PIX バージョン 5.2 以降におけるユーザの認証、許可、アカウンティングの実行

内容

概要

RADIUSおよびTACACS+認証は、Cisco Secure PIX Firewallを介したFTP、Telnet、およびHTTP接続に対して実行できます。他の一般的でないプロトコルの認証は、通常は動作するように行われます。TACACS+認可がサポートされています。RADIUS認証はサポートされていません。以前のバージョンに対するPIX 5.2の認証、許可、アカウンティング(AAA)の変更には、AAAアクセスリストのサポートが含まれ、認証者とユーザがアクセスするリソースを制御します。PIX 5.3以降では、以前のバージョンのコードに対する認証、許可、アカウンティング(AAA)の変更は、RADIUSポートが設定可能であることです。

注： PIX 6.xでは、通過トラフィックのアカウンティングは可能ですが、PIXに宛先されているトラフィックのアカウンティングは行えません。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Secure PIX ファイアウォール ソフトウェア バージョン 5.2.0.205 および 5.2.0.207

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

注：PIX/ASAソフトウェアのバージョン7.x以降を実行している場合は、『AAAサーバとローカルデータベースの設定』を参照してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

認証、許可、およびアカウンティング

認証、認可、アカウンティング(AAA)の説明を次に示します。

- 認証（Authentication）とは、ユーザが何者かを検証することです。
- 認可は、ユーザが行う機能です。
- 認証は、許可がなくても有効です。
- 許可は、認証がないと有効ではありません。
- アカウンティングとは、ユーザが行ったアカウンティングです。

ユーザがAuthentication/Authorization をオンにしたときに見る画面表示

ユーザが認証/許可をオンにして内部から外部（またはその逆）に移動しようとした場合：

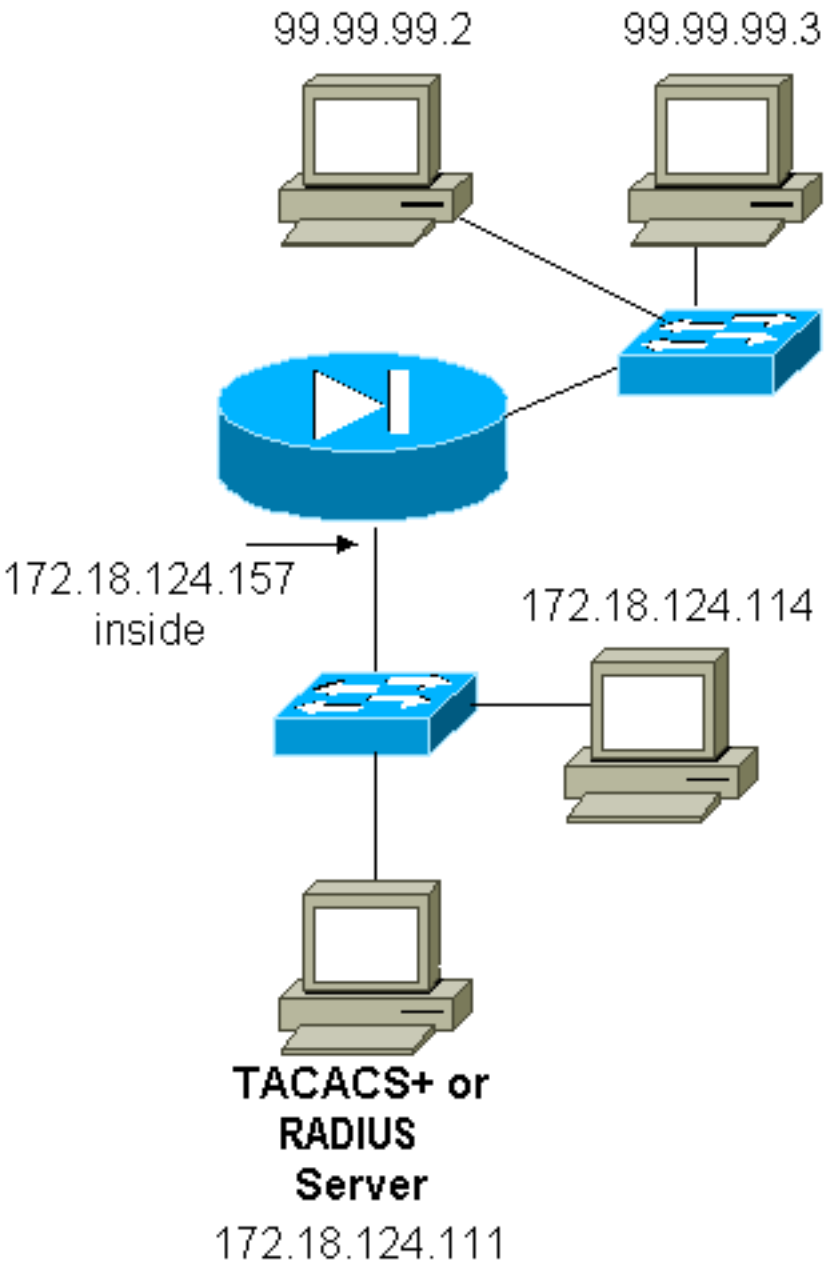
- **Telnet**：ユーザ名プロンプトが表示され、パスワードの要求が表示されます。認証（および許可）が PIX/サーバで正常に行われると、以降の宛先ホストからユーザ名とパスワードの入力を求められます。
- **FTP**：ユーザ名プロンプトが表示されます。ユーザ名に「local_username@remote_username」を、パスワードに「local_password@remote_password」を入力する必要があります。PIXは「local_username」と「local_password」をローカルセキュリティサーバに送信します。PIX/サーバで認証（および認可）が成功すると、「remote_username」と「remote_password」は宛先FTPサーバに渡されます。
- **HTTP**：ユーザ名とパスワードを要求するウィンドウがブラウザに表示されます。認証（および許可）が正常に行われると、宛先の Web サイトおよびその先に到達します。*ブラウザによってユーザ名とパスワードがキャッシュされることに注意してください。*PIXがHTTP接続をタイムアウトする必要があるにもかかわらずタイムアウトしない場合は、ブラウザがキャッシュされたユーザ名とパスワードをPIXに送信し、再認証が実際に行われる可能性があります。PIXはこれを認証サーバに転送します。この現象は、PIX syslogやサーバデバッグで示されます。TelnetとFTPが「正常」に動作しているように見えるが、HTTP接続が動作しない場合、これが原因です。

デバッグの手順

- AAA認証と認可を追加する前に、PIX設定が機能していることを確認します。認証と認可を設定する前にトラフィックを渡すことができない場合、その後はトラフィックを渡すことができません。
- PIX のいくつかのロギングを有効にします。logging console debugコマンド**を発行して**、logging console debuggingをオンにします。**注：負荷の高い**システムでは、ロギングコンソールデバッグを使用しないでください。logging monitor debug コマンドを使用して、Telnet セッションをログします。ロギング バッファ デバッグを使用してから、show logging コマンドを実行できます。ロギングは syslog サーバに送信して、そこで検査することもできます。
- TACACS+ サーバまたは RADIUS サーバでデバッグをオンにします。

