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

目次

概要

RADIUS および TACACS+ 認証は Cisco Secure PIX Firewall による FTP、Telnet および HTTP 接続のためにすることができます。 他のより少なくよくあるプロトコルのための認証は通常はたらくためになされます。 TACACS+ 許可はサポートされます。 RADIUS認証はサポートされません。 以前のバージョン上の PIX 5.2 認証、許可、アカウンティング（AAA）の変更はだれが認証され、どんなリソース ユーザアクセスか制御するために AAAアクセス リストサポートが含まれています。 PIX 5.3 およびそれ以降では、コードの以前のバージョン上の認証、許可、アカウンティング（AAA）変更は RADIUSポートが設定可能であることです。

注: PIX 6.x はパススルー トラフィックのためのない PIX に destinated トラフィックのための会計をすることができます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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くものです。

- 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

注: PIX/ASA ソフトウェア バージョン 7.x およびそれ以降を実行する場合、AAA サーバおよびローカルデータベースの設定を参照して下さい。

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、認可、アカウンティング

認証、許可および会計の説明はここにあります:

- 認証（Authentication）とは、ユーザが何者かを検証することです。
- 許可はユーザがすることです。
- 認証は、認可がなくても有効です。
- 認可は、認証がないと有効ではありません。
- 会計はユーザがしたことです。

認証/認可を有効にしたときにユーザに表示される内容

ユーザが認証/許可と内部から外部へ（または逆に）行くことを試みる時:

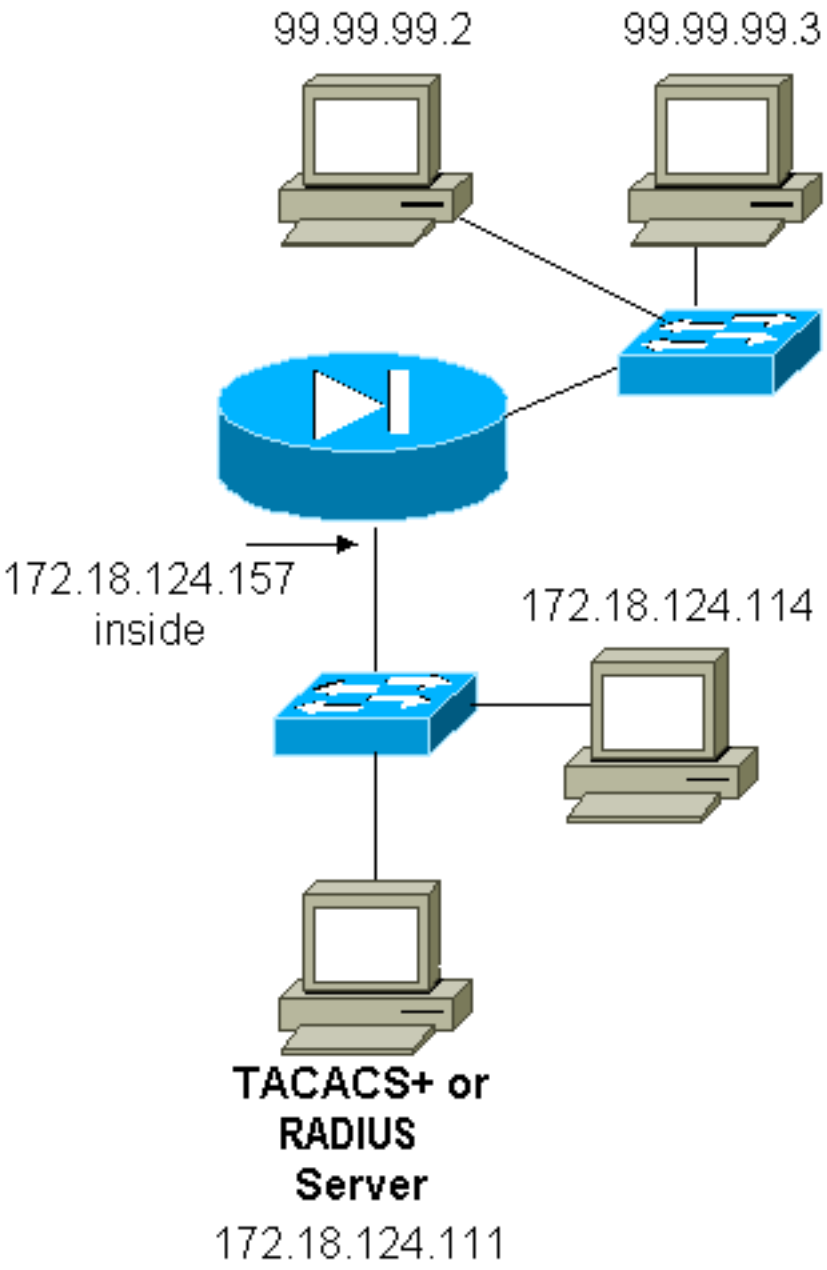
- Telnet：ユーザ名を求めるプロンプトが表示されてから、パスワードが要求されます。PIX/サーバで認証（および認可）に成功すると、外部の宛先ホストからユーザ名とパスワードの入力を求められます。
- **FTP**： ユーザ名を求めるプロンプトがユーザに表示されます。 ユーザ名に「local_username@remote_username」を、パスワードに「local_password@remote_password」を入力する必要があります。 PIX はローカルセキュリティサーバに「local_username」および「local_password」を送信 します。 認証（および許可） PIX/server で正常である場合、「remote_username」および「remote_password」は宛先FTPサーバに向こう通じます。
- HTTP： ユーザ名とパスワードを求めるウィンドウがブラウザに表示されます。 認証（および認可）に成功すると、ユーザは外部の宛先 Web サイトに到達します。 **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 は時間を計る必要があること HTTP接続を現われたりそうしない場合、再認証が PIX にブラウザ「射撃」と実際にキャッシュされたユーザ名およびパスワード起こる可能性が高いといえます。 PIX は認証サーバにこれを転送します。 PIX syslog やサーバ デバッグはこの現象を示します。 Telnet および FTP が「正常に」働くようであるが HTTP 接続が場合、これは原因です。

