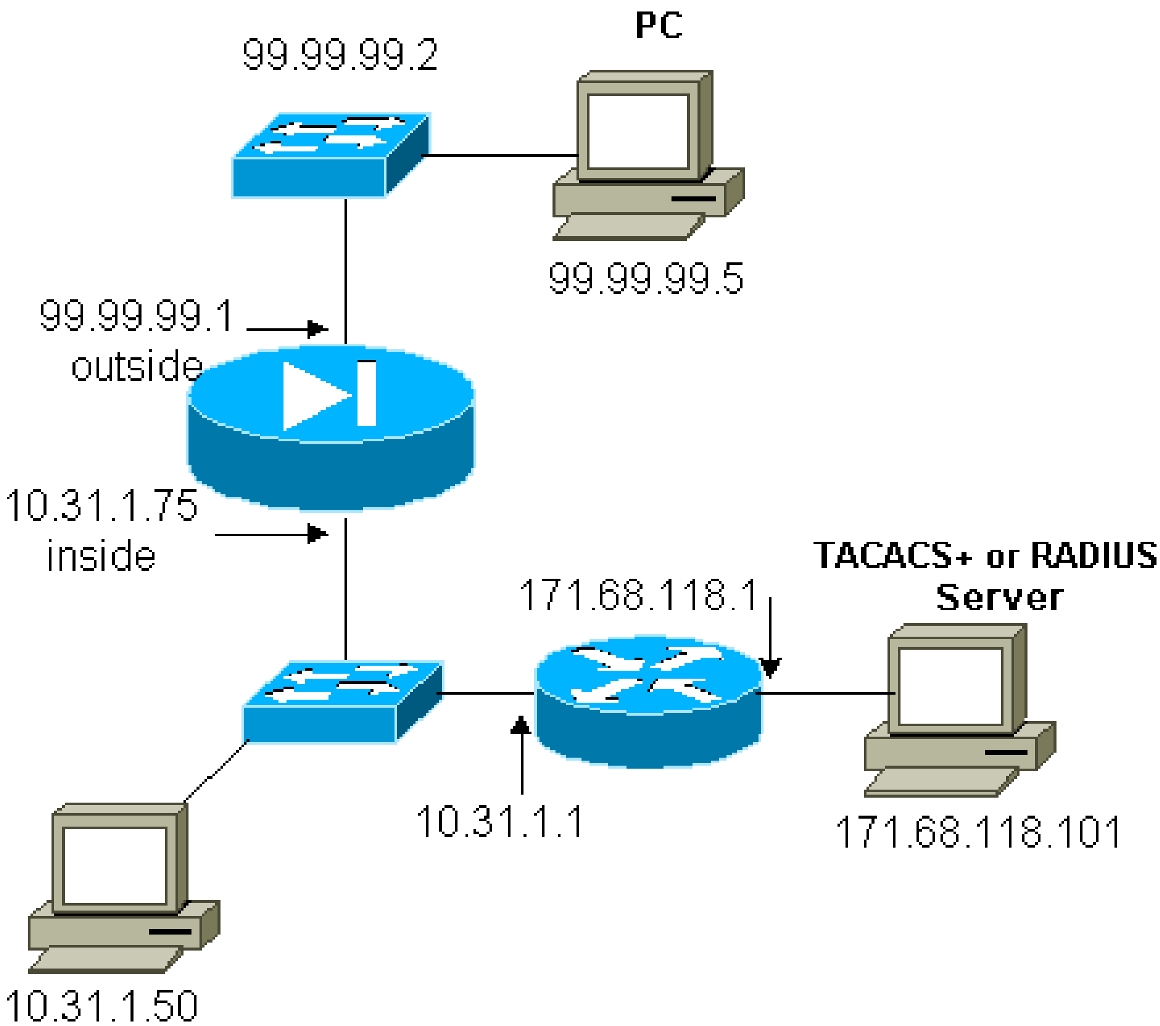
```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

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 .*
}
}
```

디버깅 단계

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

- AAA를 추가하기 전에 PIX 컨피그레이션이 작동하는지 확인합니다.인증 및 권한 부여를 시작하기 전에 트래픽을 전달할 수 없는 경우, 이후에는 트래픽을 전달할 수 없습니다.
- PIX에서 로깅을 활성화합니다.로깅 콘솔 디버깅은 로드가 많은 시스템에서 사용할 수 없습니다.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(모든 서버에 이 옵션이 있음).