認証だけ

ネットワーク図



サーバのセットアップ - 認証だけ

Cisco Secure UNIX TACACSサーバの設定

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

Cisco Secure UNIX RADIUSサーバの設定

注： 高度なGUIを使用して、PIXのIPアドレスとキーをネットワークアクセスサーバ(NAS)リストに追加します。

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

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

Cisco Secure Windows RADIUS

Cisco Secure Windows RADIUSサーバを設定するには、次の手順を使用します。

1. User Setup セクションでパスワードを入手します。
2. Group Setup セクションから、アトリビュート 6 (Service-Type) を Login または Administrative に設定します。
3. GUI の NAS Configuration セクションで PIX IP アドレスを追加します。

Cisco Secure Windows TACACS+

ユーザは User Setup セクションでパスワードを入手します。

Livingston RADIUS サーバの設定

注： PIXのIPアドレスとキーをclientsファイルに*追加*します。

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

Merit RADIUS サーバの設定

注： PIXのIPアドレスとキーをclientsファイルに*追加*します。

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

TACACS+ フリーウェア サーバの設定

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

PIX の初期設定：認証だけの場合

PIX の初期設定：認証だけの場合

`PIX Version 5.2(0)205`
`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`
`enable password 8Ry2YjIyt7RRXU24 encrypted`
`passwd OnTrBUG1Tp0edmkr encrypted`
`hostname pixfirewall`
`fixup protocol ftp 21`
`fixup protocol http 80`

```
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
```

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

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

設定可能な RADIUS ポート (5.3 以降)

一部の RADIUS サーバは、1645/1646 以外の RADIUS ポート (通常は 1812/1813) を使用します。 PIX 5.3以降では、次のコマンドを使用して、RADIUS認証ポートとアカウンティングポートをデフォルトの1645/1646以外に変更できます。

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

PIX 認証デバッグの例

デバッグをオンにする方法については、「デバッグ手順」を参照してください。これらは、内部172.18.124.114(99.99.99.99)へのトラフィックを開始する99.99.99.2のユーザの例であり、その逆も同様です。受信トラフィックは TACACS で認証し、送信トラフィックは RADIUS で認証し

ます。

認証の成功：TACACS+（受信）

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

ユーザ名/パスワードが正しくないため失敗した認証： TACACS+（受信）ユーザに「Error:最大試行回数を超えました。

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

サーバが PIX と通信しない：TACACS+（受信）。 username が一度だけ表示され PIX はパスワードを要求しません（Telnet 上）。 「Error:最大試行回数を超えました。

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

正常な認証：RADIUS（送信）

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

失敗した認証（ユーザ名またはパスワード）：RADIUS（送信）。 ユーザにユーザ名の要求が表示され、次にパスワードが表示されます。これらの入力を行う機会が3つあります。失敗した場合は、「Error:最大試行回数を超えました。

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

サーバは PING できてもデーモンが停止、サーバに PING できない、またはキー/クライアントのミスマッチにより PIX と通信しない：RADIUS（送信）。 ユーザに[Username]、[password]、[RADIUS server failed]、[Error:最大試行回数を超えました。

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
```

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

認証に許可を加えた場合

すべての認証されたユーザにPIX経由ですべての操作（HTTP、FTP、およびTelnet）を実行させる場合は、認証で十分であり、許可は必要ありません。ただし、一部のサービスを特定のユーザに許可したり、ユーザが特定のサイトにアクセスするのを制限したりする場合は、許可が必要です。RADIUS認可は、PIXを通過するトラフィックには有効ではありません。この場合、TACACS+認可は有効です。

認証に合格し、認可がオンの場合、PIXはユーザが実行しているコマンドをサーバに送信します。たとえば、「http 1.2.3.4」などです。 PIXバージョン5.2では、TACACS+認可がアクセスリストと組み合わせて使用され、ユーザの移動先を制御します。

HTTP（アクセスされたWebサイト）の認証を実装する場合は、単一のWebサイトに多数のIPアドレスを関連付けることができるため、Websenseなどのソフトウェアを使用します。

サーバのセットアップ - 認証に許可を加えた場合

Cisco Secure UNIX TACACSサーバの設定

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

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

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

Cisco Secure Windows TACACS+

Cisco Secure Windows TACACS+サーバをセットアップするには、次の手順を実行します。

1. グループ設定の下部にある[Deny unmatched IOS commands]をクリックします。
2. Add/Edit New Commandをクリックします（FTP、HTTP、Telnet）。たとえば、特定のサイト(「telnet 1.2.3.4」)へのTelnetを許可する場合、コマンドはtelnetです。引数は*1.2.3.4*です。「command=telnet」と入力した後で、Argument のボックスに「permit」の IP アドレスを入力します。（たとえば「permit 1.2.3.4」）すべての Telnet を許可する場合、コマンドは telnetのままで、Allow all unlisted argumentsをクリックします。次に、Finish editing command をクリックします。
3. ステップ 2 を許可するコマンドそれぞれに実行します（たとえば Telnet、HTTP、および FTP）。
4. GUIを使用して、[NAS Configuration]セクションにPIX IPアドレスを追加します。

TACACS+ フリーウェア サーバの設定

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

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

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

PIX 設定 - 許可の追加

認可を必要とするコマンドを追加します。

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

新しい5.2機能を使用すると、この文を以前に定義したアクセスリスト101と組み合わせて、前の3つの文を置き換えることができます。古い表現と新しい表現を一緒に用いないでください。

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

PIX 認証と許可デバッグの例

認証は正常に行われ許可も成功：TACACS+

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

認証は正常に行われたが許可は失敗：TACACS+。ユーザには「Error:Authorization Denied」と表示されます。

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

新しいアクセスリストの機能

PIXソフトウェアリリース5.2以降では、PIXでアクセスリストを定義します。サーバのユーザプロファイルに基づいて、ユーザごとに適用します。TACACS+ には、認証と許可が必要です。RADIUS では、認証だけが必要です。この例では、TACACS+に対する発信認証と認可が変更されています（TACACS+の場合）。PIXのアクセスリストが設定されている。

注：PIXバージョン6.0.1以降では、RADIUSを使用する場合は、標準IETF RADIUS属性11(Filter-Id) [CSCdt50422]にリストを入力してアクセスリストを実装します。この例では、ベンダー固有の「acl=115」の表現の代わりに、属性11が115に設定されています。

PIX の設定

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

サーバのプロファイル

注：TACACS+フリーウェアの2.1バージョンは、「acl」バージョンを認識しません。

Cisco Secure UNIX TACACS+サーバの設定

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

Cisco Secure Windows TACACS+

ユーザがアクセスリストを使用する場所を制御するためにPIXに許可を追加するには、**shell/exec**をオンにし、**Access control listボックスにチェックマークを入れ**（PIXのアクセスリスト番号と一致する）、番号を入力します。

Cisco Secure UNIX RADIUS

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

Cisco Secure Windows RADIUS

Radius/Cisco はデバイス タイプです。「pixa」ユーザには、ユーザ名、パスワード、およびチェックと「acl=115」が必要です。このボックスには、009\001 AV-Pair(vendor-specific)と表示されます。

出力

プロファイル内の「acl=115」を持つアウトバウンドユーザ「pixa」が認証および許可を行います。サーバはacl=115をPIXに渡し、PIXは次のように表示します。

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

ユーザ「pixa」が99.99.99.3(または暗黙のdenyがあるため、99.99.99.2以外の任意のIPアドレス)に移動しようとすると、次のように表示されます。

