PIX, TACACS+ 및 RADIUS 샘플 컨피그레이션 :4.2.x

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[네트워크 다이어그램](#)
[표기 규칙](#)
[인증 대 권한 부여](#)
[인증/권한 부여를 통해 사용자에게 표시되는 내용](#)
[모든 시나리오에 사용되는 서버 구성](#)
[Cisco Secure UNIX TACACS+ 서버 컨피그레이션](#)
[Cisco Secure UNIX RADIUS 서버 구성](#)
[Cisco Secure NT 2.x RADIUS](#)
[EasyACS TACACS+](#)
[Cisco Secure NT 2.x TACACS+](#)
[Livingston RADIUS 서버 구성](#)
[Merit RADIUS 서버 구성](#)
[TACACS+ 프리웨어 서버 컨피그레이션](#)
[디버깅 단계](#)
[PIX의 인증 디버그 예](#)
[권한 부여 추가](#)
[PIX의 인증 및 권한 부여 디버그 예](#)
[계정 추가](#)
[TACACS+](#)
[RADIUS](#)
[최대 세션 및 로그인한 사용자 보기](#)
[Except 명령 사용](#)
[PIX 자체에 대한 인증](#)
[사용자에게 표시되는 프롬프트 변경](#)
[관련 정보](#)

소개

FTP, 텔넷 및 HTTP 연결에 대해 RADIUS 및 TACACS+ 인증을 수행할 수 있습니다.TACACS+ 권한 부여가 지원됩니다.RADIUS 권한 부여가 아닙니다.

PIX 소프트웨어 4.2.2에서 인증 구문이 약간 변경되었습니다. 이 문서에서는 소프트웨어 버전

4.2.2에 대한 구문을 사용합니다.

사전 요구 사항

요구 사항

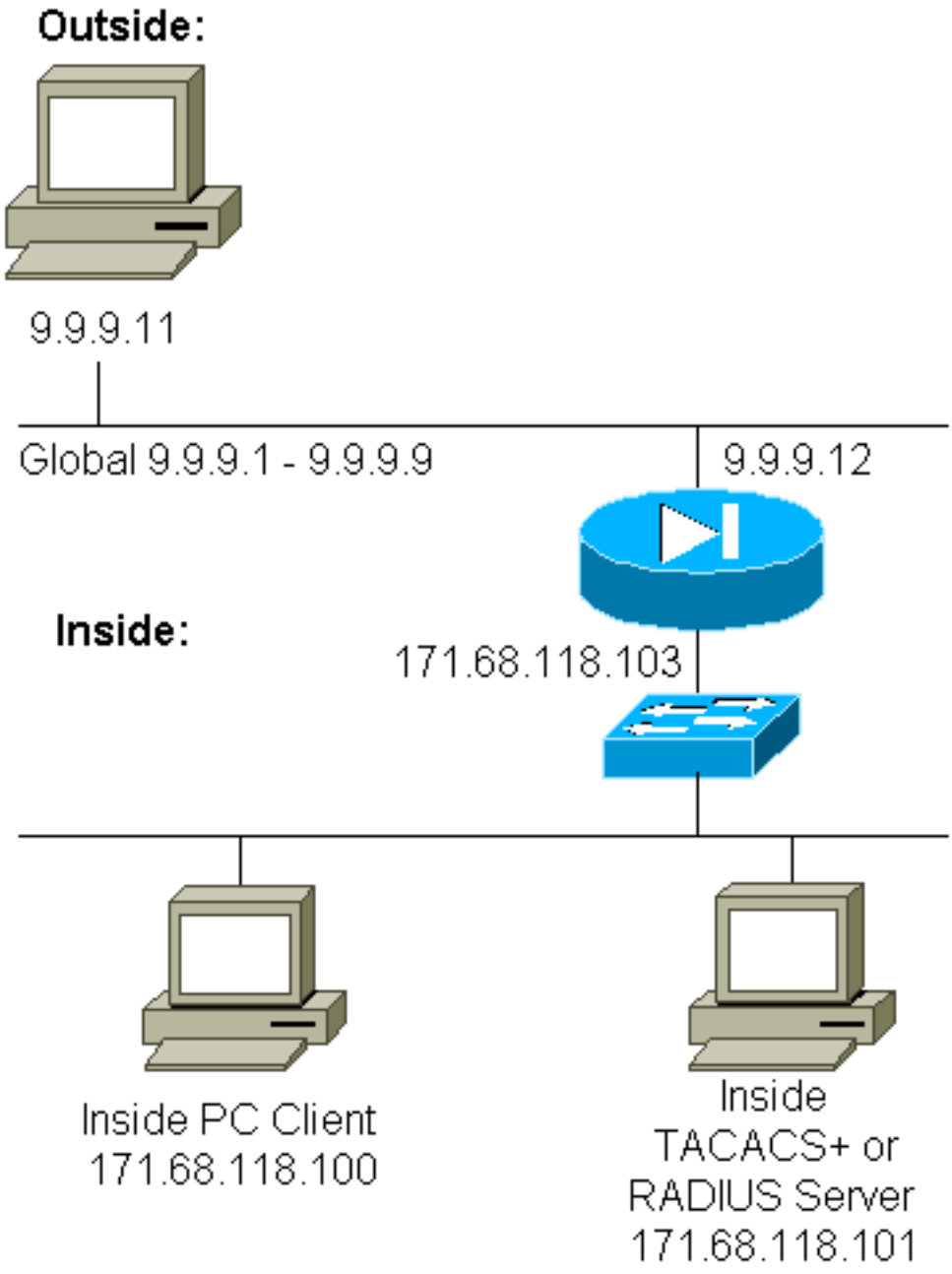
이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