네트워크 다이어그램



PIX 컨피그레이션
PIX Version 5.1(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix3 fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25

```
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
```

```
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

PIX의 인증 디버그 예

이 섹션에서는 다양한 시나리오에 대한 인증 디버깅 샘플을 보여줍니다.

인바운드

99.99.99.2의 외부 사용자는 내부 10.31.1.50(99.99.99.99)으로 트래픽을 시작하고 TACACS를 통해 인증됩니다(즉, 인바운드 트래픽은 TACACS 서버 171.68.118.101을 포함하는 서버 목록 "AuthInbound"를 사용합니다).

PIX 디버그 - 양호한 인증 - TACACS+

아래 예는 올바른 인증을 가진 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX 디버그 - 잘못된 인증(사용자 이름 또는 비밀번호) - TACACS+

아래 예는 잘못된 인증(사용자 이름 또는 비밀번호)을 가진 PIX 디버그를 보여줍니다. 사용자는 세 개의 사용자 이름/비밀번호 세트를 확인하고 다음 메시지를 표시합니다.: .

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX 디버그 - Can Ping Server, no Response - TACACS+

아래 예는 서버에서 ping할 수 있지만 PIX와 통신하지 않는 PIX 디버그를 보여줍니다.사용자는 사용자 이름을 한 번 확인하지만 PIX는 비밀번호를 묻지 않습니다(텔넷에 있음). 사용자에게 : .

```
109001: Auth start for user '???' from 99.99.99.2/11011
```

```
    to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
    (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
    (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
    (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
    to 99.99.99.2/11011 on interface outside
```

PIX 디버그 - Ping할 수 없는 서버 - TACACS+

아래 예는 서버에서 ping할 수 없는 PIX 디버그를 보여줍니다.사용자는 사용자 이름을 한 번 확인하지만 PIX는 비밀번호를 묻지 않습니다(텔넷에 있음). 다음 메시지가 표시됩니다.TACACS+ 및 : (구성에서 위조된 서버가 교체됨).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
    99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
    failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
    failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
    failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
    10.31.1.50/23 to 99.99.99.2/11012 on interface
    outside
```

PIX 디버그 - 정상 인증 - RADIUS

아래 예는 올바른 인증을 가진 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from
    10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
    'pixuser' from 10.31.1.50/11008 to
    99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
    99.99.99.2/23 gaddr 99.99.99.99/11008
    laddr 10.31.1.50/11008 (pixuser)
```

PIX 디버그 - 잘못된 인증(사용자 이름 또는 비밀번호) - RADIUS

아래 예는 잘못된 인증(사용자 이름 또는 비밀번호)을 가진 PIX 디버그를 보여줍니다. 사용자는 사용자 이름 및 비밀번호에 대한 요청을 확인하고 이를 입력할 수 있는 세 가지 기회를 갖습니다.항목이 실패하면 다음 메시지가 표시됩니다.: .

```
109001: Auth start for user '???' from 10.31.1.50/11010
    to 99.99.99.2/23
  109006: Authentication failed for user ''
    from 10.31.1.50/11010 to 99.99.99.2/23
    on interface inside
```

PIX 디버그 - 서버에 ping할 수 있음, 데몬 다운 - RADIUS

아래 예는 서버에서 ping할 수 있지만 디먼이 다운되어 PIX와 통신하지 않는 PIX 디버그를 보여줍니다.사용자는 사용자 이름, 비밀번호, RADIUS 메시지 및 : .오류 메시지.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX 디버그 - Ping 서버 또는 키/클라이언트 불일치 - RADIUS

아래 예는 서버에 ping이 불가능하거나 클라이언트/키 불일치가 있는 PIX 디버그를 보여줍니다.사용자는 사용자 이름, 비밀번호, RADIUS 메시지 및 를 . 서버를 교체한 경우의 최대 시도 가 메시지를 초과했습니다.)

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

권한 부여 추가

인증 없이 권한 부여가 유효하지 않으므로 권한 부여를 추가하기로 결정한 경우 동일한 소스 및 대상 범위에 대한 권한 부여가 필요합니다.

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

발신 트래픽은 RADIUS로 인증되고 RADIUS 권한 부여가 유효하지 않기 때문에 발신 권한 부여를 추가하지 않습니다.

PIX의 인증 및 권한 부여 디버그 예

PIX 디버그 - 인증 및 권한 부여 성공 - TACACS+

아래 예는 올바른 인증과 성공적인 권한 부여가 포함된 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX 디버그 - 정상 인증, 권한 부여 실패 - TACACS+

아래 예는 인증 수준이 높지만 권한 부여가 실패한 PIX 디버그를 보여줍니다.이 화면에는 오류 메시지가 .   .

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

계정 추가

TACACS+

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

TACACS+ 프리웨어 출력:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

```
aaa accounting include any outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

성능 RADIUS 출력:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

제외 명령 사용

네트워크에 외부(99.99.99.100)의 다른 호스트를 추가할 때 이 호스트를 신뢰할 수 있는 경우 다음 명령을 사용하여 인증 및 권한 부여에서 해당 호스트를 제외할 수 있습니다.

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
 255.255.255.255 AuthInbound

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

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.연결의 특성 때문에 HTTP에서는 이 기능이 제대로 작동하지 않습니다.다음 예에서는 다른 네트워크 컨피그레이션이 사용되지만 개념이 동일합니다.

PIX를 통해 사용자 텔넷(PIX를 통해 인증):

```
   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 171.68.118.100/12 00 to 9.9.9.25/23
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/23 gaddr 9.9.9.10/12 00
     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 또 다른 연결(다른 PC의 경우)을 시도하고 이 사용자에 대해 서버에서 max-sessions가 **1**로 설정된 경우(서버가 max-sessions를 지원한다고 가정) 서버에서 연결이 거부됩니다.

사용자는 대상 호스트에서 텔넷 또는 FTP 비즈니스를 수행한 다음 종료됩니다(10분 동안 거기서).

```
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 HTTP의 예입니다.

사용자는 PIX를 통해 171.68.118.100에서 9.9.9.25으로 이동합니다.

```
(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 여전히 웹 사이트에 로그인되어 있으며 사용자가 웹 페이지를 읽을 때 연결이 열려 있습니까?아니요. 최대 세션 또는 로그인한 사용자 보기가 여기서 작동합니까?아니요. HTTP의 연결 시간("기본 제공"과 "해체" 사이의 시간)이 너무 짧기 때문입니다.시작 및 중지 레코드가 초 미만입니다.레코드가 사실상 동일한 순간에 발생하므로 중지 레코드가 없는 시작 레코드는 없습니다.uauth가 0 이상으로 설정되었는지 아니면 그 이상으로 설정되었는지에 관계없이 모든 트랜잭션에 대해 서버로 전송되는 시작 및 중지 레코드가 계속 있습니다.그러나 HTTP 연결의 특성 때문에 최대 세션 및 로그인 사용자 보기가 작동하지 않습니다.

PIX 자체에서의 인증 및 활성화

이전 논의에서는 PIX를 통해 텔넷(및 HTTP, FTP) 트래픽을 인증하는 데 문제가 있습니다.PIX에 대한 텔넷이 다음 인증 없이 작동하는지 확인합니다.

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

그런 다음 명령을 추가하여 PIX에 텔넷 사용자를 인증합니다.

```
aaa authentication telnet console AuthInbound
```

사용자가 PIX에 텔넷할 때 텔넷 비밀번호(WW)를 입력하라는 메시지가 표시됩니다. 또한 PIX는 TACACS+ 또는 RADIUS 사용자 이름 및 비밀번호를 요청합니다.이 경우 AuthInbound 서버 목록이 사용되므로 PIX는 TACACS+ 사용자 이름 및 비밀번호를 요청합니다.

서버가 다운된 경우 사용자 이름에 pix를 **입력한** 다음 enable 비밀번호(*무엇이든 **비밀번호 활성화***)를 입력하여 PIX에 액세스할 수 **있습니다.** 명령을 사용하여 다음을 수행합니다.

```
aaa authentication enable console AuthInbound
```

TACACS 또는 RADIUS 서버로 전송되는 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.이 경우 AuthInbound 서버 목록이 사용되므로 PIX는 TACACS+ 사용자 이름 및 비밀번호를 요청합니다.

enable에 대한 인증 패킷은 로그인 인증 패킷과 동일하므로 사용자가 TACACS 또는 RADIUS를 사용하여 PIX에 로그인할 수 있는 경우 동일한 사용자 이름/비밀번호로 TACACS 또는 RADIUS를 통해 활성화할 수 있습니다.이 문제는 Cisco 버그 ID CSCdm47044에 할당되었습니다(등록된 고객만 해당).

서버가 다운된 경우 PIX에서 사용자 이름에 대한 pix와 일반 enable 비밀번호를 입력하여 PIX 활성화 모드에 액세스할 수 있습니다(**비밀번호*에 관계없이* 활성화**). PIX **컨피그레이션에 *없는* 비밀번호**를 활성화하면 사용자 이름에 pix를 입력하고 Enter 키를 **누릅니다**.enable 비밀번호가 설정되어 있지만 알려지지 않은 경우 비밀번호를 재설정하려면 비밀번호 복구 디스크를 빌드해야 합니다.

프롬프트 사용자 변경 참조

명령이 있는 경우

```
auth-prompt PIX_PIX_PIX
```

PIX를 통과하는 사용자는 다음 시퀀스를 볼 수 있습니다.

```
PIX_PIX_PIX [at which point one would enter the username]
   Password:[at which point one would enter the password]
```

최종 목적지에 도착하면 사용자 이름:및 비밀번호:대상 상자에 표시되는 프롬프트이 프롬프트는 PIX*가* 아닌 PIX를 *통과하는* 사용자에게만 영향을 줍니다.

참고: PIX에 액세스하기 위해 잘라낸 회계 레코드가 없습니다.

성공/실패 시 메시지 사용자 정의

명령이 있는 경우

```
auth-prompt accept "GOOD_AUTH"
auth-prompt reject "BAD_AUTH"
```

그러면 사용자는 PIX를 통한 실패/성공 로그인 시 다음 시퀀스를 볼 수 있습니다.

```
PIX_PIX_PIX
   Username: asjdkl
   Password: "BAD_AUTH"
   "PIX_PIX_PIX"
   Username: cse
   Password: "GOOD_AUTH"
```

사용자별 유휴 및 절대 시간 제한

이 기능은 현재 작동하지 않으며 Cisco 버그 ID CSCdp93492에 문제가 할당되었습니다(등록된 고객만 해당).

가상 HTTP

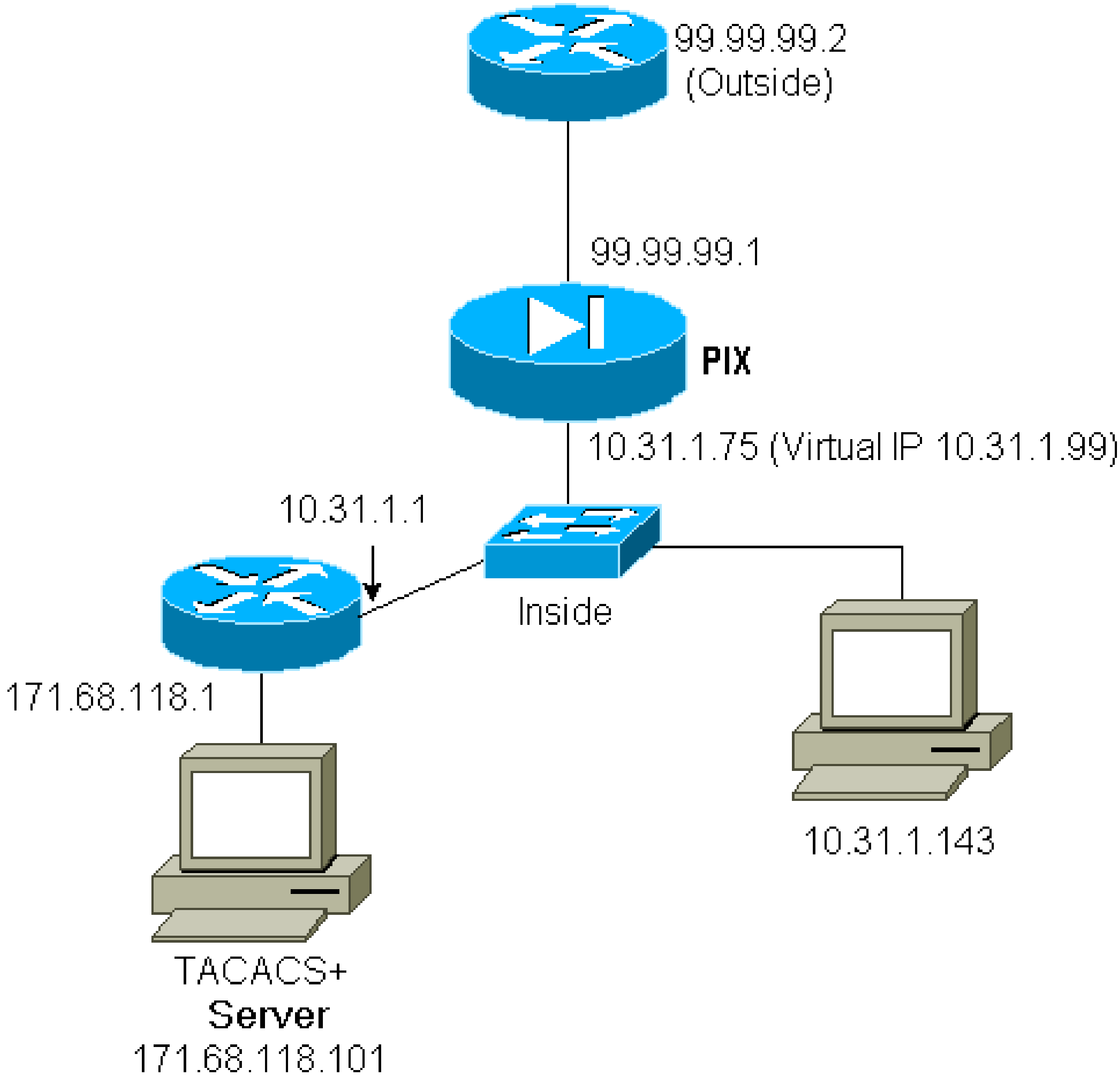
PIX 외부의 사이트나 PIX 자체에서 인증이 필요한 경우 브라우저가 사용자 이름과 비밀번호를 캐시하므로 비정상적인 브라우저 동작이 관찰될 수 있습니다.

이를 방지하려면 다음 명령을 사용하여 RFC 1918 주소(즉, 인터넷에서 라우팅할 수 없지만 PIX 내부 네트워크에 대해 유효하고 고유한 주소)를 PIX 구성에 추가하여 가상 HTTP를 구현할 수 있습니다.

```
virtual http #.#.#.# [warn]
```

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.

가상 HTTP 아웃바운드 예



PIX 컨피그레이션 가상 HTTP 아웃바운드:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

가상 텔넷

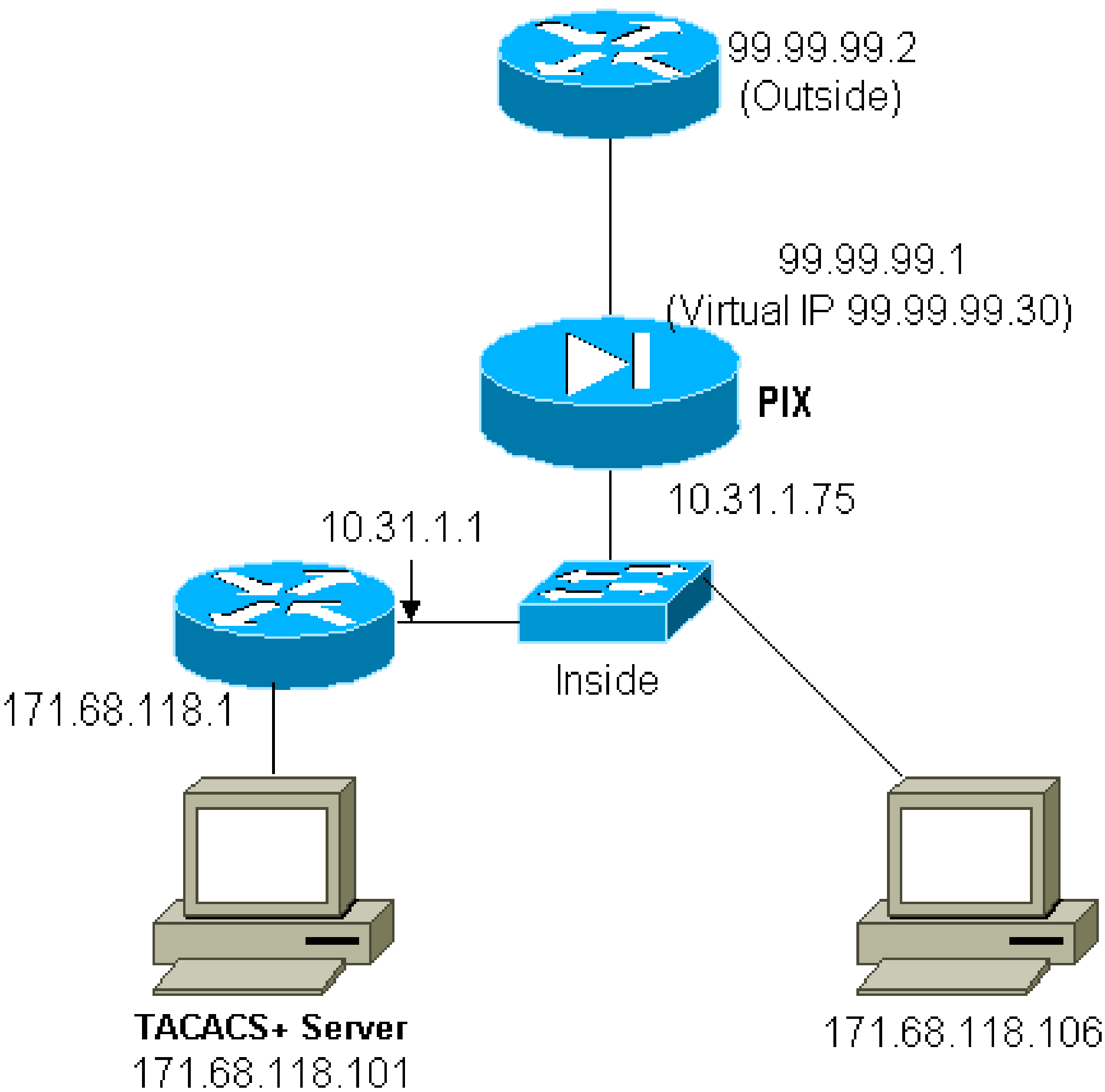
모든 인바운드 및 아웃바운드를 인증하도록 PIX를 구성할 수 있지만, 메일 등의 일부 프로토콜은 쉽게 인증되지 않기 때문에 이는 바람직하지 않습니다.PIX를 통한 모든 트래픽이 인증될 때 메일 서버와 클라이언트가 PIX를 통해 통신을 시도하는 경우 인증되지 않은 프로토콜에 대한 PIX syslog는 다음과 같은 메시지를 표시합니다.

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

그러나 어떤 종류의 특이한 서비스를 인증해야 할 경우 **virtual telnet** 명령을 사용하여 이를 수행할 수 있습니다.이 명령을 사용하면 가상 텔넷 IP 주소에 대한 인증이 발생할 수 있습니다.이 인증 후 비정상적인 서비스에 대한 트래픽은 실제 서버로 이동할 수 있습니다.

이 예에서는 TCP 포트 49 트래픽이 외부 호스트 99.99.99.2에서 내부 호스트 171.68.118.106으로 전달되도록 합니다. 이 트래픽은 실제로 인증될 수 없으므로 가상 텔넷을 설정합니다.가상 텔넷의 경우 연결된 정적이 있어야 합니다.여기서 99.99.99.20 및 171.68.118.20 모두 가상 주소입니다.

가상 텔넷 인바운드



PIX 컨피그레이션 가상 텔넷 인바운드

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
```

```
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

PIX 디버그 가상 텔넷 인바운드

99.99.99.2의 사용자는 먼저 PIX의 99.99.99.20 주소에 텔네팅을 통해 인증해야 합니다.

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

인증에 성공하면 show uauth 명령에 "time on the meter"가 표시됩니다.

```
pixfirewall# show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

그리고 99.99.99.2의 디바이스가 TCP/49 트래픽을 디바이스(171.68.118.106)으로 전송하려고 할 경우

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

권한 부여를 추가할 수 있습니다.

```
aaa authorization include tcp/49 inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

PIX를 통해 TCP/49 트래픽을 시도하면 PIX는 권한 부여 쿼리를 서버로 전송합니다.

```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

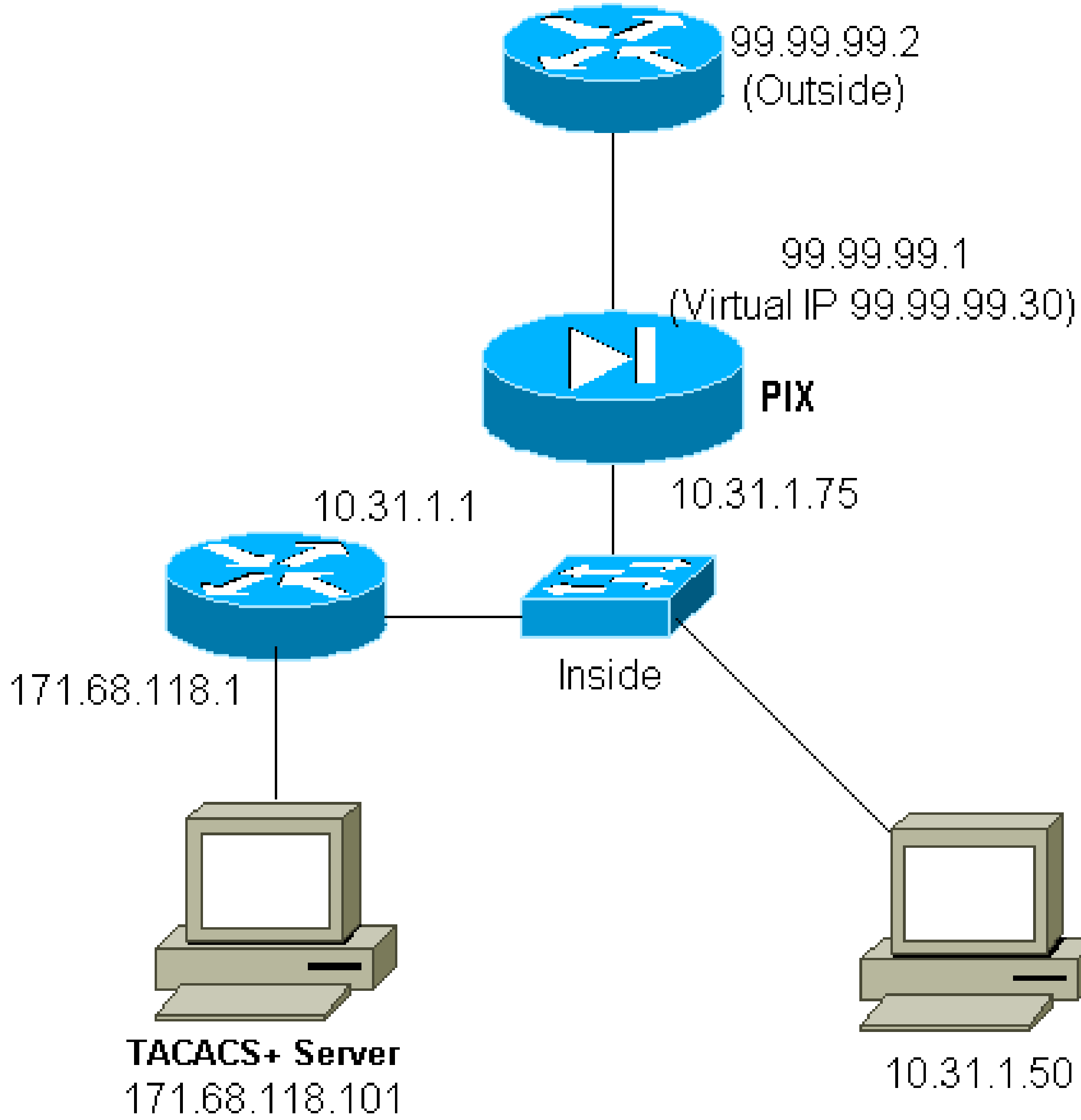
TACACS+ 서버에서는 다음과 같이 표시됩니다.

```
service=shell,
  cmd=tcp/49,
```

```
cmd-arg=171.68.118.106
```

가상 텔넷 아웃바운드

아웃바운드 트래픽은 기본적으로 허용되므로 가상 텔넷 아웃바운드 사용에 고정 트래픽이 필요하지 않습니다.다음 예에서는 Telnet의 내부 사용자10.31.1.50 가상 99.99.99.30을 인증하고 인증합니다.텔넷 연결이 즉시 삭제됩니다.인증되면 TCP 트래픽이 10.31.1.50에서 99.99.99.2의 서버로 허용됩니다.



PIX 컨피그레이션 가상 텔넷 아웃바운드:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

참고: RADIUS이므로 권한 부여가 없습니다.

PIX 디버그 가상 텔넷 아웃바운드:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

가상 텔넷 로그아웃

사용자가 가상 텔넷 IP 주소에 텔넷할 때 **show uauth** 명령은 uauth를 표시합니다.uauth에 시간이 남아 있을 때 세션이 완료된 후 트래픽이 전달되지 않도록 하려면 가상 텔넷 IP 주소에 다시 텔넷해야 합니다.이렇게 하면 세션이 해제됩니다.