```
Error: acl authorization denied
```

ユーザごとにダウンロード可能な、バージョン 6.2 の新しいアクセス リスト

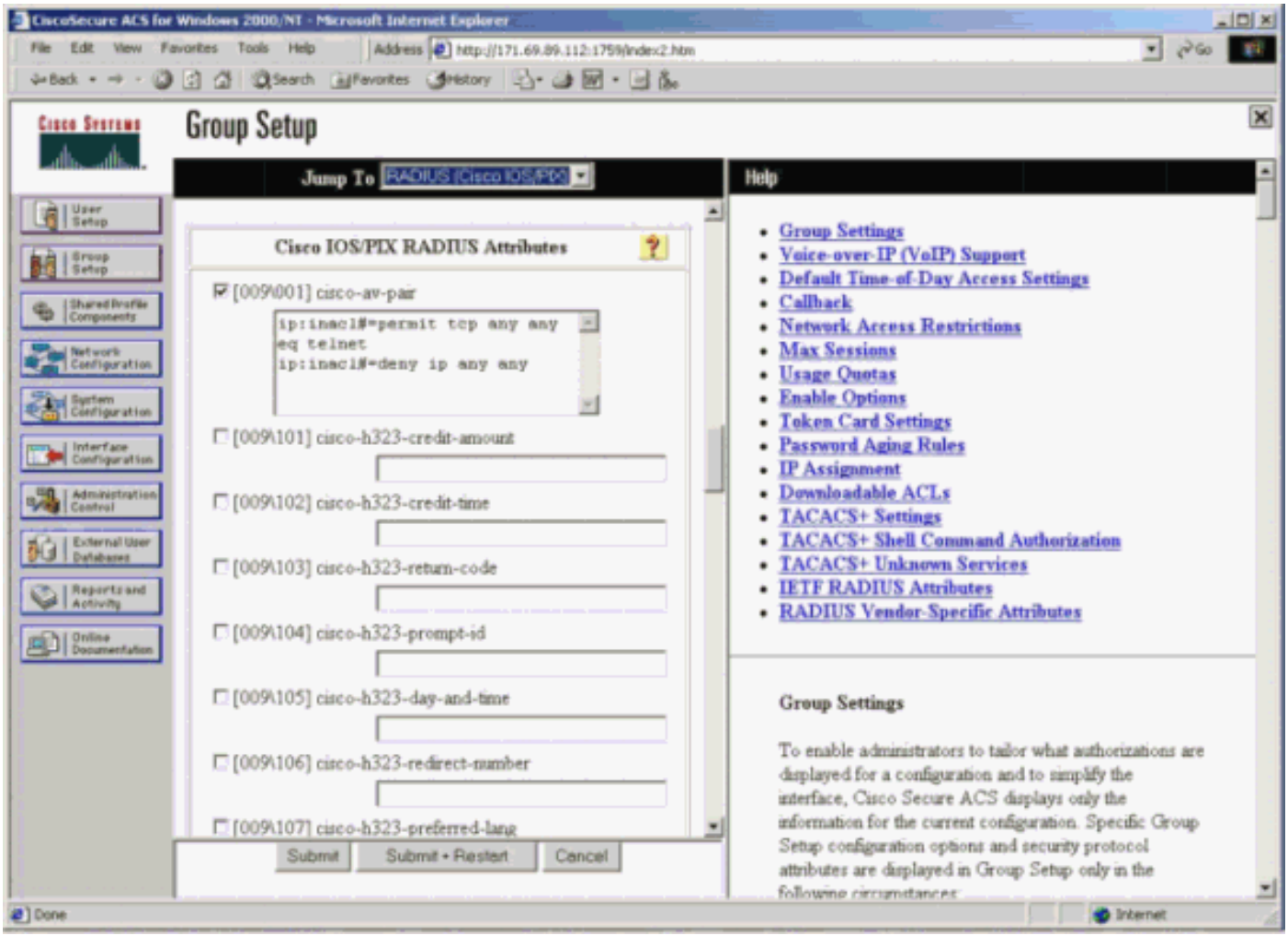
PIX Firewallのソフトウェアリリース6.2以降では、アクセスリストは認証後にPIXにダウンロードするためにアクセスコントロールサーバ(ACS)で定義されています。これは、RADIUSプロトコルでのみ動作します。アクセス リストを PIX 自体に設定する必要はありません。グループテンプレートは複数のユーザに適用されます。

以前のバージョンでは、アクセスリストはPIXで定義されています。認証時に、ACSはアクセスリスト名をPIXにプッシュしました。新しいバージョンでは、ACSがアクセスリストを直接PIXにプッシュできます。

注：フェールオーバーが発生した場合、uauthテーブルはコピーされません。ユーザは再認証されます。アクセスリストが再度ダウンロードされます。

ACS のセットアップ

[Group Setup]**をクリック**し、**RADIUS(Cisco IOS/PIX)デバイスタイプを選択**して、ユーザアカウントを設定します。ユーザに、ユーザ名 (この例では「cse」) とパスワードを割り当てます。[Attributes]リストから、[009\001] ***vendor-av-pairを設定するオプションを選択します。***次の例に示すように、アクセスリストを定義します。



PIX のデバッグ：有効な認証とダウンロードされたアクセス リスト

- Telnetのみを許可し、他のトラフィックを拒否します。

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
```

```
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

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

show uauthコマンドの出力です。

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

show access-listコマンドからの出力です。

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

- Telnetのみを拒否し、他のトラフィックを許可します。

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

show uauthコマンドの出力です。

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

show access-listコマンドからの出力です。

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

ユーザごとにダウンロード可能な、ACS 3.0 を使用した新しいアクセス リスト

ACS バージョン 3.0 では、共有プロファイル コンポーネントを使用してアクセス リストのテンプレートを作成し、特定のユーザやグループにテンプレート名を定義することができます。テンプレート名は、必要な数のユーザまたはグループで使用できます。これにより、ユーザごとに同一のアクセスリストを設定する必要がなくなります。

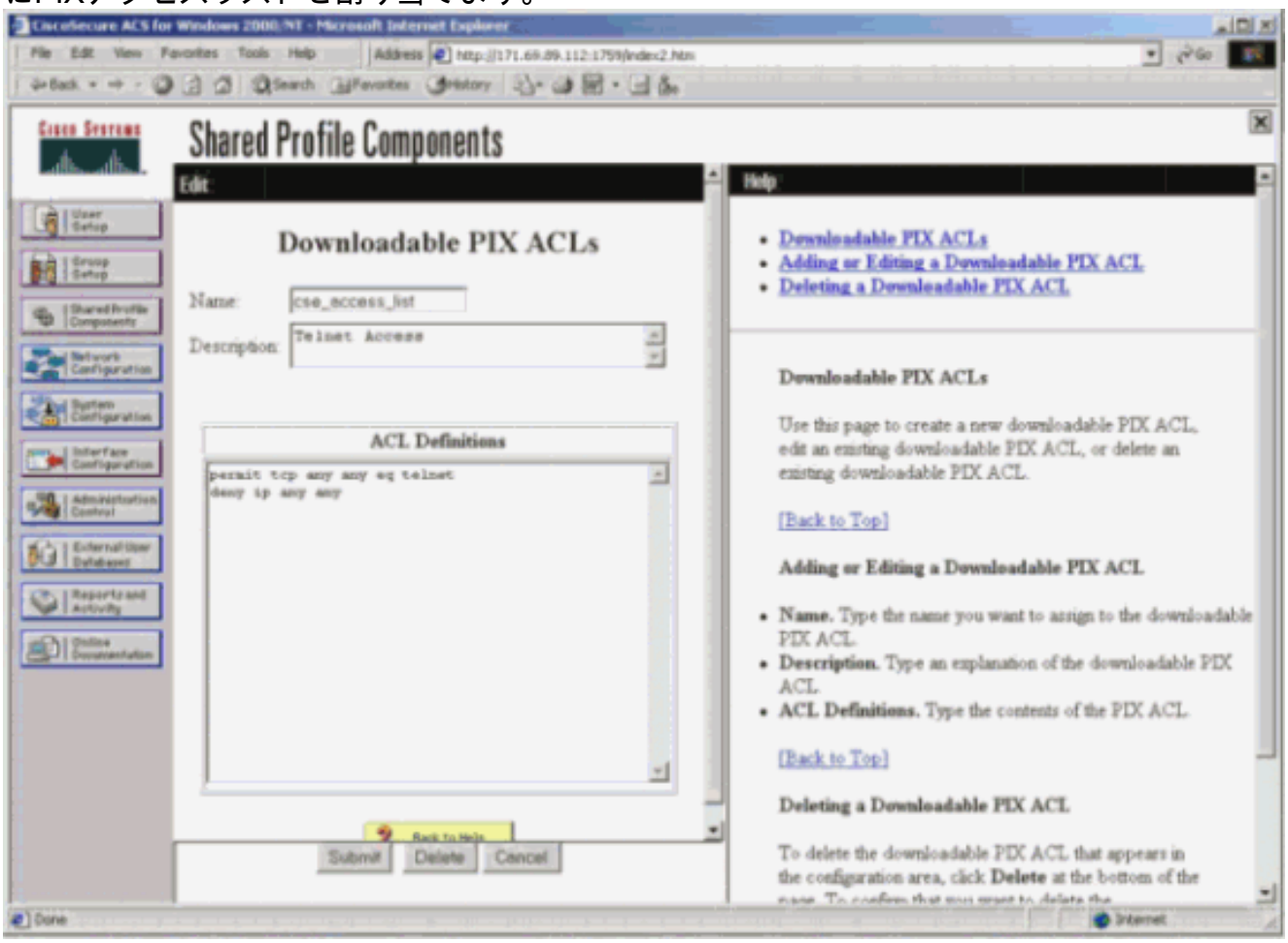
注：フェールオーバーが発生した場合、uauthはセカンダリPIXにコピーされません。ステートフルフェールオーバーでは、セッションは継続されます。ただし、新しい接続を再認証し、アクセ

スリストを再度ダウンロードする必要があります。

共有プロファイルの使用

共有プロファイルを使用する場合は、次の手順を実行します。

1. Interface Configuration をクリックします。
2. User-Level Downloadable ACLs および/または Group-Level Downloadable ACLsをチェックします。
3. [共有プロファイル**コンポーネント]をクリックします。[User-Level Downloadable ACLs]をクリックします。**
4. ダウンロード可能な ACL を定義します。
5. [グループ設**定]をクリックします。**[Downloadable ACLs]で、先ほど作成したアクセスリストにPIXアクセスリストを割り当てます。



PIX のデバッグ：有効な認証とダウンロードされたアクセス リスト (共有プロファイルを使用した場合)

- Telnetのみを許可し、他のトラフィックを拒否します。

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