PIX 컨피그레이션

```
pix2# write terminal
Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
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  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
!--- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout
10
!
!--- The focus of concern is with hosts on the inside
network !--- accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11
   255.255.255.255 tacacs+|radius
!
!--- It is possible to be less granular and authenticate
```

```
!--- all outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

표기 규칙

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

인증 대 권한 부여

- 인증*은* 사용자 입니다.
- 권한 부여는 사용자가 할 수 있는 작업입니다.
- 인증*은 권한* 없이 유효합니다.
- 인증*이* 없으면 권한 부여가 유효하지 않습니다.

예를 들어, 100명의 사용자가 내부에 있고 이러한 사용자 중 6명만 네트워크 외부에서 FTP, 텔넷 또는 HTTP를 수행할 수 있기를 원한다고 가정합니다.PIX에 아웃바운드 트래픽을 인증하고 TACACS+/RADIUS 보안 서버에 있는 6명의 사용자 ID를 모두 제공하도록 지시합니다.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 전달합니다.또한 응답에 따라 연결이 열리거나 거부됩니다.이 6명의 사용자는 FTP, 텔넷 또는 HTTP를 수행할 수 있습니다.

그러나 이 세 사용자 중 "Terry"를 신뢰할 수 없다고 가정하십시오.Terry가 FTP를 수행하도록 허용하되 HTTP나 텔넷을 외부에 허용하지 않습니다.즉, 권한 부여를 추가해야 합니다.즉, 사용자가 자신을 인증하는 것 외에 무엇을 할 수 있는지 인증합니다.PIX에 권한 부여를 추가하면 PIX는 먼저 Terry의 사용자 이름과 비밀번호를 보안 서버로 전송한 다음, Terry가 하려고 하는 "명령"을 보안 서버에 알리는 권한 부여 요청을 보냅니다.서버가 제대로 설정되면 Terry는 "FTP 1.2.3.4"을 사용할 수 있지만 어디에서든 "HTTP" 또는 "텔넷"을 사용할 수 없습니다.

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.**브라우저**에서 **사용자 이름과 암호를 캐시한다는 점에 유의하십시오**.PIX가 HTTP 연결을 시간 초과해야 하지만 시간 초과로 표시되지 않는 경우 브라우저에 캐시된 사용자 이름과 비밀번호를 PIX에 "사격"하는 방식으로 재인증이 발생할 가능성이 높습니다.그런 다음 이를 인증 서버로 전달합니다.PIX syslog 및/또는 서버 디버그는 이러한 현상을 보여줍니다.텔넷과 FTP가 정상적으로 작동하는 것처럼 보이지만 HTTP 연결이 정상적으로 작동하지 않는 경우, 이러한 이유가 됩니다.

모든 시나리오에 사용되는 서버 구성

TACACS+ 서버 컨피그레이션 예에서 인증만 설정된 경우 사용자 "all", "telnetonly", "httponly" 및 "ftponly"가 모두 작동합니다.RADIUS 서버 컨피그레이션 예에서는 "all" 사용자가 작동합니다.

PIX에 권한 부여가 추가되면 TACACS+ 인증 서버에 사용자 이름과 비밀번호를 전송하는 것 외에도 PIX는 명령(텔넷, HTTP 또는 FTP)을 TACACS+ 서버로 전송합니다.그런 다음 TACACS+ 서버는 해당 사용자가 해당 명령에 대해 권한이 있는지 확인합니다.

다음 예에서 171.68.118.100의 사용자는 **telnet 9.9.9.11** 명령을 실행합니다. PIX에서 수신되면 PIX는 사용자 이름, 비밀번호 및 명령을 TACACS+ 서버에 전달하여 처리합니다.

따라서 인증 외에도 권한 부여를 통해 "telnet only" 사용자는 PIX를 통해 텔넷 작업을 수행할 수 있습니다.그러나 "httponly" 및 "ftponly" 사용자는 PIX를 통해 텔넷 작업을 수행할 수 없습니다.

(프로토콜 사양의 특성으로 인해 RADIUS에서는 권한 부여가 지원되지 않습니다.)

Cisco Secure UNIX TACACS+ 서버 컨피그레이션

Cisco Secure 2.x

- 여기에 사용자 기준이 표시됩니다.
- PIX IP 주소 또는 정규화된 도메인 이름 및 키를 CSU.cfg에 추가합니다.

