Cisco Secure PIX Firewall에서 인증 및 활성화 방법(5.2~6.2)

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
구성 가능한 RADIUS 포트(5.3 이상)
표기 규칙
텔넷 인증 - 내부
네트워크 다이어그램
PIX 구성에 추가된 명령
콘솔 포트 인증
인증된 Cisco Secure VPN Client 1.1 - 외부
인증된 VPN 3000 2.5 또는 VPN Client 3.0 - 외부
인증된 VPN 3000 2.5 또는 VPN 클라이언트 3.0 - 외부 - 클라이언트 구성
SSH - 내부 또는 외부
네트워크 다이어그램
AAA 인증 SSH 구성
로컬 SSH 구성(AAA 인증 없음)
SSH 디버그
문제가 될 수 있는 부분
PIX에서 RSA 키를 제거하는 방법
PIX에 RSA 키를 저장하는 방법
외부 SSH 클라이언트에서 SSH를 허용하는 방법
인증 사용
syslog 정보
AAA 서버가 다운되었을 때 액세스 확보
TAC 케이스를 열 경우 수집할 정보
관련 정보

소개

이 문서에서는 PIX 소프트웨어 버전 5.2~6.2를 실행하는 PIX 방화벽에 대한 AAA 인증 액세스를 생성하는 방법과 AAA 서버가 다운되었을 때 인증 활성화, syslogging 및 액세스 권한 획득에 대한 정보를 제공합니다. PIX 5.3 이상에서는 이전 버전의 코드에 비해 AAA(Authentication, Authorization, and Accounting)가 변경되어 RADIUS 포트를 구성할 수 있습니다.

PIX 소프트웨어 버전 5.2 이상에서는 5가지 방법으로 PIX에 대한 AAA 인증 액세스를 생성할 수 있

습니다.

- 텔넷 인증 - 내부
- 콘솔 포트 인증
- 인증된 Cisco Secure VPN Client 1.1 - 외부
- 인증된 VPN 3000 2.5 - 외부
- SSH(Authenticated Secure Shell) - 내부 또는 외부

참고: PIX에서 DES 또는 3DES를 활성화해야 합니다(확인하려면 show version 명령 실행). PIX 소프트웨어 버전 6.0 이상에서는 PDM(PIX Device Manager)을 로드하여 GUI 관리를 활성화할 수도 있습니다. PDM은 이 문서의 범위를 벗어납니다.

PIX 6.2용 인증 및 권한 부여 명령에 대한 자세한 내용은 PIX 6.2: 인증 및 권한 부여 명령 컨피그레이션 예.

PIX 소프트웨어 버전 6.3 이상을 실행하는 PIX 방화벽에 대한 AAA 인증(컷스루 프록시) 액세스를 생성하려면 PIX/ASA를 참조하십시오. TACACS+ 및 RADIUS 서버 컨피그레이션 예를 사용하여 네트워크 액세스를 위한 컷스루 프록시.

사전 요구 사항

요구 사항

AAA 인증을 추가하기 전에 다음 작업을 수행합니다.

- PIX의 비밀번호를 추가하려면 다음 명령을 실행합니다.**암호 wwtelnet <local_ip> [<mask>] [<if_name>]**PIX는 이 비밀번호를 자동으로 암호화하여 키워드 **encrypted**로 암호화된 문자열을 구성합니다(예:
  `passwd OnTrBUG1Tp0edmkr encrypted`
  암호화된 키워드를 추가할 필요가 없습니다.
- 이러한 명령문을 추가한 후 AAA 인증 *없이* 내부 네트워크에서 PIX의 내부 인터페이스로 텔넷할 수 있는지 확인합니다.
- 명령을 백업해야 하는 경우 인증 문을 추가하는 동안 항상 PIX에 대한 연결을 열어 두어야 합니다.

AAA 인증(시퀀스가 클라이언트에 종속되는 SSH 제외)에서 사용자는 PIX 비밀번호(passwd <anything>과 같이)에 대한 요청*을 확인한* 다음 RADIUS 또는 TACACS 사용자 이름 및 비밀번호를 요청합니다.

참고: PIX의 외부 인터페이스에 텔넷할 수 없습니다. 외부 SSH 클라이언트에서 연결된 경우 외부 인터페이스에서 SSH를 사용할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX Software 버전 5.2, 5.3, 6.0, 6.1 또는 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 클라이언트 2.5
- Cisco VPN Client 3.0.x(PIX 6.0 코드 필요)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성 가능한 RADIUS 포트(5.3 이상)

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

aaa-server radius-authport #

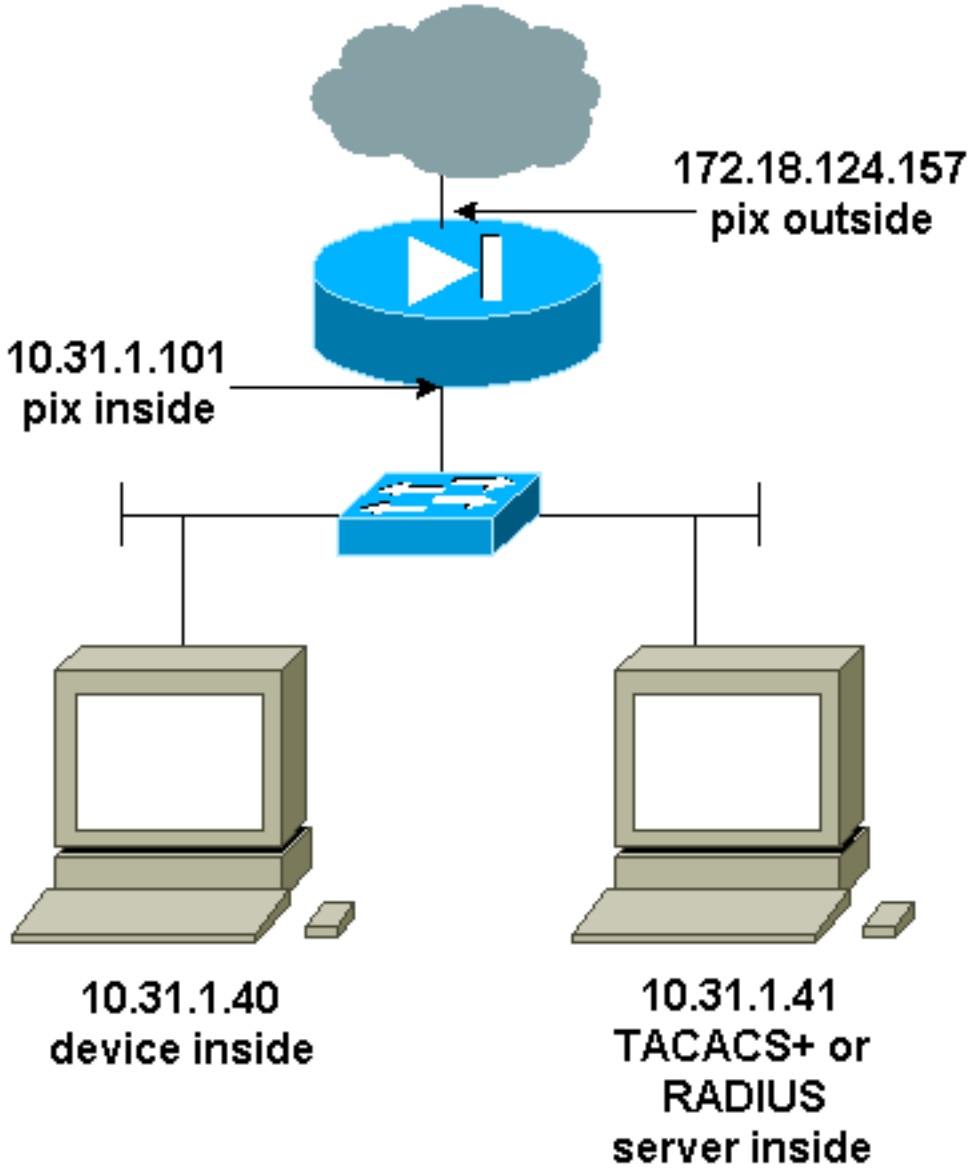
aaa-server radius-acctport #

표기 규칙

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

텔넷 인증 - 내부

네트워크 다이어그램



PIX 구성에 추가된 명령

다음 명령을 구성에 추가합니다.

aaa-server topix 프로토콜 tacacs+

aaa server tofix host 10.31.1.41 cisco timeout 5

aaa 인증 텔넷 콘솔 tofix

사용자는 PIX 비밀번호(`passwd <anything>`)에 대한 요청을 확인한 다음 RADIUS 또는 TACACS 사용자 이름 및 비밀번호(10.31.1.41 TACACS 또는 RADIUS 서버에 저장됨)에 대한 요청을 봅니다.

콘솔 포트 인증

다음 명령을 구성에 추가합니다.

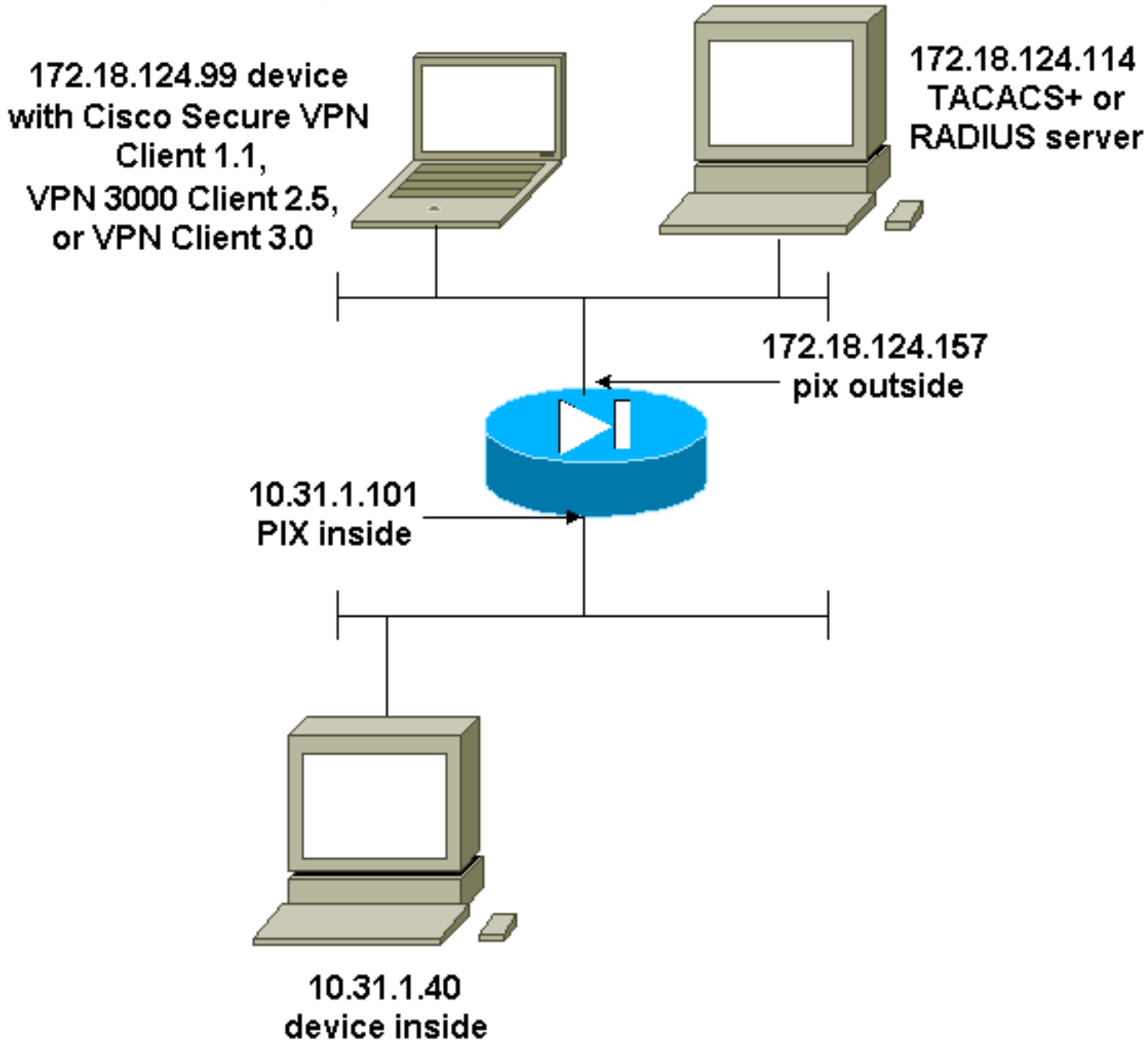
aaa-server topix 프로토콜 tacacs+

aaa server tofix host 10.31.1.41 cisco timeout 5

aaa 인증 직렬 콘솔 tofix

사용자는 PIX 비밀번호(passwd <anything>)에 대한 요청을 확인한 다음 RADIUS/TACACS 사용자 이름/비밀번호(RADIUS 또는 TACACS 10.31.1.41 서버에 저장됨)에 대한 요청을 봅니다.

다이어그램 - VPN Client 1.1, VPN 3000 2.5 또는 VPN Client 3.0 - 외부



인증된 Cisco Secure VPN Client 1.1 - 외부

인증된 Cisco Secure VPN Client 1.1 - 외부 - 클라이언트 구성
1- Myconn My Identity Connection security: Secure Remote Party Identity and addressing ID Type: IP address Port all Protocol all Pre-shared key (matches that on PIX) Connect using secure tunnel

```
          ID Type: IP address
          172.18.124.157

     Authentication (Phase 1)
     Proposal 1

          Authentication method: Preshared key
          Encryp Alg: DES
          Hash Alg: MD5
          SA life:  Unspecified
          Key Group: DH 1

     Key exchange (Phase 2)
     Proposal 1
          Encapsulation ESP
          Encrypt Alg: DES
          Hash Alg: MD5
          Encap: tunnel
          SA life: Unspecified
          no AH

 2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

인증된 Cisco Secure VPN Client 1.1 - 외부 - 부분 PIX 컨피그레이션

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
!--- If you know the IP address of the outside client,
use that !--- IP address in this statement. isakmp key
******** address 0.0.0.0 netmask 0.0.0.0 ! isakmp
identity address isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- We knew our client would access the
PIX from this !--- network. If you know the IP address
of the client, use that IP address !--- in this
statement. telnet 172.18.124.0 255.255.255.0 outside
```

인증된 VPN 3000 2.5 또는 VPN Client 3.0 - 외부

인증된 VPN 3000 2.5 또는 VPN 클라이언트 3.0 - 외부 - 클라이언트 구성

1. VPN **Dialer(VPN 다이얼러) > Properties(속성) > Name the connection** from the VPN 3000을 선택합니다.
2. Authentication **> Group Access Information을 선택합니다**. 그룹 이름과 암호는 vpngroup

<*group_name*> password ******* 문의 PIX에 있는 **것과** 일치해야 합니다.

Connect(연결)를 클릭하면 암호화 터널이 나타나고 PIX가 테스트 폴에서 IP 주소를 할당합니다(VPN 3000 클라이언트에서 mode-config만 지원됨). 그런 다음 터미널 창, 텔넷을 172.18.124.157에 연결하고 AAA 인증을 받을 수 있습니다. PIX의 **telnet 192.168.1.x** 명령을 사용하면 풀의 사용자에서 외부 인터페이스로 연결할 수 있습니다.

인증된 VPN 3000 2.5 - 외부 - 부분 PIX 컨피그레이션

```
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.31.1.101 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
!!--- ISAKMP Policy for VPN 3000 Client runs 2.5 code.
isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash md5 !--- The 2.5
client uses group 1 policy (PIX default). isakmp policy
10 group 1 isakmp policy 10 lifetime 86400 !--- ISAKMP
Policy for VPN Client runs 3.0 code. isakmp policy 20
authentication pre-share isakmp policy 20 encryption des
isakmp policy 20 hash md5 !--- The 3.0 clients use D-H
group 2 policy and require PIX 6.0 code. isakmp policy
20 group 2 isakmp policy 20 lifetime 86400 ! vpngroup
vpn3000 address-pool test vpngroup vpn3000 idle-time
1800 vpngroup vpn3000 password ******** telnet
192.168.1.0 255.255.255.0 outside
```

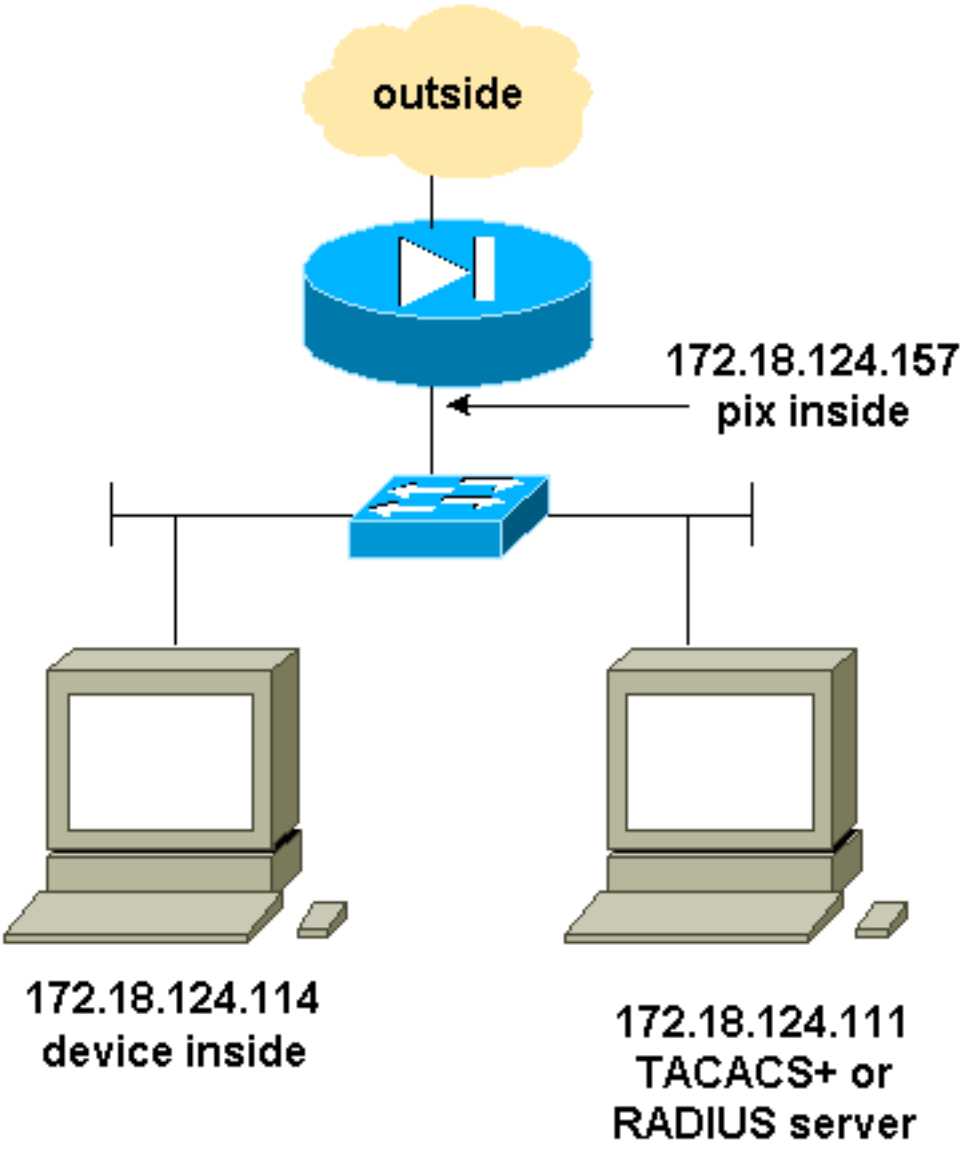
SSH - 내부 또는 외부

PIX 5.2는 SSH(Secure Shell) 버전 1 지원을 추가했습니다. SSH 1은 1995년 11월 IETF 초안을 기반으로 합니다. SSH 버전 1과 2는 서로 호환되지 않습니다. SSH에 대한 자세한 내용은 SSH(Secure Shell) FAQ 를 참조하십시오.

PIX는 SSH 서버로 간주됩니다. SSH 클라이언트(즉, SSH를 실행하는 상자)에서 SSH 서버(PIX)로의 트래픽이 암호화됩니다. 일부 SSH 버전 1 클라이언트는 PIX 5.2 릴리스 정보에 나열됩니다. Lab의 테스트는 NT의 F-Secure SSH 1.1 및 Solaris용 버전 1.2.26으로 수행되었습니다.

참고: PIX 7.x의 경우 시스템 액세스 관리의 SSH 액세스 허용 섹션을 참조하십시오.

네트워크 다이어그램



AAA 인증 SSH 구성

AAA 인증 SSH를 구성하려면 다음 단계를 완료합니다.

1. SSH를 켜지만 사용하지 않고 AAA를 사용하여 PIX에 텔넷할 수 있는지 확인합니다.
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   참고: SSH가 구성된 경우 PIX에서 ssh **172.18.124.114 255.255.255.255**가 실행되므로 **telnet 172.18.124.114 255.255.255** 명령이 필요하지 않습니다. 두 명령 모두 테스트 목적으로 포함되어 있습니다.
2. 다음 명령을 사용하여 SSH를 추가합니다.
   ```
   hostname goss-d3-pix515b
   domain-name rtp.cisco.com
   ca gen rsa key 1024!--- Caution: The RSA key is not be saved without !--- the ca save all
   command. !--- The write mem command does not save it. !--- In addition, if the PIX has
   undergone a write erase !--- or has been replaced, then cutting and pasting !--- the old
   configuration does not generate the key. !--- You must re-enter the ca gen rsa key command.
   !--- If there is a secondary PIX in a failover pair, the write standby !--- command does
   not copy the key from the primary to the secondary. !--- You must also generate and save
   the key on the secondary device.

   ssh 172.18.124.114 255.255.255.255 inside
   ssh timeout 60
   ```

```
aaa authen ssh console AuthOutbound
logging trap debug
logging console debug
```

3. config 모드에서 **show ca mypubkey rsa** 명령을 실행합니다.

```
goss-d3-pix(config)#show ca mypubkey rsa
 % Key pair was generated at: 08:22:25 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com
  Usage: General Purpose Key
  Key Data:
   30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb
   e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d
   4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7
   133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077
   81e93184 af55438b dcdcda34 c0a5f5ad 87c435ef
      67170674 4d5ba51e 6d020301 0001
 % Key pair was generated at: 08:27:18 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com.server
  Usage: Encryption Key
  Key Data:
   307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a
   4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8
   fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae
   6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
```

4. Solaris 스테이션에서 텔넷을 테스트합니다.

```
rtp-evergreen#./ssh -c 3des -l cisco -v 172.18.124.157
```

참고: "cisco"는 RADIUS/TACACS+ 서버의 사용자 이름이며 172.18.124.157은 대상입니다.

로컬 SSH 구성(AAA 인증 없음)

로컬 인증과 AAA 서버 없이 PIX에 대한 SSH 연결을 설정할 수도 있습니다. 그러나 사용자별 사용자 이름은 별도로 표시되지 않습니다. 사용자 이름은 항상 "pix"입니다.

다음 명령을 사용하여 PIX에서 로컬 SSH를 구성합니다.

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not saved without !--- the ca save all command.
!--- The write mem command does not save it. !--- In addition, if the PIX has undergone a write
erase !--- or has been replaced, then cutting and pasting !--- the old configuration does not
generate the key. !--- You must re-enter the ca gen rsa key command. !--- If there is a
secondary PIX in a failover pair, a write standby !--- command does not copy the key from the
primary to the secondary. !--- You must also generate and save the key on the secondary device.
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
passwd cisco123
```

이 정렬의 기본 사용자 이름은 항상 "pix"이므로 PIX에 연결하는 명령(Solaris 상자의 3DES)은 다음과 같습니다.

```
./ssh -c 3des -1 pix -v <ip_of_pix>
```

SSH 디버그

debug ssh 명령 없이 디버그 - 3DES 및 512-cipher

```
109005: Authentication succeeded for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
109011: Authen Session Start: user 'cse', sid 0
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
315011: SSH session from 172.18.124.114 on interface inside
   for user "cse" terminated normally
```

debug ssh 명령 - 3DES 및 512-cipher로 디버그

```
goss-d3-pix#debug ssh
SSH debugging on
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

디버그 - 3DES 및 1024-암호

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

디버그 - DES 및 1024-암호

참고: 이 출력은 Solaris가 아닌 SSH가 있는 PC에서 출력됩니다.

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
SSH(ssh): starting user authentication request,
   and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
SSH0: starting exec shell5: Authentication succeeded for user 'ssh'
   from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
   for user "ssh"
```

디버그 - 3DES 및 2048-암호

참고: 이 출력은 Solaris가 아닌 SSH가 있는 PC에서 출력됩니다.

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3.
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
SSH1: invalid request - 0x255:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
   for user "cse"
```

문제가 될 수 있는 부분

Solaris 디버그 - 2048-cipher 및 Solaris SSH

참고: Solaris에서 2048 암호를 처리할 수 없습니다.

```
rtp-evergreen.cisco.com: Initializing random;
seed file /export/home/cse/.ssh/random_seed
RSA key has too many bits for RSAREF to handle (max 1024).
```

RADIUS/TACACS+ 서버의 잘못된 비밀번호 또는 사용자 이름

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA serverss-d3-pix#
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

다음 명령을 통해 허용되지 않는 사용자:

ssh 172.18.124.114 255.255.255.255 내부

연결 시도:

315001: 내부 인터페이스의 161.44.17.151에서 거부된 SSH 세션

PIX에서 키 제거(**ca zero rsa** 명령 사용) 또는 ca save all 명령과 함께 저장되지 않은 경우

```
Device opened successfully.
SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com',
   terminate SSH connection.
SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
   disconnected by SSH server, reason: "Internal error" (0x00)
```

AAA 서버가 다운되었습니다.

```
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
```

```
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server1090
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH0: password authentication failed for cse0
SSH0: authentication failed for cse
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
   on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

클라이언트가 3DES에 대해 설정되었지만 PIX에는 DES 키만 있습니다.

참고: 클라이언트가 DES를 지원하지 않는 Solaris였습니다.

```
GOSS-PIX# Device opened successfully.
SSH: host key initialised
SSH: license supports DES: 1.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

Solaris CLI에서 다음을 수행합니다.

```
Selected cipher type 3DES not supported by server.
```

PIX에서 RSA 키를 제거하는 방법

ca 영 rsa

PIX에 RSA 키를 저장하는 방법

ca 모두 저장

외부 SSH 클라이언트에서 SSH를 허용하는 방법

ssh outside_ip *255.255.255.255* 외부

인증 사용

명령을 사용하여 다음을 수행합니다.

aaa authentication enable 콘솔 tofix

(여기서 *tofix*는 서버 목록) TACACS 또는 RADIUS 서버로 전송되는 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 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.

이러한 문제에 대한 자세한 내용은 Cisco 버그 ID CSCdm47044(등록된 고객만 해당)를 참조하십시오.

syslog 정보

AAA 어카운팅은 PIX를 통한 연결에 대해서만 유효하지만, PIX에 대한 연결에는 사용할 수 없지만 sysloging이 설정된 경우 인증된 사용자가 수행한 작업에 대한 정보가 syslog 서버(구성된 경우 syslog MIB를 통해 네트워크 관리 서버)로 전송됩니다.

syslog가 설정된 경우 다음과 같은 메시지가 syslog 서버에 표시됩니다.

로깅 트랩 알림 수준:

```
111006: Console Login from pixuser at console
111007: Begin configuration: 10.31.1.40 reading from terminal
111008: User 'pixuser' executed the 'conf' command.
111008: User 'pixuser' executed the 'hostname' command.
```

로깅 트랩 정보 수준(알림 수준 포함):

307002: 10.31.1.40에서 허용된 텔넷 로그인 세션

AAA 서버가 다운되었을 때 액세스 확보

AAA 서버가 다운된 경우, 텔넷 비밀번호 액세스를 초기에 PIX에 입력한 다음 사용자 이름에 대한 pix를 입력한 다음 비밀번호에 대한 enable 비밀번호(**enable password *anything*)를** 입력할 수 있습니다. PIX **컨피그레이션에 *없는* 비밀번호**를 활성화하면 사용자 이름에 pix를 입력하고 Enter 키를 **누릅니다**. enable 비밀번호가 설정되어 있지만 알려지지 않은 경우 비밀번호를 재설정하려면 비밀번호 복구 디스크가 필요합니다.

TAC 케이스를 열 경우 수집할 정보

위의 트러블슈팅 단계를 거친 후에도 지원이 필요한 경우 Cisco TAC에서 케이스를 열려면 다음 정보를 포함해야 합니다.
• 문제 설명 및 관련 토폴로지 세부사항 • 케이스를 열기 전에 수행된 트러블슈팅 • **show tech-support** 명령의 출력

- **logging buffered 디버깅** 명령을 사용한 실행 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 첨부하십시오. Case Query Tool(등록된 고객만)을 사용하여 케이스를 업로드하여 해당 케이스에 정보를 첨부할 수 있습니다. Case Query Tool에 액세스할 수 없는 경우 이메일 첨부 파일의 정보를 attach@cisco.com으로 보낼 수 있으며, 케이스 번호는 메시지의 제목 줄에 있습니다.

관련 정보

- Cisco Secure PIX Firewall 명령 참조
- PIX RADIUS TACACS+