```
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

show uauthコマンドの出力です。

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

show access-listコマンドからの出力です。

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

- Telnetのみを拒否し、他のトラフィックを許可します。

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

show uauthコマンドの出力です。

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

show access-listコマンドからの出力です。

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

アカウンティングの追加

PIXの設定：アカウンティングの追加

TACACS (AuthInbound=tacacs)

このコマンドを追加します。

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

または、5.2の新機能を使用して、アクセスリストで何を考慮するかを定義します。

```
aaa accounting match 101 outside AuthInbound
```

注：アクセスリスト101は別々に定義されます。

RADIUS (AuthOutbound=radius)

このコマンドを追加します。

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

または、5.2の新機能を使用して、アクセスリストで何を考慮するかを定義します。

```
aaa accounting match 101 outside AuthOutbound
```

注：アクセスリスト101は別々に定義されます。

注：PIX 7.0コード以降のPIX上の管理セッションに対して、アカウンティングレコードを生成できます。

アカウンティングの例

- TACACSアカウンティングの例：99.99.99.2 outsideから172.18.124.114 inside(99.99.99.99)へのTelnet。

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

- 172.18.124.114 inside(Telnet)から99.99.99.2 outside(Telnet)への接続および99.99.99.3 outside(HTTP)へのRADIUSアカウンティングの例。

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

```
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

    Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

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

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

exclude コマンドの使用

このネットワークでは、特定の送信元または宛先に認証、許可、アカウンティングが必要ないと判断した場合は、次のコマンドを発行します。

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

注： includeコマンドはすでに**あります**の**です**。

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

または、5.2の新機能を使用して、除外する対象を定義します。

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

注：認証からボックスを除外し、認証をオンにしている場合は、そのボックスも許可から除外する必要があります。

最大セッション数とログインユーザ数の表示

一部の TACACS+ および RADIUS サーバには、「最大セッション」または「ログイン ユーザの表示」機能があります。最大セッションを実行したりログイン ユーザをチェックしたりする機能は、アカウンティング レコードによって変わります。アカウンティングの「開始」レコードが生成されているが「停止」レコードがない場合、TACACS+ または RADIUS サーバは、だれかがまだログインしている（つまり、ユーザは PIX を介したセッションを維持している）と見なします。 これは Telnet や FTP 接続では接続の性質上うまく機能します。ただし、これはHTTPでは適切に動作しません。この例では、異なるネットワーク設定を使用していますが、概念は同じです。

ユーザがPIXを介してTelnetを実行し、途中で認証を行います。

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

サーバは「開始」レコードを認識したが「停止」レコードを認識していないため、この時点でサーバは「Telnet」ユーザがログインしていることを示します。ユーザが（おそらく別のPCからの）認証を必要とする別の接続を試み、このユーザのサーバでmax-sessionsが「1」に設定されている場合（サーバがmax-sessionsをサポートしている場合）、サーバによって接続が拒否されます。ユーザはターゲットホスト上でTelnetまたはFTPビジネスを行い、終了します（そこまで10分かかります）。