```
user = all {
password = clear "all"
default service = permit
}

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

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

```
}
}

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

Cisco Secure UNIX RADIUS 서버 구성

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

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

Cisco Secure NT 2.x RADIUS

CiscoSecure 2.1 온라인 및 웹 설명서의 샘플 구성 섹션에서는 설정에 대해 설명합니다.특성 6(Service-Type)은 로그인 또는 관리입니다.

GUI를 사용하여 NAS Configuration(NAS 컨피그레이션) 섹션에서 PIX의 IP를 추가합니다.

EasyACS TACACS+

EasyACS 설명서는 설정 정보를 제공합니다.

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 명령에 대해 **Add/Edit**(예: 텔넷)를 선택합니다.
4. 텔넷을 특정 사이트에 허용하려면 인수 섹션에 IP를 입력합니다.모든 사이트에 텔넷을 허용하려면 목록에 없는 **모든 인수 허용 을** 클릭합니다.
5. 편집 **완료 명령을 클릭합니다**.
6. 허용되는 각 명령(예: 텔넷, HTTP 및/또는 FTP)에 대해 1단계부터 5단계까지 수행합니다.
7. GUI를 사용하여 NAS Configuration(NAS 컨피그레이션) 섹션에서 PIX의 IP를 추가합니다.

Cisco Secure NT 2.x TACACS+

설정 정보는 Cisco Secure 2.x 설명서를 참조하십시오.

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. 하단의 **명령** 확인란을 선택하고 허용할 명령을 입력합니다(예: 텔넷).
4. 텔넷을 특정 사이트에 허용하려면 인수 섹션에 IP를 입력합니다(예: "permit 1.2.3.4"). 모든 사이트에 텔넷을 허용하려면 목록에 없는 인수 **허용 을** 클릭합니다.
5. Submit(제출)**을 클릭합니다**.
6. 허용되는 각 명령(예: 텔넷, FTP 및/또는 HTTP)에 대해 1단계부터 5단계까지 수행합니다.

7. GUI를 사용하여 NAS Configuration(NAS 컨피그레이션) 섹션에서 PIX의 IP를 추가합니다.

Livingston RADIUS 서버 구성

클라이언트 파일에 PIX IP 및 키를 추가합니다.

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

Merit RADIUS 서버 구성

PIX IP 및 키를 클라이언트 파일에 추가합니다.

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

TACACS+ 프리웨어 서버 컨피그레이션

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

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

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

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

디버깅 단계

- AAA(Authentication, Authorization, and Accounting)를 추가하기 전에 PIX 컨피그레이션이 작동하는지 확인합니다.AAA를 시작하기 전에 트래픽을 전달할 수 없는 경우 나중에 트래픽을 전달할 수 없습니다.
- PIX에서 로깅을 활성화합니다.**logging console 디버깅** 명령은 로드가 많은 시스템에서 사용할 수 없습니다.logging buffered **디버깅** 명령을 사용할 수 있습니다.그런 다음 **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.

PIX의 인증 디버그 예

PIX 디버그 - 정상 인증 - RADIUS

다음은 올바른 인증으로 PIX 디버그의 예입니다.

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

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

이는 잘못된 인증(사용자 이름 또는 비밀번호)을 사용하는 PIX 디버그의 예입니다. 사용자에게 네 개의 사용자 이름/비밀번호 세트가 표시됩니다."오류:최대 재시도 횟수 초과" 메시지가 표시됩니다.

참고: FTP 시도인 경우 한 번의 시도가 허용됩니다.HTTP의 경우 무한 재시도가 허용됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX 디버그 - 서버 다운 - RADIUS

이것은 서버가 다운된 PIX 디버그의 예입니다.사용자는 사용자 이름을 한 번 확인합니다.그런 다음 서버가 "중단"하고 비밀번호를 요청합니다(3회).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX 디버그 - 양호한 인증 - TACACS+

다음은 올바른 인증으로 PIX 디버그의 예입니다.

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

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

이는 잘못된 인증(사용자 이름 또는 비밀번호)을 사용하는 PIX 디버그의 예입니다. 사용자에게 네 개의 사용자 이름/비밀번호 세트가 표시됩니다."오류:최대 재시도 횟수 초과" 메시지가 표시됩니다.

참고: FTP 시도인 경우 한 번의 시도가 허용됩니다.HTTP의 경우 무한 재시도가 허용됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX 디버그 - 서버 다운 - TACACS+

이것은 서버가 다운된 PIX 디버그의 예입니다.사용자는 사용자 이름을 한 번 확인합니다.즉시 "오류 :최대 시도 횟수 초과" 메시지가 표시됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

권한 부여 추가

인증 없이 권한 부여가 유효하지 않으므로 동일한 소스 및 대상에 권한 부여가 필요합니다.

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius
```