デバッグの手順

- AAA認証および認証を追加する前に PIX 設定作業を確かめて下さい。 認証 および 権限を実施する前にトラフィックを通過させることができなければ、そうその後することができません。
- PIX のいくつかのロギングを有効にします。logging console debugging をつける **logging console debug コマンドを**発行して下さい。**注:** ロードされたシステムの logging console debugging を重く使用しないで下さい。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 設定

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

Cisco Secure UNIX RADIUS サーバコンフィギュレーション

注: PIX IP アドレスを追加し、（NAS）リストにアドバンストGUI の助けによって VPDN ダイヤルインのネットワーク アクセス サーバ（NAS）キー入力して下さい。

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
```

```
reply_attributes= {
6=6
}
}
}
```

Cisco Secure Windows RADIUS

RADIUS が断絶する Cisco Secure Windows を設定するのにこれらのステップを使用して下さい。

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 IP アドレスを追加し、クライアントにファイルをキー入力して下さい。

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

Merit RADIUS サーバの設定

注: PIX IP アドレスを追加し、クライアントにファイルをキー入力して下さい。

- 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 およびそれ以降では、RADIUS認証およびアカウンティングポートはこれらのコマンドでデフォルト 1645/1646 以外何かに変更することができます:

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

PIX 認証デバッグの例

デバッグを回す方法についての情報についてはデバッグのステップを参照して下さい。 これらは内部 172.18.124.114 へ 99.99.99.2 にユーザの例その開始 トラフィックです（99.99.99.99）またその逆にも。 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）ユーザは「エラーを見ます: 超過する試みの最大数」。

```
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）。 ユーザは「エラーを見ます: 超過する試みの最大数」。

```
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）。 ユーザはユーザ名については要求を見ます、そして不成功ならパスワードに、これらを、入力する、3 つの機会が見ます「エラーをあり: 超過する試みの最大数」。

```
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) 。 次にユーザはユーザ名を、そしてパスワード、それから「RADIUSサーバ最終的に失敗しました」、「エラー見、：超過する試みの最大数」。

```
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

すべての認証済みユーザを PIX によってすべてのオペレーション (HTTP、FTP するため、および Telnet を) 行う割り当てたいと思う場合認証は十分であり、許可は必要ではないです。 ただし、サービスのサブセットを一定のユーザに許可するか、または行くことからある一定のサイトにユーザを制限したいと思えば許可は必要です。 RADIUS認証は PIX によってトラフィックのために無効です。 TACACS+ 許可はこの場合有効です。

認証が渡り、許可がオンになっていれば、PIX はユーザがサーバにしているコマンドを送信 します。 ユーザがどこに行くか制御するのにたとえば、「アクセス リストと共に PIX のバージョン 5.2 の http 1.2.3.4." が、TACACS+ 許可使用されています。

HTTP (参照される Webサイト) のための許可を設定したいと思ったら単一 Webサイトはそれと関連付けられる多数の IP アドレスがある場合があるので Websense のようなソフトウェアを使用して下さい。

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 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+ サーバを設定するためにこれらのステップを完了して下さい。

1. グループセットアップの下部ので『Deny unmatched IOS commands』 をクリック して下さい。
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"）に Telnet を許可したいと思えばコマンドは **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 の助けによって NAS Configuration セクションの PIX IP アドレスを追加して下さい。

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

許可を求める Add コマンド:

```
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 は以前に定義されたアクセス リスト 101 と共に前の 3 つの文を取り替えるために割り当てをこの文特色にします。 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+。 ユーザはまたメッセージ「エラー見ます: 拒否される許可」。

```
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 と それ以降では、PIX のアクセス リストを定義して下さい。 サーバのユーザ プロファイルに基づいてユーザー単位でそれらを加えて下さい。 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+ へのアウトバウンド認証および許可は変更されます。 PIX のアクセス リストは設定されます。

注: PIXバージョン 6.0.1 およびそれ以降では、RADIUS を使用すれば、アクセス リストは標準の IETF RADIUS特性でリストを 11 入力することによって（フィルタid）[CSCdt50422] 設定されます。 この例では、アトリビュート 11 はベンダー別 "acl=115" 冗漫をすることの代りに 115 に設定 されます。

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」の表現を認識しません。

Cisco Secure UNIX TACACS+ サーバコンフィギュレーション

```
user = pixa{
```

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

Cisco Secure Windows TACACS+

ユーザがアクセス リストとどこに行くか制御する認証を PIX に追加するために、**シェル/exec をチェックし、アクセスコントロールリストボックスをチェックし、数を記入して下さい（PIX のアクセスリスト番号と一致します）。**

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」ユーザーのニーズ 009\001 AV-Pair を言う Cisco/Radius長方形のボックスのユーザ名、パスワードおよびチェックおよび "acl=115"（ベンダー別）。

出力

プロファイルの "acl=115" のアウトバウンドユーザ「pixa」は認証を受け、承認します。 サーバは PIX に acl=115 の下で通じ、PIX はこれを示します:

```
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 暗黙の deny があるので、（か 99.99.99.2 を除く IP アドレスに）行くことを試みる時ユーザはこれを見ます:

```
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

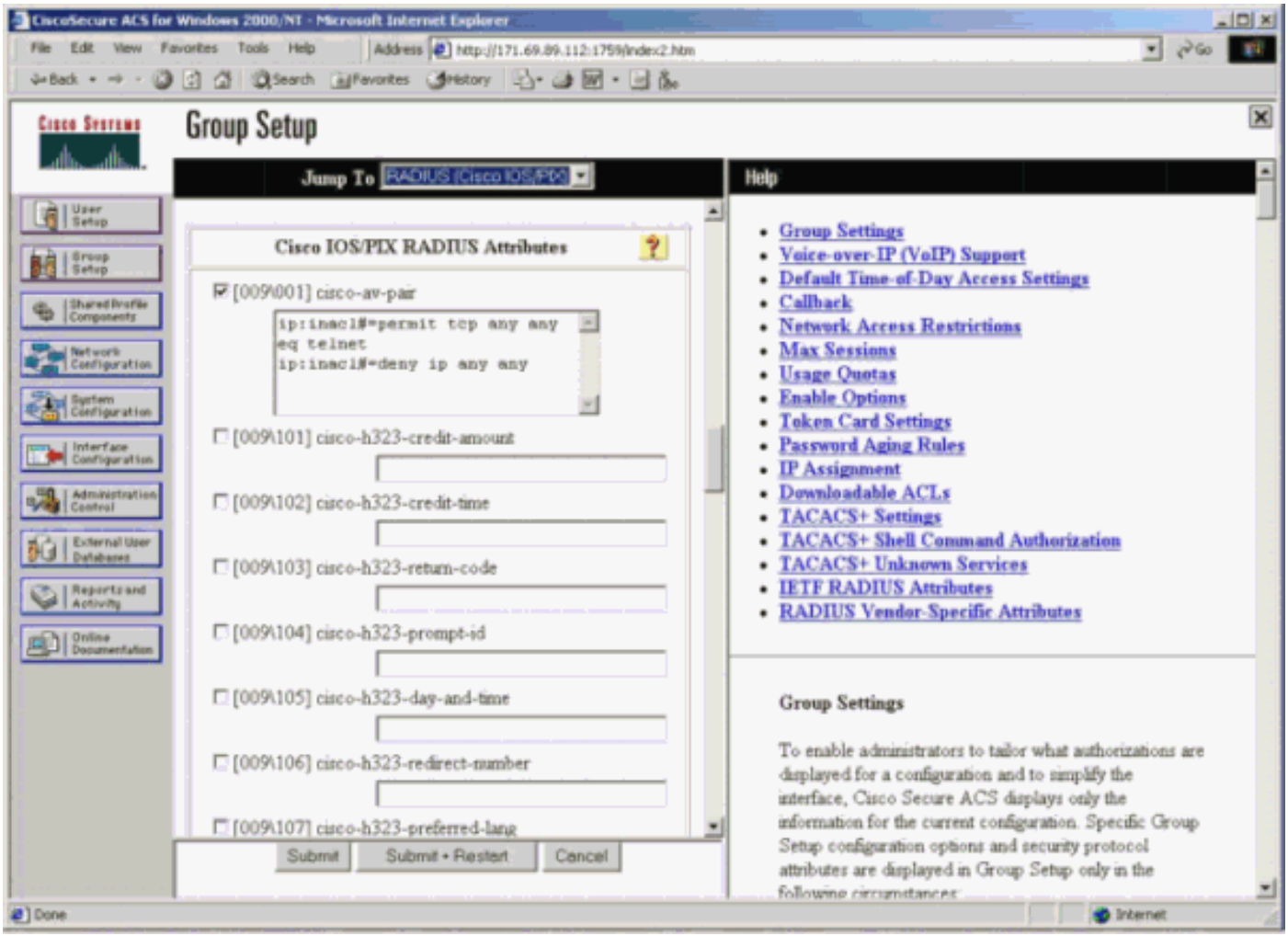
PIXファイアウォールのソフトウェアリリース 6.2 およびそれ以降では、アクセス リストは Access Control Server（ACS）で認証の後で PIX にダウンロードするために定義されます。 これは RADIUSプロトコルをだけ使用します。 アクセス リストを PIX 自体に設定する必要はありません。 グループ テンプレートは複数のユーザに加えられます。

以前のバージョンでは、アクセス リストは PIX で定義されます。 認証に、ACS は PIX にアクセス リスト名前を押しました。 新しい バージョンは ACS が PIX にアクセス リストを直接押すようにします。

注: フェールオーバーが発生する場合、ユーザ認証 表はコピーされなかったユーザ再認証されますではないです。 アクセス リストは再度ダウンロードされます。

ACS のセットアップ

RADIUS（Cisco IOS/PIX）デバイスの種類を『Group Setup』 をクリック し、ユーザアカウントを設定するために選択して下さい。 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て下さい。 この例に示すようにアクセス リストを定義して下さい:



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

- 割り当て Telnet だけ他のトラフィックを拒否し。`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 コマンドからの出力。**`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。**`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)`

- 拒否 Telnet だけ他のトラフィックを割り当て。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 insideshow uauth コマンドからの出力。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: 0:00:00show access-list コマンドからの出力。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

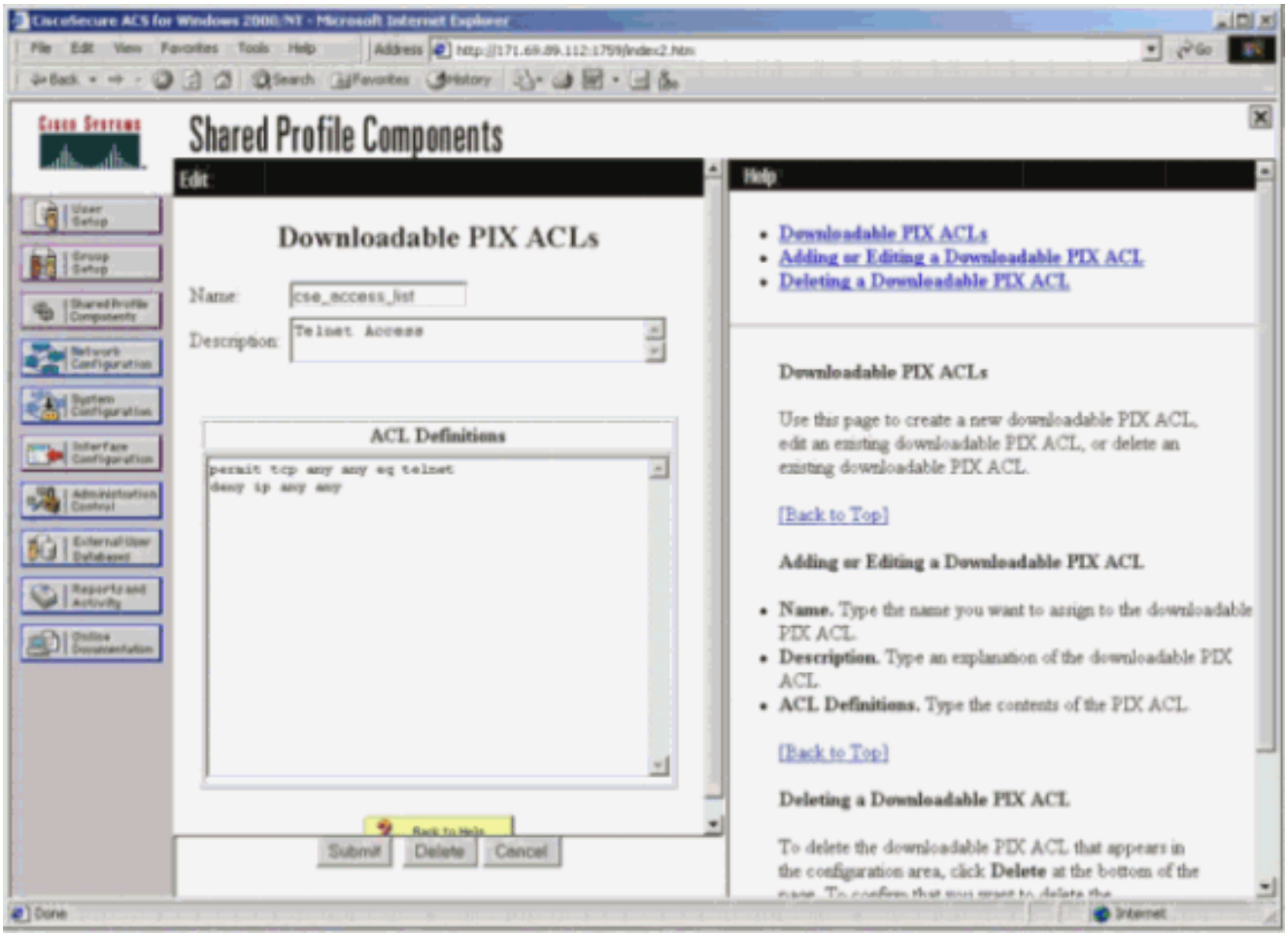
ACS バージョン 3.0 では、共有プロファイル コンポーネントを使用してアクセス リストのテンプレートを作成し、特定のユーザやグループにテンプレート名を定義することができます。 テンプレート名は必要に応じて多くのユーザかグループと使用することができます。 これは各ユーザ向けの同一のアクセス リストを設定する必要を省きます。

注: フェールオーバーが発生する場合、ユーザ認証はセカンダリ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、セッションは支えられます。 ただし、新しい接続は再認証し、アクセス リストは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

共用 プロファイルを使用するときこれらのステップを完了して下さい。

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. 『Shared Profile Components』 をクリック して下さい。 『User-Level Downloadable ACLs』 をクリック して下さい。
4. ダウンロード可能な ACL を定義します。
5. 『Group Setup』 をクリック して下さい。 ダウンロード可能 ACL の下で、先に作成されるアクセス リストに PIX アクセス リストを割り当てて下さい。



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）

- 割り当て Telnet だけ他のトラフィックを拒否し。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**からの出力。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。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
- 拒否 Telnet だけ他のトラフィックを割り当て。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 insideshow uauth コマンドからの出力。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 uauthshow access-list コマンドからの出力。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 設定-会計を追加して下さい

TACACS (AuthInbound=tacacs)

このコマンドを追加して下さい。

aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
またはアクセス リストによって説明されるべきであるものが定義するのに 5.2 で新しい 機能を使用して下さい。

aaa accounting match 101 outside AuthInbound
注: アクセス リスト 101 は個別に定義されます。

RADIUS (AuthOutbound=radius)

このコマンドを追加して下さい。

aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
またはアクセス リストによって説明されるべきであるものが定義するのに 5.2 で新しい 機能を使用して下さい。

aaa accounting match 101 outside AuthOutbound
注: アクセス リスト 101 は個別に定義されます。

注: アカウンティング レコードは PIX 7.0 コードから始まって PIX で管理上のセッションのために作成することができます。

アカウンティングの例

- 99.99.99.2 からの Telnet のための TACACS アカウンティング例外部で 172.18.124.114 内部に (99.99.99.99) 。
```
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
```

- 外部で 99.99.99.2 の外部の（Telnet）および 99.99.99.3 への 172.18.124.114 からの接続のための RADIUSアカウンティングの例中（HTTP）。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

特定ソースか宛先は認証、許可、または説明を必要としないことをこのネットワークでは決定したら、これらのコマンドを発行して下さい。

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: 既に include コマンドを作成しています。

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

または、5.2 の新しい 機能と、たいと思うものを定義して下さい除き。

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き、許可があれば、また許可からボックスを除いて下さい。

Max-sessions and view logged-in users

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 でうまく作動しません。 この例では、別のネットワークコンフィギュレーションは使用されますが、概念は同じです。

ユーザは方法で認証を受ける PIX によって Telnet で接続します。

```
(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
```

「開始する」は記録するが、ことをサーバが見たので「停止」レコードは、この時点で、サーバ「Telnet」ユーザがログオンされることを示しません。 ユーザが認証を最大セッション数がこのユーザ向けのサーバの "1" に (仮定しているサーバが最大セッション数を設定 されれば) (多分別の PC から) 必要とする、およびサポートすれば別の接続を試みれば、接続はサーバによって拒否されます。 ユーザは Telnet か FTPビジネスにターゲットホスト、そして終了の取り掛かります (10 分をそこに使います)。

```
    (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。 ユーザが 171.68.118.100 から 9.9.9.25 PIX によってブラウズするところに HTTPの例はここにあります。

```
(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 にポストされ、停止レコードは 16:35:35 にポストされます。 このダウンロードには 1 秒かかりました (つまり、開始と停止のレコード間は 1 秒未満でした)。 ユーザは Webサイトにログオンされません。 接続はユーザが Webページを読んでいるとき開いていません。 Max-sessions または view logged-in users はここにはたらきません。 これは HTTP の接続時間 (」構築される「と「ティアダウン」間の時間) が余りに短いという理由によります。 「開始」および「停止」レコードは、1 秒以下です。 レコードが殆ど同時に発生するので「開始する」レコードは「停止」レコードなしではありません。 ユーザ認証がより大きい 0 または何かのために設定 されるかどうか今でも各トランザクションのためのサーバに送られる「開始する」および「停止」レコードがあります。 ただし、max-sessions and view logged-in users は HTTP 接続の性質が原因ではたらかせません。

ユーザ インターフェイス

プロンプトユーザを見ます変更して下さい

コマンドがあれば:

auth-prompt prompt PIX515B

それから PIX を通過しているユーザはこのプロンプトを見ます。

```
PIX515B
```

メッセージユーザを見ますカスタマイズして下さい

コマンドを作成すれば:

auth-prompt accept "GOOD_AUTHENTICATION" auth-prompt reject "BAD_AUTHENTICATION"
それからユーザは失敗した/成功したログインの認証状況についてのメッセージを見ます。

```
  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/許可がオンになっている場合、これはユーザー単位で制御されます。 このユーザ プロファイルはタイムアウトを制御するために設定されます (これは TACACS+ フリーウェアサーバにあり、タイムアウトは分にあります) 。

```
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 分の終わりに:

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

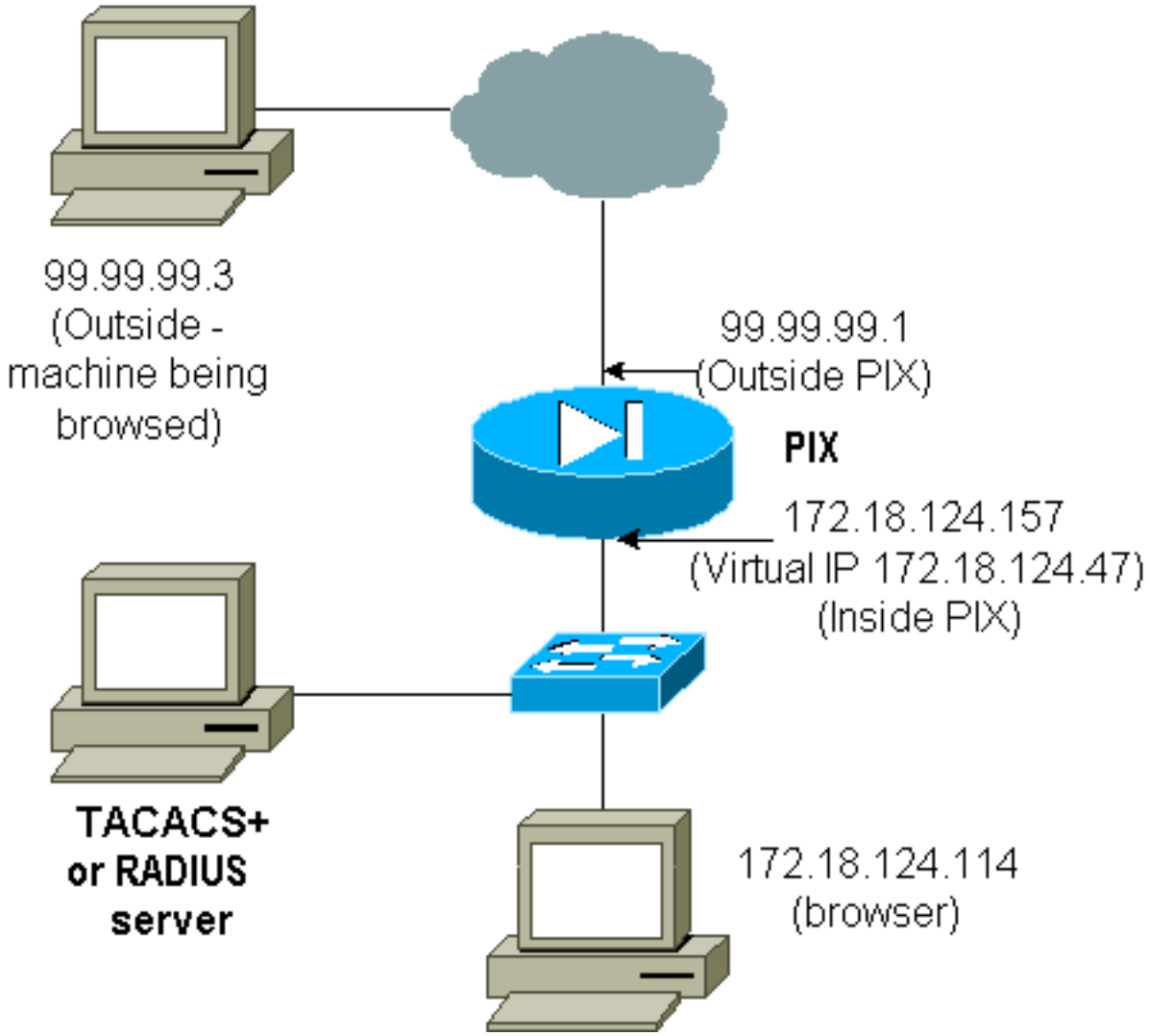
認証が PIX の外部のサイトで、また PIX 自体で必要となる場合、異例なブラウザの動作は時々ブラウザがユーザ名 および パスワードをキャッシュするので、観察されます。

これを、実装する バーチャル HTTP 形式の PIX 設定へ RFC 1918 アドレス (PIX 内部ネットワークのためにインターネットのルート不可能なアドレス、しかし有効およびユニーク) を追加することによって避けるため。

virtual http #.#.#.# <warn>
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。 ドキュメントに示すように、バーチャル HTTP の 0 秒に **timeout uauth コマンド**実行時間を設定

しない で下さい。 HTTP が実際の Web サーバに接続できなくなります。

注: バーチャル HTTP および仮想Telnet IP アドレスは **AAA認証**文に含んでいる必要があります。この例では、0.0.0.0 を規定 することはこれらのアドレスが含まれています。



PIX 設定でこのコマンドを追加して下さい。

```
virtual http 172.18.124.47
```

ユーザは 99.99.99.3 でブラウザをポイントします。 このメッセージは表示する。

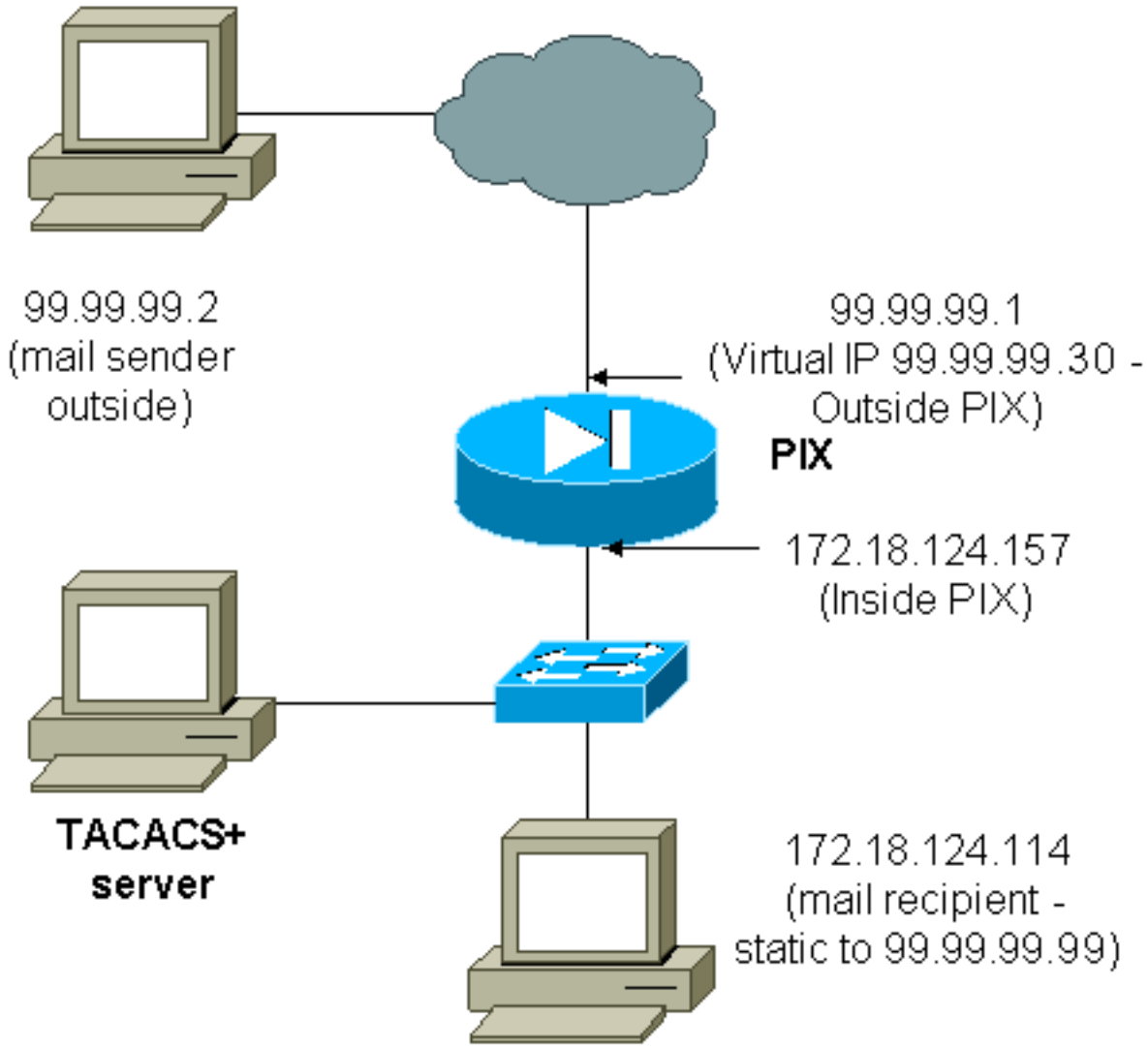
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

認証の後で、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: バーチャル HTTP および仮想Telnet IP アドレスは **AAA認証**文に含んでいる必要があります。この例では、0.0.0.0 を規定 することはこれらのアドレスが含まれています。

仮想 Telnet 受信



それはメールが送信 された 受信であることができるようにウィンドウが表示するので受信 メールを認証するよい考えではないです。 **exclude コマンドを**代りに使用して下さい。 しかし実例の目的で、これらのコマンドは追加されます。

```
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 {
```

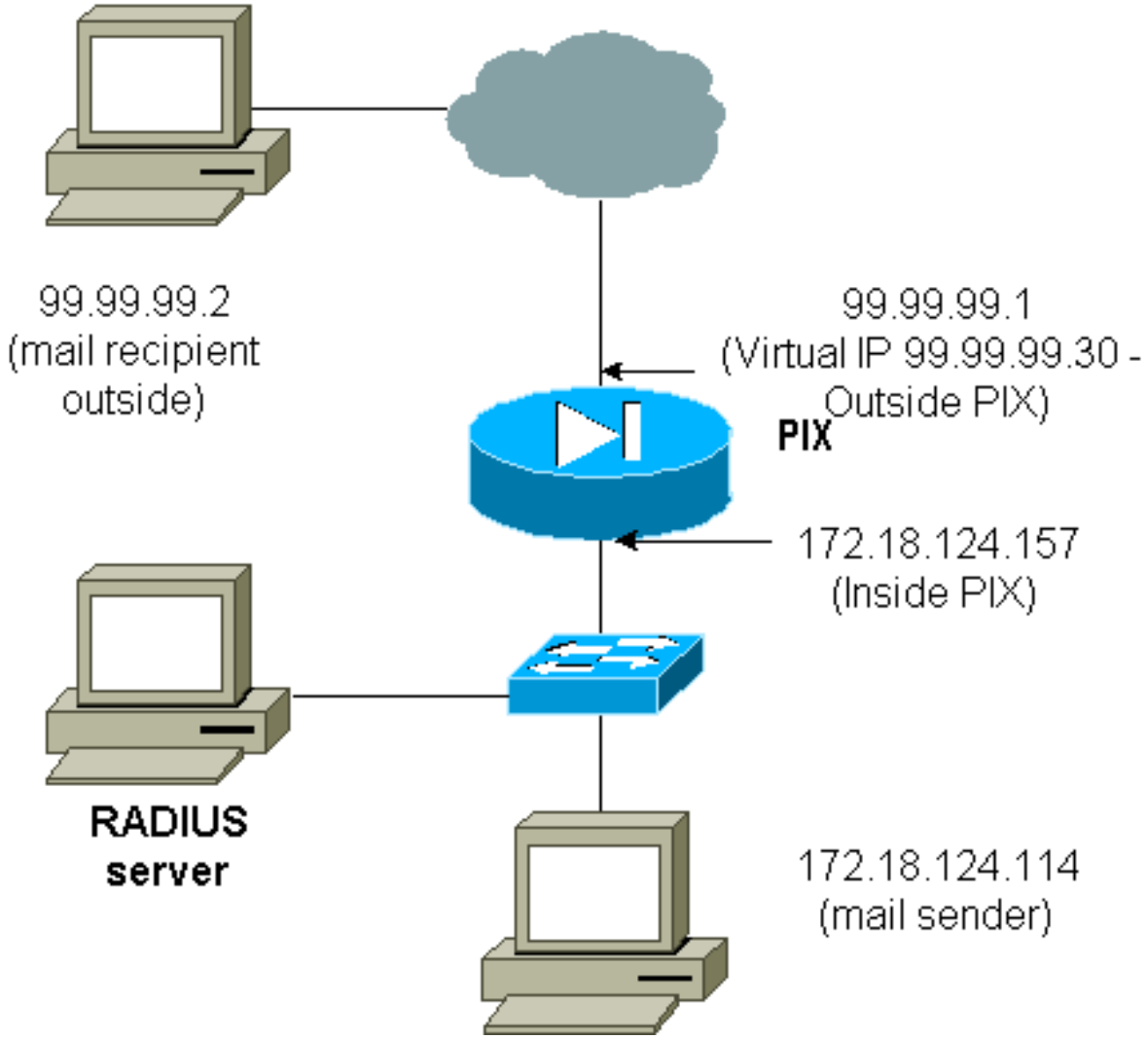
```
  }
  cmd = telnet {
  permit .*
  }
  }
```

認証だけオンになっている場合、ユーザは両方とも IP アドレス 99.99.99.30 に Telnet で認証を受けることの後で受信 メールを送信します。 許可が有効に なる場合、ユーザ「cse」は 99.99.99.30 に Telnet で接続し、TACACS+ username/password を入力します。 Telnet接続ドロップ。 99.99.99.99 へのユーザ「cse」そして送信メール (172.18.124.114) 。 認証はユーザ「pixuser 向けに」成功します。 ただし、PIX が cmd=tcp/25 および cmd-arg=172.18.124.114 のための認証要求を送信 するとき、要求はこの出力に示すように、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



それはメールが送信 された 受信であることができるようにウィンドウが表示するので受信 メールを認証するよい考えではないです。 **exclude コマンドを**代りに使用して下さい。 しかし実例の目的で、これらのコマンドは追加されます。

それはメールが送信 された 発信であることができるようにウィンドウが表示するのでメール 発信を認証するよい考えではないです。 **exclude コマンドを**代りに使用して下さい。 しかし実例の為に、これらのコマンドは追加されます。

```
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.
```

メール送信 99.99.99.30 への内部から外部へ、始動 メールホストのコマンド プロンプトおよび Telnet。 これは行くためにメールのためのホールを開きます。 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。 これはこの例によって説明されます。

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
```

最初の認証の後

```
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
```

第 2 認証

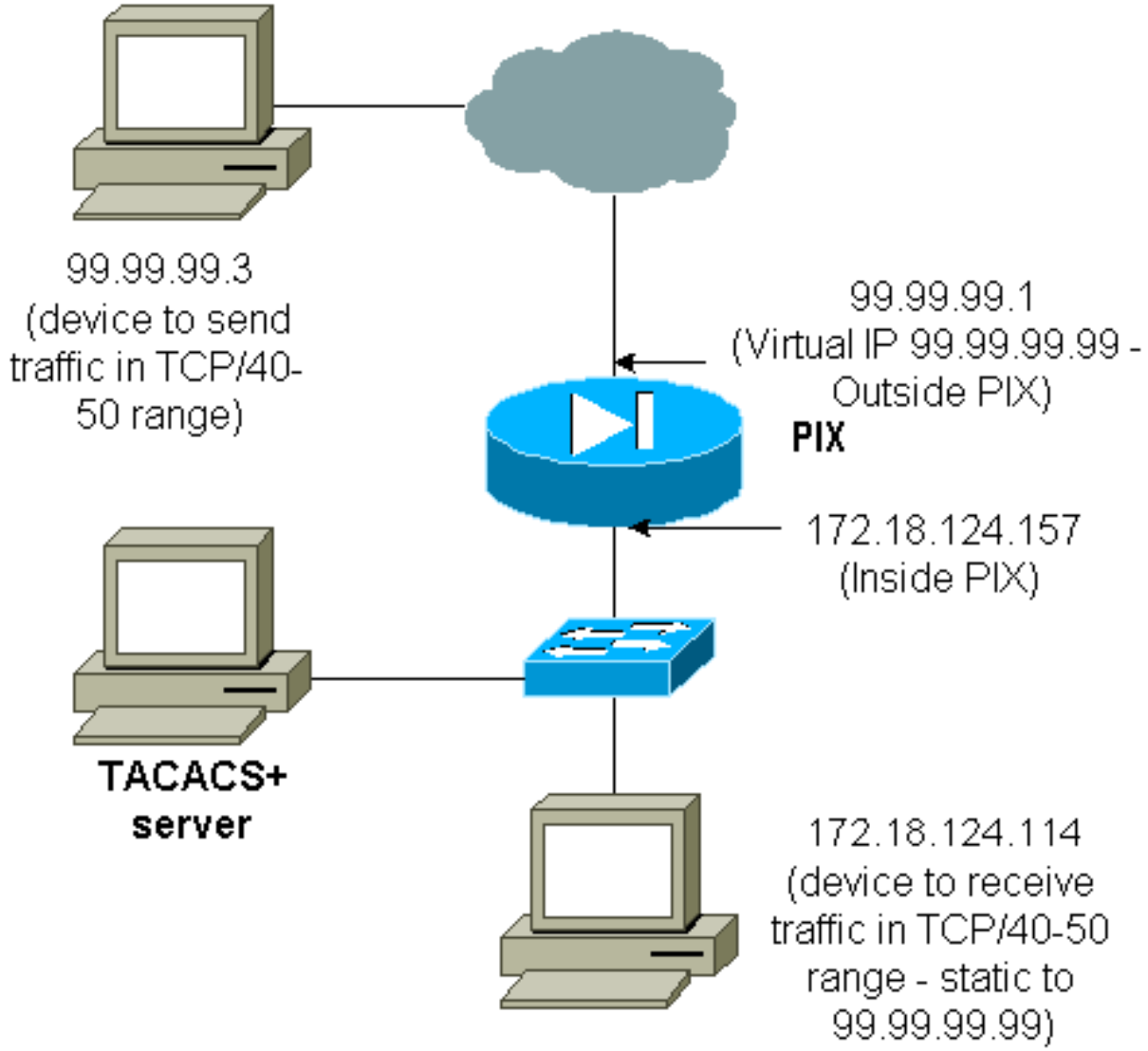
```
   pixfirewall#109001: Auth start for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23 on
interface inside
```

第 2 認証の後

```
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。 仮想Telnet が PIX で設定され、許可がポート範囲のために設定されれば場合、ユーザは仮想Telnet のホールを開きます。 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。 この例はポート範囲のインバウンド認証を示したものです。

```
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 へ Telnet する必要があります。 認証の後で、ユーザが 99.99.99.99 に PIX にポート 40-50 範囲の TCPトラフィックを押通すことを試みるとき（172.18.124.114）、cmd=tcp/40-50 はここに説明されるように cmd-arg=172.18.124.114 の

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

ネットワークの中のホストに TCP/40-50 トラフィックを許可するために仮想Telnet 作業を確かめた後これらのコマンドでこのトラフィックのための会計を追加して下さい。

```
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

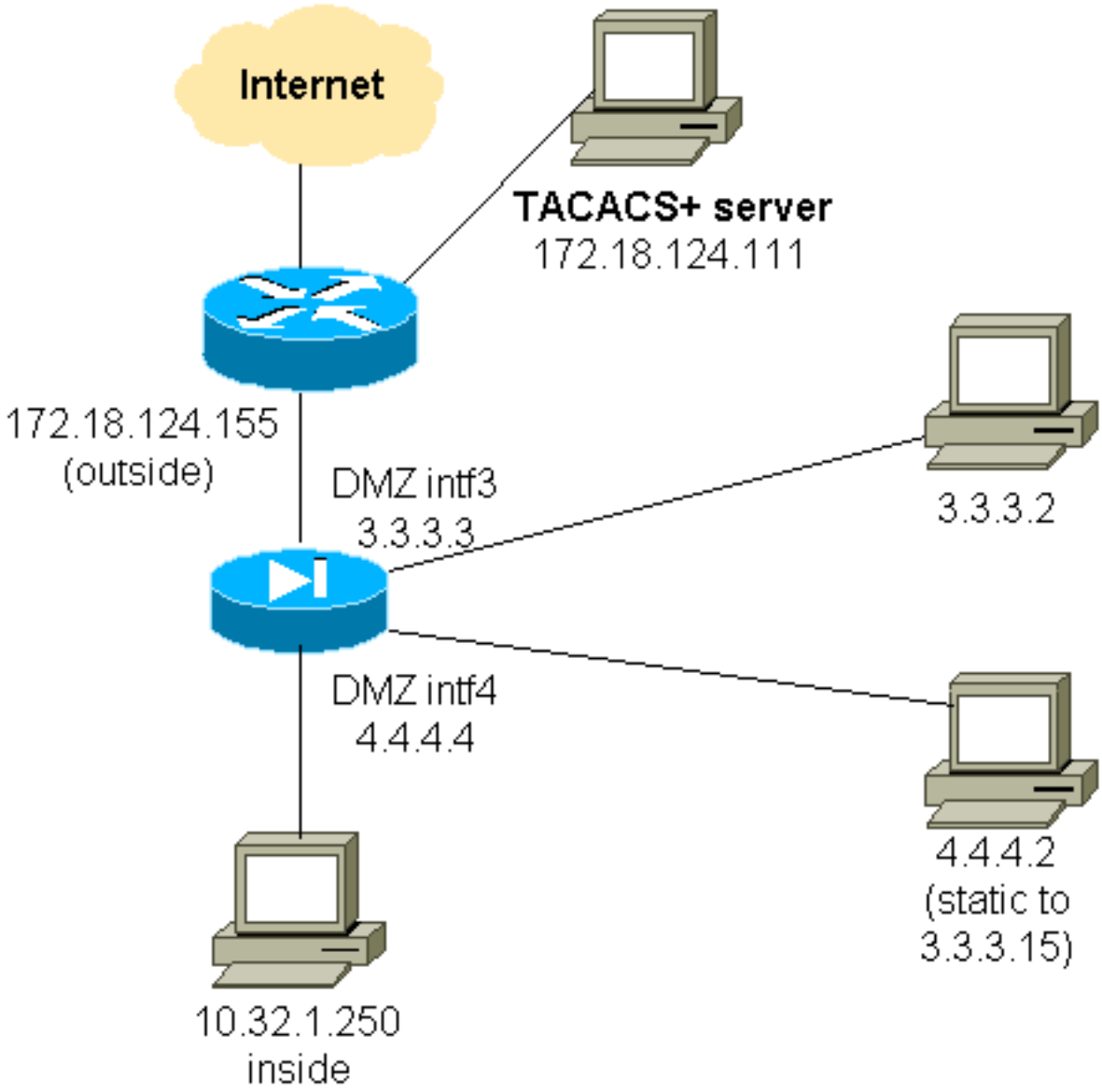
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8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

DMZ での認証

1 つの DMZ インターフェイスから別のものに行くユーザを認証するために、PIX を指定されたインターフェイスのためのトラフィックを認証するように言って下さい。 PIX で、配置はこれのようです:

```
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

ここに示される pix/intf3 と pix/intf4 間の認証する Telnetトラフィック。

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 のサービス リクエストをオープンする場合に収集しておく情報

必要とし、上記のトラブルシューティング の 手順に従った後更にアシスタンスを Cisco TAC のケースをオープンしたいと思う場合 PIXファイアウォールのトラブルシューティングためのこの情報を含むこと確実でであって下さい。

- 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 コマンドで動作した後問題を示す show log コマンドからの出力、またはコンソールキャプチャ（もし可能であれば）

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。 TAC Service Request Tool（登録ユーザのみ）の助けによってそれのアップロードによって情報をケースに添付して下さい。 TAC Service Request Tool にアクセスすることができない場合メッセージの件名にケース番号を記入して attach@cisco.com への電子メールの添付ファイルの情報を送信 して下さい。

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（RFC）
- 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