```
(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
```

uauth が 0 (つまり、毎回認証する) の場合でも、0 以上の場合でも (認証を 1 回行い uauth 期間中は再度行わない)、アカウンティング レコードはアクセスされたすべてのサイトで削除されます。

HTTP は、そのプロトコルの性質によって、動作が異なります。HTTPの例を次に示します。この例では、PIXを介して171.68.118.100から9.9.9.25にブラウズします。

```
(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
```

ユーザは、ダウンロードされた Web ページを読みます。開始レコードは16:35:34に投稿され、停止レコードは16:35:35に投稿されます。このダウンロードには1秒かかりました (つまり、開始レコードと停止レコードの間に1秒未満でした)。 ユーザがWebサイトにログインしていない。ユーザーがWebページを読み取っている場合、接続は開かれません。ここでは、最大セッションまたはログインユーザの表示は機能しません。これは、HTTPの接続時間 (「Built」と「Teardown」の間の時間) が短すぎるためです。「開始」および「停止」レコードは、1 秒以下です。ほぼ同じ瞬間に記録が発生するため、「停止」レコードのない「開始」レコードはありません。uauthが0に設定されていても、それ以上に設定されていても、トランザクションごとにサーバに「start」および「stop」レコードが送信されます。ただし、HTTP接続の性質により、max-sessionsとview logged-in usersは機能しません。

ユーザ インターフェイス

ユーザに表示するプロンプトの変更

次のコマンドがある場合：

```
auth-prompt prompt PIX515B
```

PIXを通過するユーザには、次のプロンプトが表示されます。

```
PIX515B
```

メッセージユーザのカスタマイズ表示

次のコマンドがある場合：

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

ログインに失敗または成功した場合の認証ステータスに関するメッセージが表示されます。

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

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

ユーザごとのアイドル/絶対タイムアウト

PIX の timeout uauth コマンドは、認証をどのくらいの頻度で必要とするかを調節します。TACACS+認証/認可がオンの場合、これはユーザごとに制御されます。このユーザプロファイルは、タイムアウトを制御するように設定されています（これはTACACS+フリーウェアサーバ上にあり、タイムアウトは分単位です）。

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

認証/許可の後

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

2分後：

絶対的なタイムアウトセッションは削除されます。

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

仮想 HTTP 送信

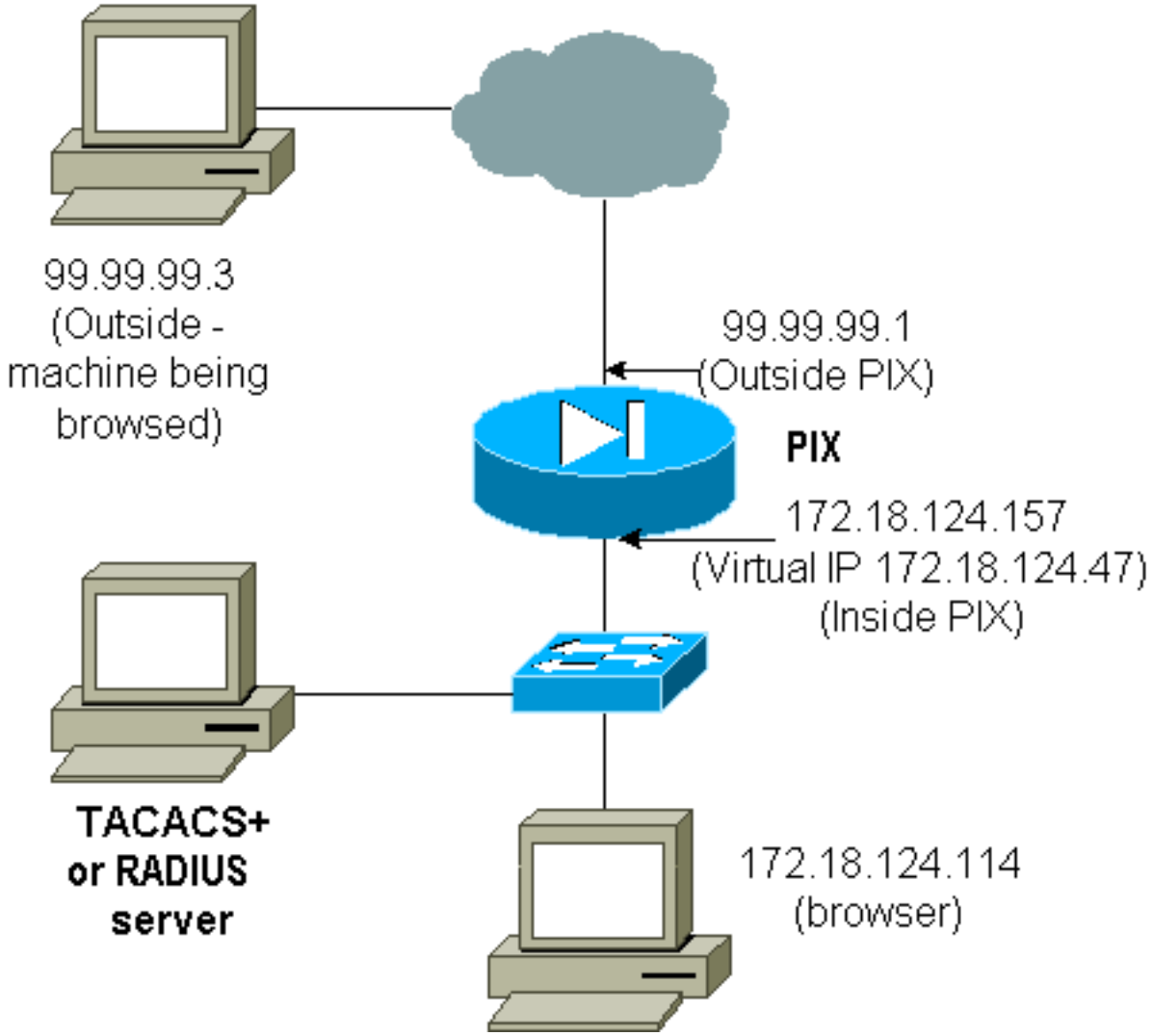
PIX外部のサイトやPIX自体で認証が必要な場合は、ブラウザがユーザ名とパスワードをキャッシュするため、異常なブラウザの動作が見られる場合があります。

これを回避するには、RFC 1918 アドレス(インターネット上でルーティング不可能なアドレスで、PIX内部ネットワークに対して有効で一意)を形式でPIX設定に追加して、仮想HTTPを実装します。

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

ユーザが PIX 外部に移動しようとすると、認証が必要になります。warn パラメータがある場合、ユーザはリダイレクト メッセージを受信します。認証は、uauth の中の期間に行われます。ドキュメントに示されているように、仮想HTTPでは**timeout uauthコマンド**の期間を0秒に設定しないでください。HTTP が実際の Web サーバに接続できなくなります。

注：仮想HTTPおよび仮想Telnet IPアドレスは、aaa authentication文に含める必要**があ**ります。この例では、0.0.0.0を指定すると、これらのアドレスが含まれます。



PIX設定で、次のコマンドを追加します。

```
virtual http 172.18.124.47
```

ユーザがブラウザを99.99.99.3にポイントすると、このメッセージが表示されます。

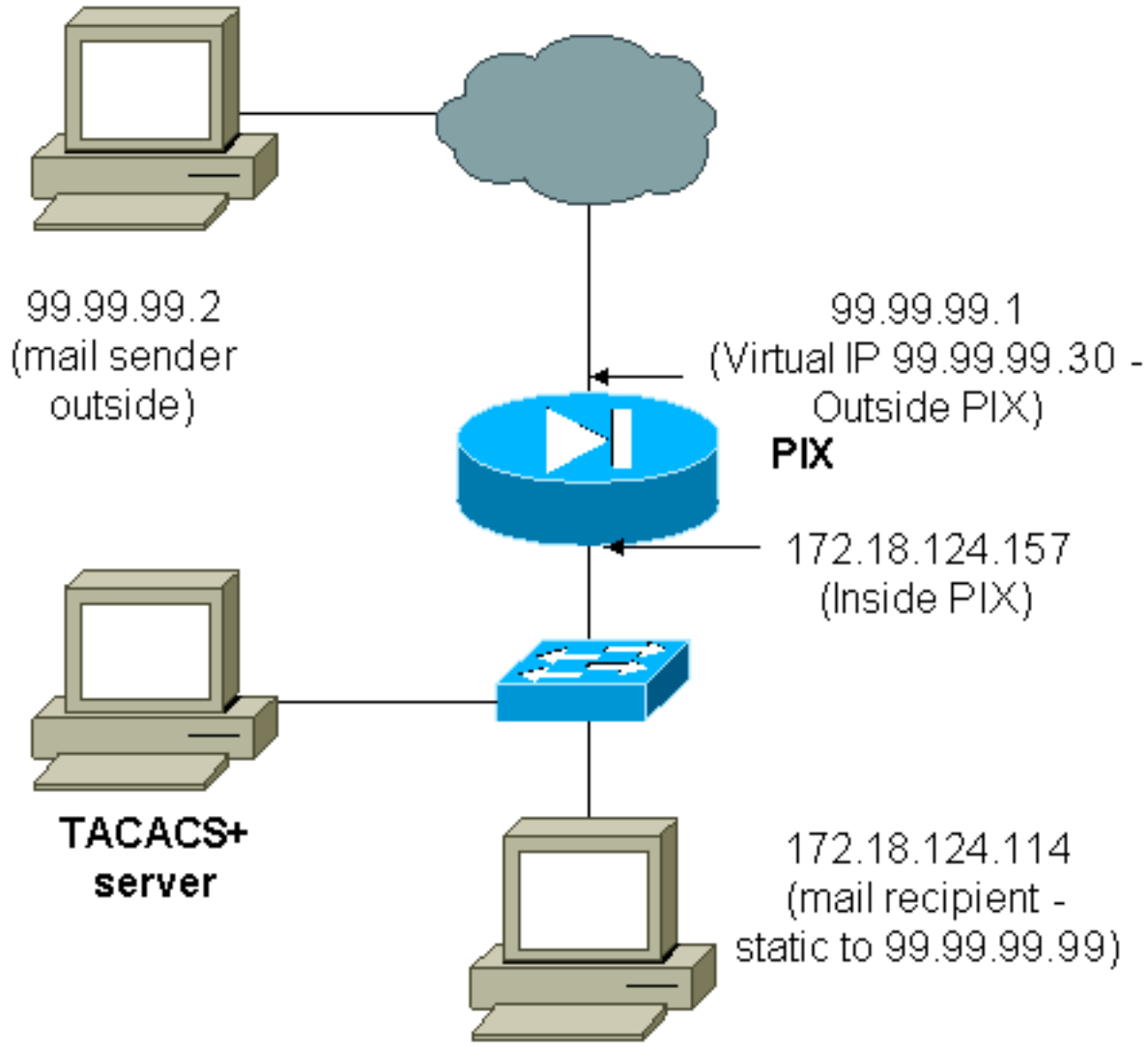
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

認証後、トラフィックは99.99.99.3にリダイレクトされます。

仮想 Telnet

注：仮想HTTPおよび仮想Telnet IPアドレスは、aaa authentication文に含める必要**があ**ります。この例では、0.0.0.0を指定すると、これらのアドレスが含まれます。

仮想 Telnet 受信



着信メールを送信するためのウィンドウが表示されないため、着信メールを認証することは推奨できません。代わりに**excludeコマンド**を使用します。ただし、説明のために、次のコマンドが追加されています。

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

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

ユーザ（これはTACACS+フリーウェアです）：

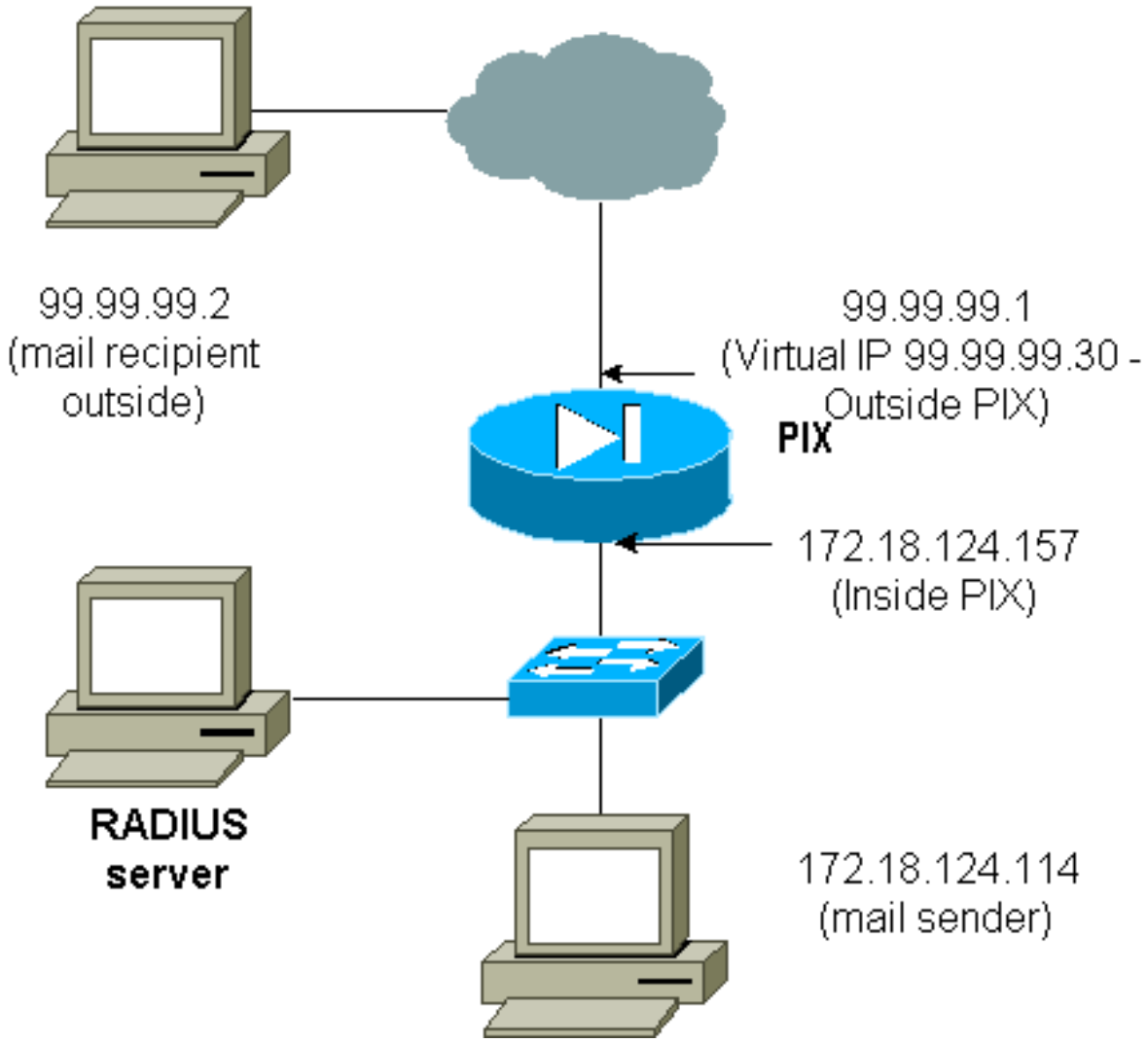
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


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

認証のみがオンの場合、両方のユーザはIPアドレス99.99.99.30へのTelnet認証の後に着信メールを送信します。認証が有効な場合、ユーザ「cse」は99.99.99.30にTelnetし、TACACS+ユーザ名/パスワードを入力します。Telnet接続が切断されます。次に、ユーザ「cse」が99.99.99.99 (172.18.124.114)にメールを送信します。 ユーザ「pixuser」の認証は成功します。 ただし、PIXがcmd=tcp/25およびcmd-arg=172.18.124.114に対する許可要求を送信すると、次の出力に示すように要求が失敗します。

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

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

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

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

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

仮想 Telnet 送信



着信メールを送信するためのウィンドウが表示されないため、着信メールを認証することは推奨できません。代わりに**excludeコマンド**を使用します。ただし、説明のために、次のコマンドが追加されています。

送信メールを送信するためのウィンドウが表示されないため、送信メールを認証することは推奨できません。代わりに**excludeコマンド**を使用します。ただし、説明のために、次のコマンドが追加されています。

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

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
```

```
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

内部から外部にメールを送信するには、メールホストでコマンドプロンプトを起動し、99.99.99.30にTelnetします。これにより、メールが通る穴が開きます。メールは172.18.124.114から99.99.99.2に送信されます。

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

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

仮想 Telnet ログアウト

ユーザは仮想 Telnet IP アドレスへ Telnet するとき、show uauth コマンドで、ホールが開いている時間を表示できます。ユーザがセッションの終了後に、トラフィックが通過しないようにする場合は（uauth に時間が残っているとき）、仮想 Telnet IP アドレスに再度 Telnet する必要があります。これによりセッションはオフに切り替わります。これを次の例で示します。

最初の認証

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

最初の認証後

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

2番目の認証