또는 세 아웃바운드 서비스가 모두 원래 인증된 경우

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
```

PIX의 인증 및 권한 부여 디버그 예

PIX 디버그 - 올바른 인증 및 권한 부여 - TACACS+

다음은 올바른 인증 및 권한 부여가 있는 PIX 디버그의 예입니다.

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
```

```
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX 디버그 - 양호한 인증이지만 권한 부여에서 실패 - TACACS+

다음 예는 인증 수준이 높지만 권한 부여에서 실패한 PIX 디버그의 예입니다.

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX 디버그 - 잘못된 인증, 권한 부여를 시도하지 않음 - TACACS+

인증 및 권한 부여가 있는 PIX 디버그의 예시이지만 잘못된 인증(사용자 이름 또는 비밀번호)으로 인해 권한 부여를 시도하지 않았습니다. 사용자에게 네 개의 사용자 이름/비밀번호 세트가 표시됩니다."오류:최대 재시도 횟수를 초과했습니다." 메시지가 표시됩니다.

참고: FTP 시도인 경우 한 번의 시도가 허용됩니다.HTTP의 경우 무한 재시도가 허용됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX 디버그 - 인증/권한 부여, 서버 다운 - TACACS+

다음은 인증 및 권한 부여가 있는 PIX 디버그의 예입니다.서버가 다운되었습니다.사용자가 사용자 이름을 한 번 확인합니다.즉시 "오류:최대 시도 횟수를 초과했습니다." 표시됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

계정 추가

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+
```

Debug는 어카운팅이 켜져 있는지 꺼져 있는지 확인합니다.그러나 "Built(기본 제공)"일 때 "시작" 회계 레코드가 전송됩니다.또한 "해체" 시 "중지" 회계 기록이 전송됩니다.

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
```

```
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

TACACS+ 어카운팅 레코드는 이 출력과 같습니다(CiscoSecure UNIX에서 가져온 것입니다.Cisco Secure Windows의 레코드는 쉼표로 구분될 수 있습니다.

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

이 필드는 다음과 같이 구분됩니다.

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

Debug는 어카운팅이 켜져 있는지 꺼져 있는지 확인합니다.그러나 "Built(기본 제공)"일 때 "시작" 회계 레코드가 전송됩니다.또한 "해체" 시 "중지" 회계 기록이 전송됩니다.