첫 번째 인증 후:

```
 pix3# show uauth
                          Current    Most Seen
 Authenticated Users        1          2
 Authen In Progress         0          1
 user 'pixuser' at 10.31.1.50, authenticated
    absolute   timeout: 0:05:00
    inactivity timeout: 0:00:00
 pix3# 109001: Auth start for user 'pixuser' from
    10.31.1.50/11038 to 99.99.99.30/23
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11038 to 99.99.99.30/23 on
    interface inside
```

두 번째 인증 후(즉, 구멍이 닫힌 상태로 전환됨):

```
 pix3# show uauth
                          Current    Most Seen
 Authenticated Users        0          2
 Authen In Progress         0          1
```

포트 권한 부여

포트 범위(예: TCP/30-100)에 대해 권한 부여가 허용됩니다. 가상 텔넷이 PIX에서 구성되고 포트 범위에 대한 권한 부여가 구성된 경우 가상 텔넷으로 구멍이 열리면 PIX는 권한 부여를 위해 TACACS+ 서버**에 tcp/30-100** 명령을 발행합니다.

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

TACACS+ Freeware 서버 구성:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

HTTP, FTP 및 텔넷 이외의 트래픽에 대한 AAA 어카운팅

가상 텔넷이 네트워크 내부의 호스트에 대한 TCP/49 트래픽을 허용하기 위해 작동하는지 확인한 후 이에 대한 어카운팅을 하기로 결정했으므로 다음을 추가했습니다.

```
aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

이렇게 하면 tcp/49 트래픽이 통과할 때 어카운팅 레코드가 잘리게 됩니다(이 예는 TACACS+ 프리웨어의 예).

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

확장 인증(Xauth)

샘플 구성

- Xauth를 사용하여 여러 Cisco Secure PIX 방화벽 인터페이스에서 IPSec 터널 종료
- Cisco Secure PIX Firewall과 확장된 인증을 사용하는 VPN 클라이언트 간 IPSec

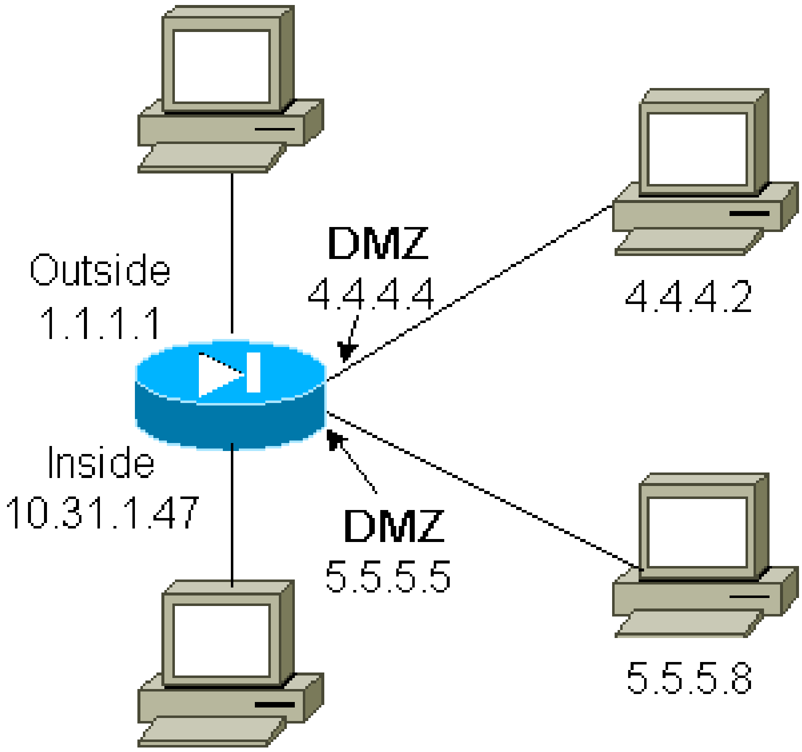
DMZ의 인증

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

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2
```

```
pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

네트워크 다이어그램



PIX 컨피그레이션

pix/intf4와 pix/intf5 간의 텔넷 트래픽을 인증하고자 합니다.

```
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
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Xauth 계정 관리

sysopt **connection permit-ipsec** 명령(sysopt ipsec pl**-compatible** 명령 아님)이 PIX에서 xauth를 사용하여 구성된 경우 어카운팅은 TCP 연결에 유효하지만 ICMP 또는 UDP에는 유효하지 않습니다.

관련 정보

- PIX 제품 지원 페이지
- PIX 명령 참조
- RADIUS 지원 페이지
- RFC(Request for Comments)
- Cisco Secure UNIX 지원 페이지
- Cisco Secure ACS for Windows 지원 페이지
- Technical Support - Cisco Systems