```
   pixfirewall# 109001: Auth start for user 'cse'
```

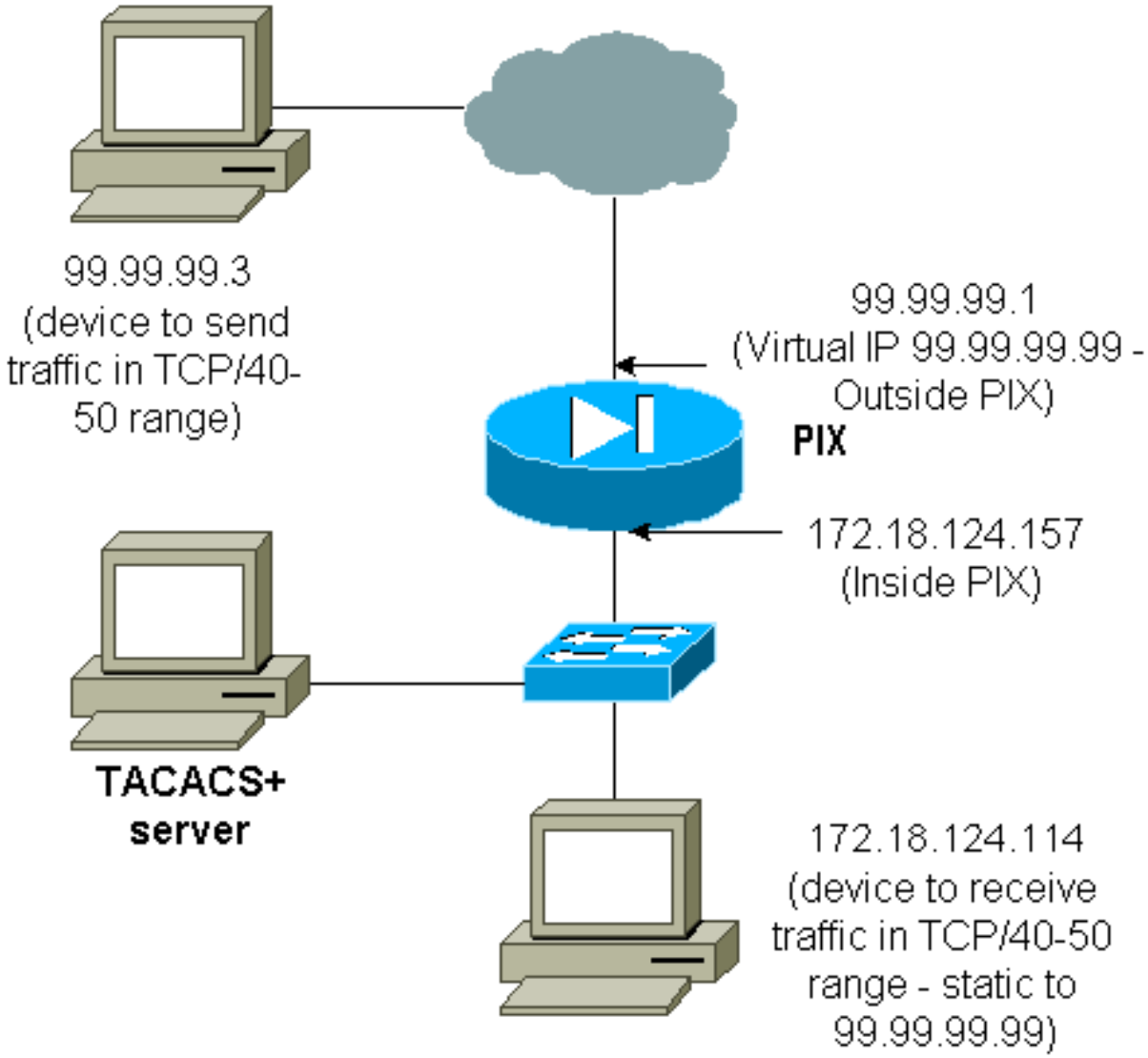
```
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