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

RADIUS 어카운팅 레코드는 이 출력과 같습니다(Cisco Secure UNIX에서 가져온 것입니다.Cisco Secure Windows의 경우 쉼표로 구분됩니다.

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
```

```
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

이 필드는 다음과 같이 구분됩니다.

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

최대 세션 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 개인이 아직 로그인되어 있다고 가정합니다.PIX를 통한 세션이 있습니다. 이는 연결의 특성 때문에 텔넷 및 FTP 연결에 적합합니다.예를 들면 다음과 같습니다.

사용자 텔넷은 PIX를 통해 171.68.118.100에서 9.9.9.25까지 전송되며, 다음 중 인증 절차를 수행합니다.

```
(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(이 시점에서) 서버에 "텔넷" 사용자가 로그인되어 있음을 표시합니다.사용자가 인증을 필요로 하는 또 다른 연결(다른 PC의 경우)을 시도하고 이 사용자에 대해 최대 세션이 서버에서 "1"로 설정된 경우 서버에서 연결이 거부됩니다.

사용자는 대상 호스트에서 비즈니스를 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 0인지 여부(즉,매번 인증) 또는 그 이상(uauth 기간 동안 한 번 인증 및 다시 인증 안 함), 액세스한 모든 사이트에 대한 계정 레코드 컷이 있습니다.

그러나 HTTP는 프로토콜의 특성 때문에 다르게 작동합니다.예:

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.

시간을 확인합니다.이 다운로드는 1초(시작 레코드와 중지 레코드 사이에 1초 미만)이 걸렸습니다. 사용자가 여전히 웹 사이트에 로그인되어 있으며 연결이 여전히 열려 있습니까?아니요.

최대 세션 또는 로그인한 사용자 보기가 여기서 작동합니까?아니요, HTTP의 연결 시간이 너무 짧기 때문입니다."Built(기본 설정)"에서 "Teardown"("start(시작)" 및 "stop(중지)" 레코드) 사이의 시간은 초 미만입니다."중지" 기록이 없는 "시작" 레코드는 거의 동일한 순간에 발생하므로 없습니다 .uauth가 0으로 설정되었는지 또는 그 이상의 값으로 설정되었는지에 관계없이 모든 트랜잭션에 대해 서버에 "시작" 및 "중지" 레코드가 여전히 전송됩니다.그러나 HTTP 연결의 특성 때문에 최대 세션 및 로그인 사용자 보기가 작동하지 않습니다.

Except 명령 사용

네트워크에서 한 발신 사용자(171.68.118.100)을 인증할 필요가 없다고 결정하면 다음을 수행할 수 있습니다.

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
   255.255.255.255 tacacs+
```

PIX 자체에 대한 인증

이전의 논의에서는 PIX를 통해 텔넷(및 HTTP, FTP) 트래픽을 인증하는 것입니다.4.2.2을 사용하면 PIX에 대한 텔넷 연결도 인증할 수 있습니다.여기서는 PIX에 텔넷할 수 있는 박스 IP를 정의합니다.

```
telnet 171.68.118.100 255.255.255.255
```

그런 다음 텔넷 비밀번호를 입력합니다.**passwd ww**.

PIX에 텔네팅을 사용하여 사용자를 인증하는 새 명령을 추가합니다.

```
aaa authentication telnet console tacacs+|radius
```

사용자가 PIX에 텔넷하면 텔넷 비밀번호("ww")를 입력하라는 프롬프트가 표시됩니다. 또한 PIX는 TACACS+ 또는 RADIUS 사용자 이름 및 비밀번호를 요청합니다.

사용자에게 표시되는 프롬프트 변경

명령을 추가하는 경우**auth-prompt YOU_ARE_AT_THE_PIX**, PIX를 통과하는 사용자는 다음 시퀀스를 볼 수 있습니다.

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter the password]
```

최종 목적지에 도착하면 "Username:" 및 "Password:" 프롬프트가 표시됩니다.이 프롬프트는 PIX가 아닌 PIX를 통과하는 사용자에게만 영향을 미칩니다.

참고: PIX에 액세스하기 위해 잘라낸 회계 레코드가 없습니다.

관련 정보

- Cisco PIX 방화벽 소프트웨어 제품 지원
- Cisco Secure PIX Firewall 명령 참조
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems