

PIX, TACACS+ 및 RADIUS 샘플 컨피그레이션 :4.4.x

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[인증 대 권한 부여](#)

[인증/권한 부여를 통해 사용자에게 표시되는 내용](#)

[모든 시나리오에 사용되는 보안 서버 구성](#)

[CiscoSecure UNIX TACACS 서버 컨피그레이션](#)

[CiscoSecure UNIX RADIUS 서버 구성](#)

[CiscoSecure NT 2.x RADIUS](#)

[EasyACS TACACS+](#)

[CiscoSecure 2.x TACACS+](#)

[Livingston RADIUS 서버 구성](#)

[Merit RADIUS 서버 구성](#)

[TACACS+ 프리웨어 서버 컨피그레이션](#)

[디버깅 단계](#)

[네트워크 다이어그램](#)

[PIX의 인증 디버그 예](#)

[권한 부여 추가](#)

[PIX의 인증 및 권한 부여 디버그 예](#)

[계정 추가](#)

[TACACS+](#)

[RADIUS](#)

[Except 명령 사용](#)

[최대 세션 수 및 로그인한 사용자 보기](#)

[PIX 자체에서의 인증 및 활성화](#)

[직렬 콘솔 인증](#)

[프롬프트 사용자 변경 참조](#)

[성공/실패 시 메시지 사용자 정의](#)

[사용자별 유효 및 절대 시간 제한](#)

[가상 HTTP](#)

[가상 텔넷](#)

[가상 텔넷 로그아웃](#)

[포트 권한 부여](#)

[관련 정보](#)

소개

FTP, 텔넷 및 HTTP 연결에 대해 RADIUS 및 TACACS+ 인증을 수행할 수 있습니다. 일반적으로 다른 덜 일반적인 TCP 프로토콜에 대한 인증은 작동하도록 할 수 있습니다.

TACACS+ 권한 부여가 지원됩니다. RADIUS 권한 부여가 아닙니다. 이전 버전에 대한 PIX 4.4.1 인증, 권한 부여 및 계정 관리(AAA)의 변경 사항은 다음과 같습니다. AAA 서버 그룹 및 장애 조치, 활성화 및 직렬 콘솔 액세스를 위한 인증, 프롬프트 메시지를 수락 및 거부합니다.

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 규칙에 대한 자세한 내용은 [Cisco 기술 팀 표기 규칙](#)을 참조하십시오.

인증 대 권한 부여

- 인증은 사용자의 이름입니다.
- 권한 부여는 사용자가 수행할 수 있는 작업입니다.
- 권한 부여 없이 인증이 유효합니다.
- 인증 없이 권한 부여가 유효하지 않습니다.

사용자 100명이 안에 있고 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 6개의 사용자 ID를 모두 제공합니다. 간단한 인증으로 이 6명의 사용자는 사용자 이름과 비밀번호를 사용하여 인증한 다음 로그아웃할 수 있습니다. 나머지 94명의 사용자는 나갈 수 없습니다. 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 세 사용자 중 "Terry"를 신뢰할 수 없다고 가정해 보겠습니다. Terry가 FTP를 수행하도록 허용하되 HTTP나 텔넷을 외부에 허용하지 않습니다. 이는 권한 부여를 추가해야 한다는 것을 의미합니다. 즉, 사용자가 자신이 누구인지를 인증하는 것 외에도 권한을 부여할 수 있습니다. PIX에 권한 부여를 추가할 때 PIX는 먼저 Terry의 사용자 이름과 비밀번호를 보안 서버에 보낸 다음 Terry가 하려고 하는 "명령"을 보안 서버에 알리는 권한 부여 요청을 보냅니다. 서버가 제대로 설정되면 Terry는 "FTP 1.2.3.4"를 허용받을 수 있지만, HTTP 또는 텔넷 기능을 어디서든 거부합니다.

인증/권한 부여를 통해 사용자에게 표시되는 내용

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

- **텔넷** - 사용자 이름 프롬프트가 표시되고 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 전송하고 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 초과로 표시되지 않는 경우, 브라우저가 캐시된 사용자 이름 및 비밀번호를 PIX로 "슈팅(sho팅)"하고 재인증이 이루어지며 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.