2回目の認証後

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

ポートの認可

ネットワーク図



許可をポート範囲に与えることができます。PIXで仮想Telnetが設定されており、ある範囲のポートに対して許可が設定されている場合、ユーザは仮想Telnetでホールを開きます。そして、ポート範囲に対する許可がオンでありこの範囲のトラフィックが PIX をヒットすると、PIX は許可を行うためコマンドを TACACS+ サーバに送信します。次の例は、ポート範囲の着信認証を示しています。

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

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

TACACS+ サーバ設定の例（フリーウェア）：

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

ユーザは、最初に仮想IPアドレス99.99.99.99にTelnet接続する必要があります。認証後、ユーザがPIXから99.99.99.99 (172.18.124.114)までのポート40 ~ 50の範囲のTCPトラフィックをプッシュしようとすると、cmd=tcp/40-50がTACACS+サーバに送信されます。

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

HTTP、FTP、および Telnet 以外のトラフィックのための AAA アカウンティング

仮想Telnetがネットワーク内のホストへのTCP/40-50トラフィックを許可することを確認したら、次のコマンドを使用して、このトラフィックのアカウンティングを追加します。

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

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

TACACS+ アカウンティング レコードの例

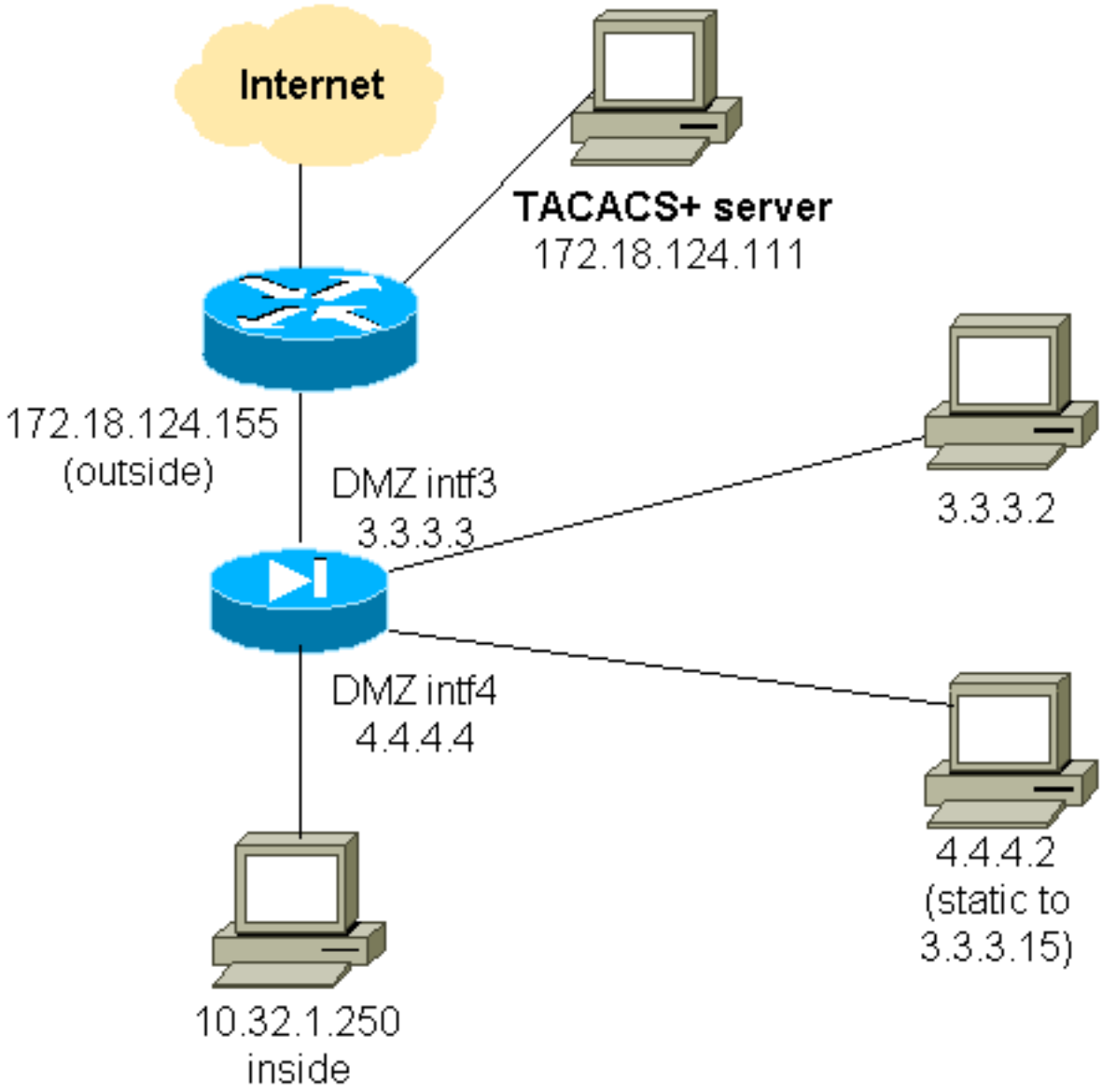
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80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

DMZ での認証

あるDMZインターフェイスから別のDMZインターフェイスに移動するユーザを認証するには、名前付きインターフェイスのトラフィックを認証するようにPIXに指示します。PIXの配置は次のようになります。

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

ネットワーク図



PIX の部分設定

次に示すように、pix/intf3とpix/intf4の間のTelnetトラフィックを認証します。

PIX の部分設定

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

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

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

TAC サービス リクエストをオープンする場合に収集する情報

上記のトラブルシューティング手順を実行した後もサポートが必要で、Cisco TACでケースをオープンする場合は、PIX Firewallのトラブルシューティングにこの情報を必ず含めてください。

- 問題の説明と関連するトポロジの詳細
- サービスリクエストをオープンする前のトラブルシューティング
- show tech-support コマンドの出力
- logging buffered debuggingコマンドを実行した後の**show logコマンド**の出力、または問題を示すコンソールキャプチャ(可能な場合)

収集したデータは、圧縮しないプレーン テキスト形式（.txt）でサービス リクエストに添付してください。 ケースに情報を添付するには、Case Query Tool（登録ユーザ専用）を使用してアップロードし、情報をケースに添付してください。 Case Query Toolにアクセスできない場合は、情報を電子メールの添付ファイルとしてattach@cisco.comに送信し、メッセージの件名にケース番号を記入してください。

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments (RFCs)
- Cisco Secure Access Control Server for Windows
- Cisco Secure Access Control Server for Unix
- Terminal Access Controller Access Control System（TACACS+）

- Remote Authentication Dial-In User Service (RADIUS)
- テクニカル サポートとドキュメント – Cisco Systems