모든 시나리오에 사용되는 보안 서버 구성

CiscoSecure UNIX TACACS 서버 컨피그레이션

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 .*
}
}
}

```

CiscoSecure UNIX RADIUS 서버 구성

고급 GUI(그래픽 사용자 인터페이스)를 사용하여 PIX IP 및 키를 NAS(Network Access Server) 목록에 추가합니다.

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

CiscoSecure NT 2.x RADIUS

다음 단계를 완료합니다.

1. User Setup GUI 섹션에서 비밀번호를 가져옵니다.
2. Group Setup GUI 섹션에서 특성 6(Service-Type)을 Login 또는 Administrative로 설정합니다.
3. NAS 구성 GUI에서 PIX IP를 추가합니다.

EasyACS TACACS+

EasyACS 설명서에서는 설정에 대해 설명합니다.

1. 그룹 섹션에서 **Shell exec**(exec 권한 부여)을 클릭합니다.
2. PIX에 권한 부여를 추가하려면 그룹 설정 하단의 **Deny unmatched IOS 명령**을 클릭합니다.
3. 허용할 각 명령(예: 텔넷)에 대해 **Add/Edit new** 명령을 선택합니다.
4. 텔넷을 특정 사이트에 허용하려면 "permit #.#.##" 형식의 인수 섹션에 IP를 입력합니다. 모든 사이트에 텔넷을 허용하려면 목록에 없는 **모든 인수 허용** 을 클릭합니다.
5. 편집 **완료 명령**을 클릭합니다.
6. 허용되는 각 명령(예: 텔넷, HTTP 및/또는 FTP)에 대해 1~5단계를 수행합니다.
7. NAS Configuration GUI 섹션에서 PIX IP를 추가합니다.

CiscoSecure 2.x TACACS+

사용자는 GUI의 사용자 설정 섹션에서 비밀번호를 연습니다.

1. 그룹 섹션에서 **Shell exec**(exec 권한 부여)을 클릭합니다.
2. PIX에 권한 부여를 추가하려면 그룹 설정 하단의 **Deny unmatched IOS 명령**을 클릭합니다.
3. 허용할 각 명령(예: 텔넷)에 대해 **Add/Edit**를 선택합니다.
4. 텔넷을 특정 사이트에 허용하려면 인수 사각형(예: "permit 1.2.3.4")에 permit IP를 입력합니다 . 모든 사이트에 텔넷을 허용하려면 목록에 없는 **모든 인수 허용** 을 클릭합니다.
5. 편집 **완료 명령**을 클릭합니다.
6. 허용되는 각 명령(예: 텔넷, HTTP 또는 FTP)에 대해 1~5단계를 수행합니다.
7. NAS Configuration GUI 섹션에서 PIX IP를 추가합니다.

Livingston RADIUS 서버 구성

PIX IP 및 키를 클라이언트 파일에 추가합니다.

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

Merit RADIUS 서버 구성

PIX IP 및 키를 클라이언트 파일에 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

- AAA(Authentication, Authorization, and Accounting)를 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. **logging console 디버깅 명령**은 로드가 많은 시스템에서 사용할 수 없습니다. **logging buffered 디버깅 명령**을 사용할 수 있습니다. **show logging** 또는 **logging** 명령의 출력을 syslog 서버로 전송하고 검사할 수 있습니다.
- TACACS+ 또는 RADIUS 서버에 대한 디버깅이 켜져 있는지 확인합니다. 모든 서버에 이 옵션이 있습니다.

네트워크 다이어그램

Outside:



11.11.11.15



11.11.11.15



10.31.1.150

Inside:

10.31.1.1



10.31.1.5

171.68.118.1

171.68.118.101

171.68.118.115



Tacacs Server



Radius Server

PIX 컨피그레이션

```
pix-5# write terminal
Building configuration...
: Saved
:
PIX Version 4.4(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
nameif ethernet3 pix/intf3 security15
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-5
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
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
mtu pix/intf3 1500
ip address outside 11.11.11.1 255.255.255.0
ip address inside 10.31.1.150 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255
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
failover ip address pix/intf3 0.0.0.0
arp timeout 14400
global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip pix/intf2 passive
no rip pix/intf2 default
no rip pix/intf3 passive
no rip pix/intf3 default
route inside 0.0.0.0 0.0.0.0 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 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

PIX의 인증 디버그 예

다음 디버그 예에서는 다음을 수행합니다.

아웃바운드

10.31.1.5의 내부 사용자는 외부 11.11.11.15에 대한 트래픽을 시작하고 TACACS+를 통해 인증됩니다(아웃바운드 트래픽은 TACACS 서버 171.68.118.101을 포함하는 서버 목록 "Outgoing"을 사용합니다).

인바운드

11.11.11.15의 외부 사용자는 내부 10.31.1.5(11.11.11.22)에 대한 트래픽을 시작하고 RADIUS를 통해 인증됩니다(인바운드 트래픽은 RADIUS 서버 171.68.118.115을 포함하는 서버 목록 "Incoming"을 사용합니다).

PIX 디버그 - 양호한 인증 - TACACS+

아래 예는 올바른 인증으로 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
109011: Authen Session Start: user 'ddunlap', sid 3
109005: Authentication succeeded for user 'ddunlap'
from 10.31.1.5/11004 to 11.11.11.15/23
109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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

아래 예는 잘못된 인증(사용자 이름 또는 비밀번호)을 사용하는 PIX 디버그를 보여줍니다. 사용자에게 네 개의 사용자 이름/비밀번호 세트가 표시됩니다.다음 메시지가 표시됩니다."오류:최대 시도 횟수 초과"

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX 디버그 - Ping할 수 있지만 응답 없음 - TACACS+

아래 예는 PIX와 통신하지 않는 ping 가능 서버에 대한 PIX 디버그를 보여줍니다.사용자는 사용자 이름을 한 번 보고 PIX는 비밀번호를 묻지 않습니다(텔넷에 있음).


```
'Error: Max number of tries exceeded'
109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
(server 171.68.118.101 failed)
109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

PIX 디버그 - 서버에 ping할 수 없음 - TACACS+

아래 예는 ping할 수 없는 서버에 대한 PIX 디버그를 보여줍니다.사용자는 사용자 이름을 한 번 확인합니다.PIX는 비밀번호를 묻지 않습니다(텔넷에 있음). 다음 메시지가 표시됩니다."TACACS+ 서버에 대한 시간 초과" 및 "오류:최대 시도 횟수 초과됨"(이 예의 컨피그레이션은 가짜 서버를 반영함)

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
(server 171.68.118.199 failed)
109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

PIX 디버그 - 정상 인증 - RADIUS

아래 예는 올바른 인증과 함께 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
109011: Authen Session Start: user 'adminuser', sid 4
109005: Authentication succeeded for user 'adminuser'
from 10.31.1.5/23 to 11.11.11.15/11003
109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
302001: Built inbound TCP connection 5 for faddr
11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

아래 예는 잘못된 인증(사용자 이름 또는 비밀번호)을 사용하는 PIX 디버그를 보여줍니다. 사용자 이름 및 비밀번호에 대한 요청이 표시됩니다.둘 중 하나가 잘못되면 "잘못된 암호"라는 메시지가 네 번 표시됩니다.그러면 사용자의 연결이 끊어집니다.이 문제에 버그 ID #CSCdm46934이 할당되었습니다.

```
'Error: Max number of tries exceeded'
109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

PIX 디버그 - 디먼 다운, PIX - RADIUS와 통신하지 않음

아래 예는 ping할 수 있는 서버가 있는 PIX 디버그를 보여주지만 디먼이 다운되었습니다.서버가 PIX와 통신하지 않습니다.사용자는 사용자 이름 다음에 비밀번호가 표시됩니다.다음 메시지가 표시됩니다."RADIUS 서버 실패" 및 "오류:최대 시도 횟수 초과"입니다.

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

PIX 디버그 - 서버 또는 키/클라이언트 불일치 ping할 수 없음 - RADIUS

아래 예는 ping할 수 없는 서버 또는 키/클라이언트 불일치가 있는 서버의 PIX 디버그를 보여줍니다. 사용자는 사용자 이름과 비밀번호를 확인합니다. 다음 메시지가 표시됩니다. "RADIUS 서버에 대한 시간 초과" 및 "오류: 최대 시도 횟수 초과됨"(컨피그레이션의 서버는 예시용으로만 사용됩니다).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

권한 부여 추가

인증 없이 권한 부여가 유효하지 않으므로 동일한 소스 및 대상 범위에 대한 권한 부여가 필요합니다.

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

발송

수신 트래픽이 RADIUS로 인증되고 RADIUS 권한 부여가 유효하지 않으므로 "수신"에 대한 권한 부여를 추가하지 않습니다

PIX의 인증 및 권한 부여 디버그 예

PIX 디버그(인증 및 권한 부여 성공) - TACACS+

아래 예는 올바른 인증 및 성공적인 권한 부여와 함께 PIX 디버그를 보여줍니다.

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
109005: Authentication succeeded for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
```

```
109007: Authorization permitted for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109012: Authen Session End: user 'can_only_do_telnet', sid 7,
elapsed 1 seconds
302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX 디버그 - 정상 인증, 권한 부여 실패 - TACACS+

아래 예는 인증 수준이 높지만 권한 부여가 실패한 PIX 디버그를 보여줍니다.

이 화면에서는 "오류:권한 부여 거부됨"

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_ftp', sid 5
109005: Authentication succeeded for user 'can_only_do_ftp'
from 10.31.1.5/11000 to 11.11.11.15/23
109008: Authorization denied for user 'can_only_do_ftp' from
10.31.1.5/11000 to 11.11.11.15/23
109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

계정 추가

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Debug는 계정 관리 설정 또는 해제 여부와 상관없이 동일하게 표시됩니다.그러나 "기본 제공"일 때 "시작" 회계 레코드가 전송됩니다."해체" 당시, "중지" 회계 기록이 전송될 것입니다.

TACACS+ 어카운팅 레코드는 다음과 같습니다(CiscoSecure UNIX에서 가져온 레코드 ,CiscoSecure NT에 있는 항목은 대신 쉼표로 구분될 수 있습니다.)

```
Thu Jun 3 10:41:50 1999 10.31.1.150 can_only_do_telnet
PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet
Thu Jun 3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

Debug는 계정 관리 설정 또는 해제 여부와 상관없이 동일하게 표시됩니다.그러나 "Built(기본 제공)"일 때 "시작" 회계 레코드가 전송됩니다."Teardown" 시 "stop" 회계 기록이 전송됩니다.

RADIUS 계정 관리 레코드는 다음과 같습니다.(이는 CiscoSecure UNIX에서 가져온 것입니다 .CiscoSecure NT에 있는 항목은 대신 쉼표로 구분될 수 있습니다.)

```

10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
Thu Jun  3 15:53:11 1999
    Acct-Status-Type = Start
    Client-Id = 10.31.1.150
    Login-Host = 10.31.1.5
    Login-TCP-Port = 23
    Acct-Session-Id = "0x00000008"
    User-Name = "adminuser"
10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
Thu Jun  3 15:54:24 1999
    Acct-Status-Type = Stop
    Client-Id = 10.31.1.150
    Login-Host = 10.31.1.5
    Login-TCP-Port = 23
    Acct-Session-Id = "0x00000008"
    User-Name = "adminuser"
    Acct-Session-Time = 73
    Acct-Input-Octets = 27
    Acct-Output-Octets = 73

```

Except 명령 사용

네트워크에서 특정 소스 및/또는 대상에 인증, 권한 부여 또는 어카운팅이 필요하지 않다고 판단하면 다음과 같은 작업을 수행할 수 있습니다.

```

aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing

```

인증에서 IP 주소를 "예외"하고 권한 부여가 설정된 경우 권한 부여에서 IP 주소를 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. 어카운팅 "시작" 레코드가 생성되었지만 "중지" 레코드가 없는 경우 TACACS+ 또는 RADIUS 서버는 해당 사용자가 아직 로그인되어 있다고 가정합니다(즉, PIX를 통한 세션이 있는 경우).

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.

사용자는 PIX를 통해 텔넷하고 이동 중에 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
171.68.118.100/12 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(현재) 서버에 "텔넷" 사용자가 로그인되어 있음을 표시합니다. 사용자가 인증을 필요로 하는 다른 연결(아마도 다른 PC의 연결)을 시도하고 이 사용자에게 대해 서버에서 max-sessions가 "1"로 설정된 경우(서버가 max-sessions를 지원하지는 것으로 가정) 서버에서 연결이 거부됩니다.

사용자는 대상 호스트에서 텔넷 또는 FTP 비즈니스를 계속 수행한 다음 종료됩니다(여기서 10분 소요).

```
(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(매번 인증) 또는 그 이상(uauth 기간 동안 한 번 인증하고 다시 인증하지 않음)인지 여부는 액세스한 모든 사이트에 대해 계정 레코드가 잘립니다.

그러나 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 게시되었으며 중지 레코드는 16:35:35에 게시되었습니다. 이 다운로드에는 1초(즉, 시작 레코드와 중지 레코드 사이에 1초 미만이 있었습니다. 사용자가 여전히 웹 사이트에 로그인되어 있으며 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."start" 및 "stop" 레코드는 초 미만의 것입니다."중지" 기록이 없는 "시작" 레코드는 거의 동일한 순간에 발생하므로 없습니다.uauth가 0으로 설정되었든 그보다 큰 것으로 설정되었든 모든 트랜잭션에 대해 서버로 전송된 "시작" 및 "중지" 레코드가 계속 있습니다.그러나 HTTP 연결의 특성 때문에 최대 세션 및 로그인 사용자 보기가 작동하지 않습니다.

[PIX 자체에서의 인증 및 활성화](#)

이전의 논의에서는 PIX를 통해 텔넷(및 HTTP, FTP) 트래픽을 인증하는 것이었습니다.아래 예에서

는 pix에 대한 텔넷이 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 Outgoing
```

사용자가 PIX에 텔넷하면 텔넷 비밀번호("ww")를 입력하라는 프롬프트가 표시됩니다. PIX는 이 경우("발신" 서버 목록이 사용되기 때문) 또는 RADIUS 사용자 이름 및 비밀번호를 요청합니다.

```
aaa authentication enable console Outgoing
```

이 명령을 사용하면 TACACS 또는 RADIUS 서버로 전송되는 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 이 경우 "Outgoing(발신)" 서버 목록이 사용되므로 요청이 TACACS 서버로 이동합니다. enable에 대한 인증 패킷은 로그인 인증 패킷과 동일하므로 사용자는 TACACS 또는 RADIUS를 통해 TACACS 또는 RADIUS를 사용하여 PIX에 로그인할 수 있다고 가정합니다. 이 문제에 버그 ID #CSCdm47044이 할당되었습니다.

서버가 다운된 경우 사용자는 사용자 이름에 "PIX"를 입력하고 PIX에서 일반 enable 비밀번호 ("enable password anything")를 입력하여 PIX 활성화 모드에 액세스할 수 있습니다. PIX 컨피그레이션에 "enable password anything"이 없는 경우 사용자는 사용자 이름에 "PIX"를 입력하고 Enter 키를 눌러야 합니다. enable 비밀번호가 설정되어 있지만 알 수 없는 경우 재설정하려면 비밀번호 복구 디스크가 필요합니다.

직렬 콘솔 인증

PIX의 직렬 콘솔에 액세스하려면 aaa authentication serial console 명령을 사용하려면 인증 확인이 필요합니다. 사용자가 콘솔에서 컨피그레이션 명령을 수행하면 syslog 메시지가 잘립니다(PIX가 디버그 레벨에서 syslog를 syslog 호스트로 전송하도록 구성된 경우). 다음은 syslog 서버의 예입니다.

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed the 'hostname' command.
```

프롬프트 사용자 변경 참조

명령이 있는 경우

```
auth-prompt THIS_IS_PIX_5
```

PIX를 통과하는 사용자는 다음 시퀀스를 볼 수 있습니다.

```
THIS_IS_PIX_5 [at which point one would enter the username]
```

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

그런 다음 최종 목적지 상자에 도착하면 "Username:" 및 "Password:"를 클릭하면 목적지 상자가 표시됩니다.

이 프롬프트는 PIX가 아닌 PIX를 통과하는 사용자에게만 영향을 미칩니다.

참고: PIX에 액세스하기 위해 잘라낸 회계 레코드가 없습니다.

성공/실패 시 메시지 사용자 정의

명령이 있는 경우

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

사용자는 PIX를 통한 로그인 실패/성공 시 다음을 볼 수 있습니다.

```
THIS_IS_PIX_5
Username: asjdkl
Password:
"You blew it"
"THIS_IS_PIX_5"
Username: cse
Password:
"You're allowed through the pix"
```

사용자별 유휴 및 절대 시간 제한

유휴 및 절대 uauth 시간 제한은 사용자별로 TACACS+ 서버에서 전송될 수 있습니다.네트워크의 모든 사용자가 동일한 "timeout uauth"를 가질 경우 이를 구현하지 마십시오!그러나 사용자별로 다른 uauths가 필요한 경우 계속 읽으십시오.

PIX의 예에서는 timeout uauth **3:00:00** 명령을 사용합니다.이는 한 사람이 인증을 받으면 3시간 동안 재인증할 필요가 없다는 것을 의미합니다.그러나 다음 프로파일을 사용하여 사용자를 설정하고 PIX에서 TACACS AAA 권한 부여가 설정된 경우 사용자 프로필의 유휴 및 절대 시간 초과는 해당 사용자에게 대한 PIX의 시간 제한 uauth를 재정의합니다.이는 유휴/절대 시간 제한 후 PIX를 통한 텔넷 세션의 연결이 끊긴다는 것을 의미하지는 않습니다.재인증 발생 여부를 제어할 수 있습니다.

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

인증 후 PIX에서 **show uauth** 명령을 실행합니다.

```
pix-5# show uauth
```

```
Current      Most Seen
```

```
Authenticated Users      1          1
Authen In Progress      0          1
user 'timeout' at 10.31.1.5, authorized to:
  port 11.11.11.15/telnet
  absolute timeout: 0:02:00
  inactivity timeout: 0:01:00
```

사용자가 1분 동안 유휴 상태로 있으면 PIX의 디버그가 표시됩니다.

```
109012: Authen Session End: user 'timeout', sid 19, elapsed 91 seconds
```

사용자는 동일한 대상 호스트 또는 다른 호스트로 돌아갈 때 다시 인증해야 합니다.

가상 HTTP

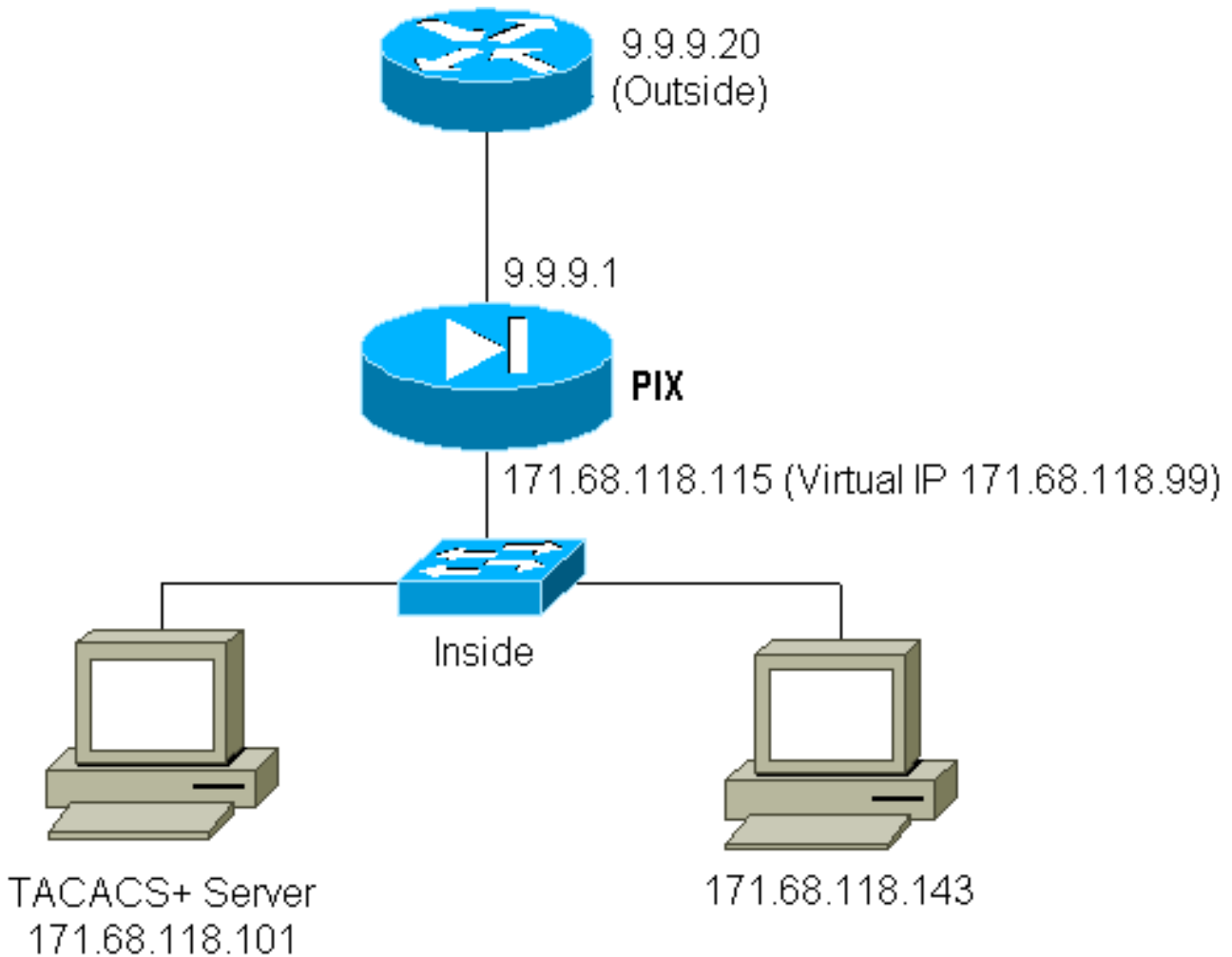
PIX 외부의 사이트와 PIX 자체에서 인증이 필요한 경우 브라우저가 사용자 이름과 비밀번호를 캐시하므로 비정상적인 브라우저 동작이 관찰될 수 있습니다.

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 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 01:00:00
aaa-server TACACS+ protocol tacacs+
aaa-server Outgoing protocol tacacs+
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual http 171.68.118.99
auth-prompt THIS_IS_PIX_5
```

가상 텔넷

모든 인바운드 및 아웃바운드 트래픽을 인증하도록 PIX를 구성하는 것은 바람직하지 않습니다. "mail"과 같은 일부 프로토콜은 쉽게 인증되지 않기 때문입니다. PIX를 통한 모든 트래픽이 인증될 때 메일 서버 및 클라이언트가 PIX를 통해 통신을 시도하는 경우 인증되지 않은 프로토콜에 대한 PIX syslog에 다음과 같은 메시지가 표시됩니다.

```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated)
```

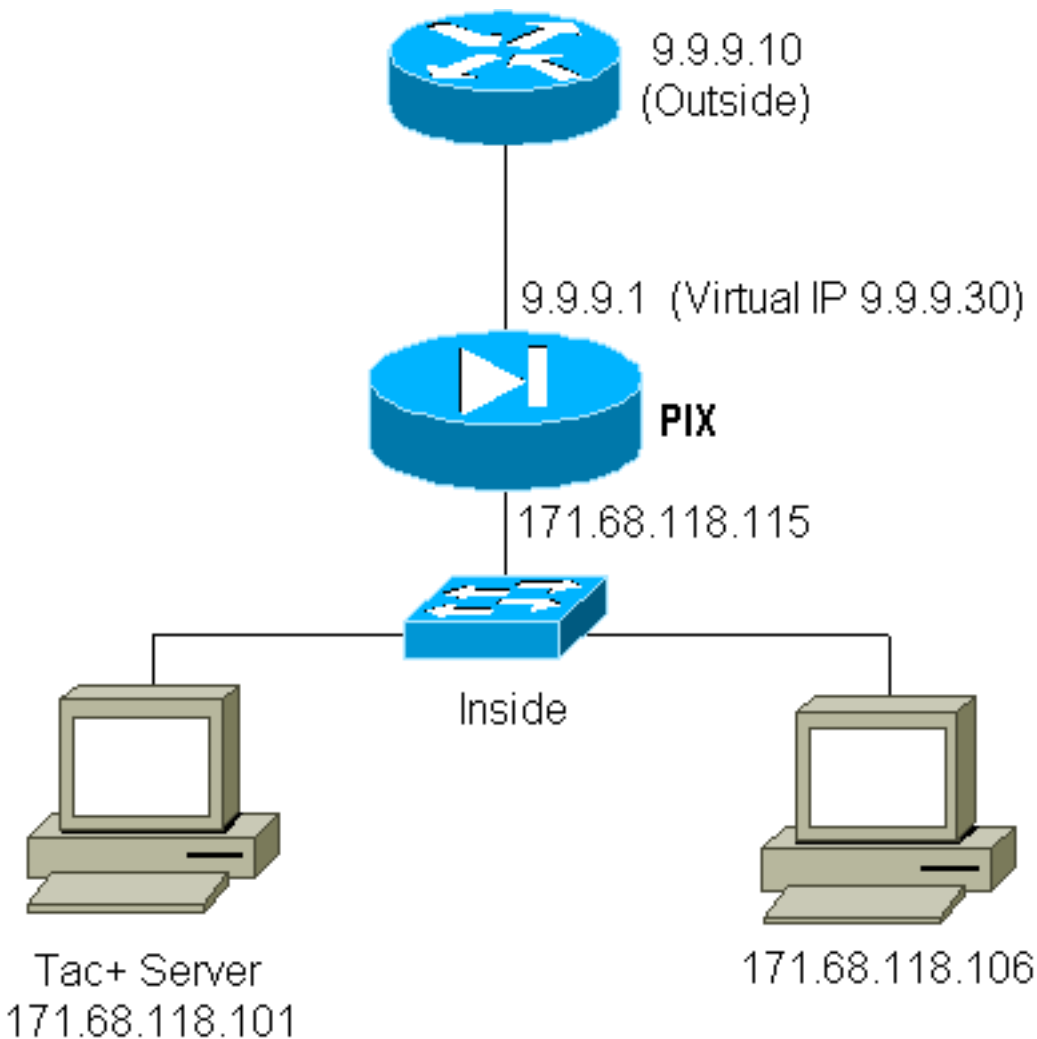
메일 및 일부 기타 서비스는 인증하기에 충분한 인터랙티브 방식이 아니므로 한 솔루션은 인증/권한 부여를 위해 **except** 명령을 사용합니다(메일 서버/클라이언트의 소스/목적지를 제외한 모두 인

중).

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

이 예에서는 TCP 포트 49 트래픽이 외부 호스트 9.9.9.10에서 내부 호스트 171.68.118.106으로 이동할 수 있도록 허용하려고 합니다. 이 트래픽은 실제로 인증될 수 없으므로 가상 텔넷을 설정합니다.

가상 텔넷 인바운드:



PIX 컨피그레이션 가상 텔넷 인바운드:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 9.9.9.30 host 9.9.9.10
aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
virtual telnet 9.9.9.30
```

TACACS+ 서버 사용자 구성 가상 텔넷 인바운드:

```
user = pinecone {
default service = permit
    login = cleartext "pinecone"
service = exec {
    timeout = 10
    idletime = 10
    }
}
```

PIX 디버그 가상 텔넷 인바운드:

9.9.9.10의 사용자는 먼저 PIX의 9.9.9.30 주소에 텔네팅을 통해 인증해야 합니다.

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
to 171.68.118.106/23
109011: Authen Session Start: user 'pinecone', sid 13
109005: Authentication succeeded for user 'pinecone' from
171.68.118.106/23 to 9.9.9.10/11099
```

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

```
pixfirewall# show uauth
Current      Most Seen
Authenticated Users      1          1
Authen In Progress       0          1
user 'pinecone' at 9.9.9.10, authenticated
    absolute timeout: 0:10:00
    inactivity timeout: 0:10:00
```

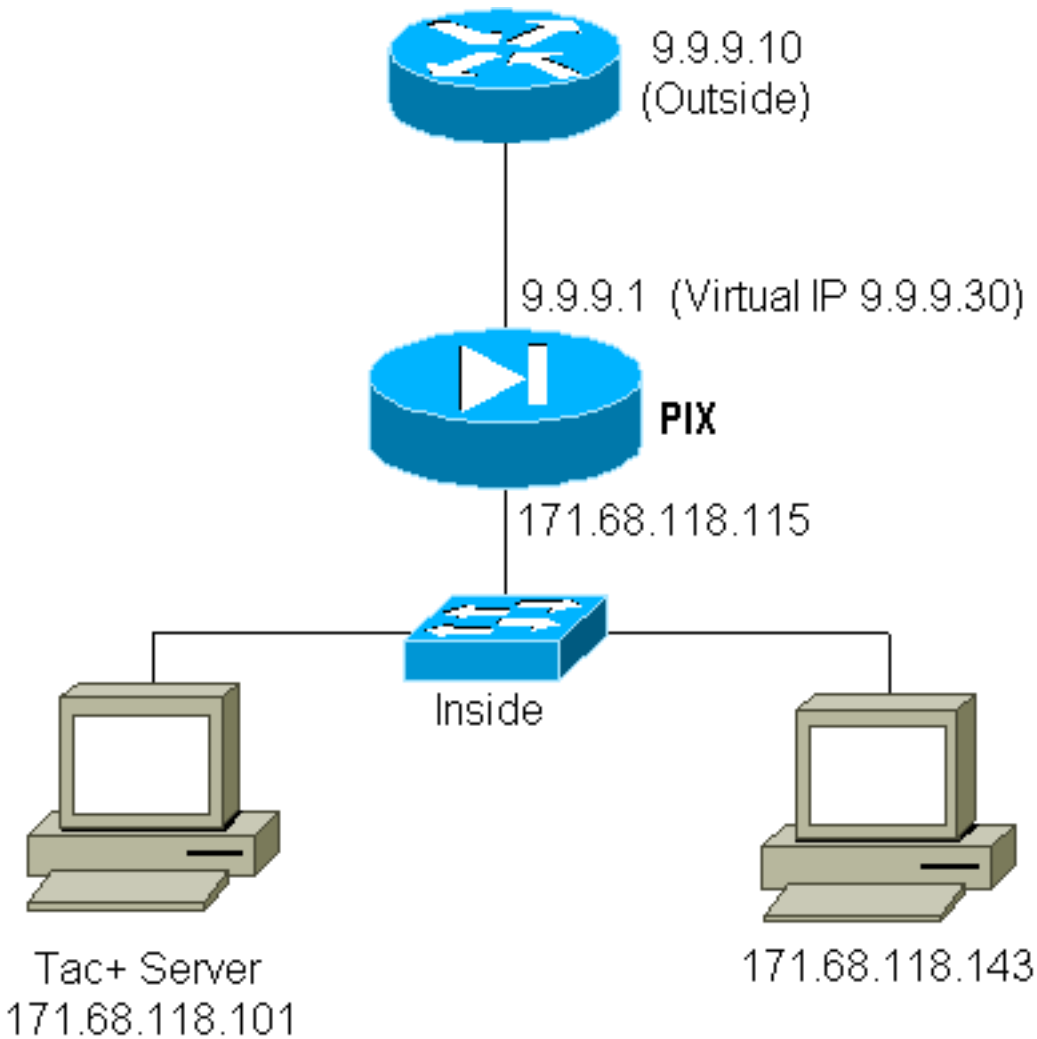
그리고 9.9.9.10의 디바이스가 TCP/49 트래픽을 디바이스(171.68.118.106)으로 전송하려고 할 경우

```
pixfirewall# 109001: Auth start for user 'pinecone'
from 9.9.9.10/11104 to 171.68.118.106/49
109011: Authen Session Start: user 'pinecone', sid 14
109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
to 171.68.118.106/49
302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr
9.9.9.30/49 laddr 171.68.118.106/49 (pinecone)
302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

가상 텔넷 아웃바운드:

아웃바운드 트래픽은 기본적으로 허용되므로 가상 텔넷 아웃바운드 사용에 고정 트래픽이 필요하지 않습니다. 다음 예에서 171.68.118.143의 내부 사용자는 텔넷으로 가상 9.9.9.30에 연결하고 인증합니다. 텔넷 연결이 즉시 삭제됩니다.

인증되면 TCP 트래픽이 171.68.118.143에서 9.9.9.10의 서버로 허용됩니다.



PIX 컨피그레이션 가상 텔넷 아웃바운드:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 00:05:00
aaa-server TACACS+ protocol tacacs+
aaa-server Outgoing protocol tacacs+
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual telnet 9.9.9.30
```

PIX 디버그 가상 텔넷 아웃바운드:

```
109001: Auth start for user '???' from 171.68.118.143/1536 to 9.9.9.30/23
109011: Authen Session Start: user 'timeout_143', sid 25
109005: Authentication succeeded for user 'timeout_143' from
171.68.118.143/1536 to 9.9.9.30/23
302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
laddr 171.68 .118.143/1537 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
laddr 171.68 .118.143/1538 (timeout_143)
302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
laddr 171.68. 118.143/1537 duration 0:00:03 bytes 625 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
```

```
laddr 171.68. 118.143/1538 duration 0:00:01 bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

가상 텔넷 로그아웃

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

포트 권한 부여

포트 범위에 대한 권한 부여가 필요할 수 있습니다. 다음 예에서는 모든 아웃바운드에 대해 인증이 여전히 필요했지만 TCP 포트 23-49에 대해서만 권한 부여가 필요합니다.

PIX 구성:

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

따라서 텔넷 포트 23이 23-49 범위에 있기 때문에 텔넷에서 171.68.118.143에서 9.9.9.10까지 인증 및 권한 부여가 발생했습니다. HTTP 세션을 171.68.118.143에서 9.9.9.10으로 진행하는 경우 여전히 인증해야 하지만 80이 23-49 범위에 있지 않으므로 PIX는 TACACS+ 서버에 HTTP를 승인하도록 요청하지 않습니다.

TACACS+ 프리웨어 서버 컨피그레이션

```
user = telnetrange {
    login = cleartext "telnetrange"
    cmd = tcp/23-49 {
        permit 9.9.9.10
    }
}
```

PIX는 TACACS+ 서버에 "cmd=tcp/23-49" 및 "cmd-arg=9.9.9.10"을 보냅니다.

PIX에서 디버그:

```
109001: Auth start for user '???' from 171.68.118.143/1051 to 9.9.9.10/23
109011: Authen Session Start: user 'telnetrange', sid 0
109005: Authentication succeeded for user 'telnetrange' from
171.68.118.143/1051 to 9.9.9.10/23
109011: Authen Session Start: user 'telnetrange', sid 0
109007: Authorization permitted for user 'telnetrange' from
171.68.118.143/1051 to 9.9.9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23 gaddr 9.9.9.5/1051
laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105 to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110 to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', sid 1
109005: Authentication succeeded for user 'telnetrange' from
171.68.118.143/1110 to 9.9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
laddr 171.68.1 18.143/1110 (telnetrange)
```

```
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111  
laddr 171.68.1 18.143/1111 (telnetrange)  
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110  
laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)  
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/  
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 laddr  
171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

관련 정보

- [Cisco PIX 방화벽 소프트웨어 제품 지원](#)
- [Cisco Secure PIX Firewall 명령 참조](#)