PIX 5.1.x の設定： TACACS+ および RADIUS

目次

概要

RADIUS および TACACS+ 認証は、FTP、Telnet、および HTTP の接続に対して実行できます。 認証は、一般的ではない他のプロトコルでも、通常は行うことができます。 TACACS+ 認証がサポートされています。 RADIUS 許可はサポートされません。 以前のバージョンと比較すると、PIX 5.1 の認証、許可、アカウンティング（AAA）は、拡張認証（xauth）（Cisco Secure VPN Client 1.1 からの IPSec トンネルの認証）が変更されています。--

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

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

背景説明

認証と認可の比較

- 認証（Authentication）とは、ユーザが何者かを検証することです。
- 認可（Authorization）とは、ユーザが何をできるかを許可することです。
- 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。

内部百人のユーザがあり、ほしいためにこれらのユーザの 6 つにネットワークの外部の FTP、Telnet、または HTTP をされるほしいことを仮定して下さい。 PIX を送信 トラフィックを認証し、すべての 6 人のユーザに TACACS+/RADIUS セキュリティサーバの ID を与えるように言います。 シンプル認証によって、この 6 人のユーザはユーザ名 および パスワードによって認証できますそして出かけます。 他の 94 人のユーザは出かけることができませんでした。 PIX はユーザ名とパスワードの入力をユーザに求め、そのユーザ名とパスワードを TACACS+/RADIUS セキュリティ サーバに渡し、その応答に応じて接続を開くか、拒否します。 この 6 人のユーザは FTP、Telnet、または HTTP をする可能性があります。

しかしこの 6 人のユーザの *1* 人を、「Festus」、ではないです信頼されること仮定して下さい。 するように Festus 外部に FTP を、ない HTTP または Telnet が望みます。 この場合、ユーザが

誰かを確認する認証に加えて、認可（つまりユーザが実行できる操作を許可する機能）を追加する必要があります。 これは TACACS+ とだけ有効です。 PIX に*認証*を追加するとき、PIX はセキュリティサーバに最初に「*コマンド*」が Festus 試みているものを Festus のユーザ名 および パスワードを送信 しましたり、セキュリティサーバにすることを述べている認証要求を送信 します。 きちんとサーバセットアップによって、Festus は「ftp 1.2.3.4」に許可することができましたが、どこでも HTTP または Telnet への能力を否定されます。

認証/認可を有効にしたときにユーザに表示される内容

認証/認可が有効な場合に、内部から外部に（またはその逆方向に）移動しようとすると：

- 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。 ユーザ名のための **local_username@remote_username** およびパスワードのための **local_password@remote_password を**入力することをユーザーのニーズ。 PIX はローカルセキュリティサーバに local_username および local_password、および認証（および許可） PIX/server で正常なら、remote_username を送信 し、remote_password は宛先FTPサーバに向こう通じます。
- HTTP： ウィンドウはユーザ名 および パスワードを要求するブラウザで表示する。 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、再認証が認証サーバにこれを転送する PIX にキャッシュされたユーザ名およびパスワードを撃つブラウザと実際に起こっている可能性が高いといえます。 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、こういうわけで。
- **トンネル**- VPN クライアントおよび Xauth のネットワークに IPSecトラフィックをトンネル伝送するように試みるとき「新しい接続のユーザ認証」のための灰色ボックスは username/password のために表示する。**注:** この認証は Cisco Secure VPN Client 1.1 にはじまってサポートされます。 **Help > About** メニューが show version 2.1.x またはそれ以降場合、これははたらきません。

すべてのシナリオに適用できるセキュリティ サーバ設定

Cisco Secure UNIX TACACSサーバ 設定

このセクションではセキュリティサーバを、設定するための情報が表示されます。

PIX の IP アドレスまたは完全修飾ドメイン名とキーが CSU.cfg ファイルに含まれていることを確認します。

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

user = can_only_do_telnet {
password = clear "telnetonly"
service = shell {
```

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

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

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

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

VPDN ダイヤルインのネットワーク アクセス サーバ（NAS）追加するのに GUI を（NAS）リストに PIX IP アドレスおよびキーを使用して下さい。

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

Cisco Secure ACS for Windows 2.x RADIUS

Cisco Secure ACS for Windows 2.x RADIUS 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 GUI セクションのパスワードを入手して下さい。
2. Group Setup GUI セクションから、**ログインするために**アトリビュート 6（サービス タイプ）をまたは**管理上**設定 して下さい。
3. NAS Configuration セクション GUI の PIX IP アドレスを追加して下さい。

EasyACS TACACS+

EasyACS のドキュメントで、セットアップについて説明されています。

1. グループ セクションで、実行特権を与えるために『Shell exec』 をクリック して下さい。
2. 認証を PIX に追加するために、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。
3. たい各コマンドのために、たとえば、**Telnet を**許可し『Add/Edit new command』 を選択 し

て下さい。
4. 特定のサイトへ Telnet で接続することが許可される場合、形式「割り当て #.#.#.#」の引数部分の IP アドレスを記入して下さい。 さもなければ、Telnet で接続することを割り当てるために『Allow all unlisted arguments』 をクリック して下さい。
5. [Finish editing command] をクリックします。
6. 許可されるコマンド (Telnet、HTTP または FTP) ごとに、それぞれステップ 1 ~ 5 を行います。
7. [NAS Configuration GUI] セクションで PIX IP を追加します。

Cisco Secure 2.x TACACS+

ユーザは User Setup GUI セクションのパスワードを入手します。

1. グループ セクションでは、実行特権を与えるために『Shell exec』 をクリック して下さい。
2. グループセットアップの下部ので PIX へ認証を、追加することは、『Deny unmatched IOS commands』 をクリック します。
3. 割り当てたい各コマンドのために『Add/Edit new command』 を選択 して下さい (たとえば、**Telnet**)。
4. 特定のサイトに Telnet で接続することを割り当てるために形式「割り当て #.#.#.#」の引数部分で IP アドレスを入力して下さい。 あらゆるサイトに Telnet で接続することを割り当てるために『Allow all unlisted arguments』 をクリック して下さい。
5. [Finish editing command] をクリックします。
6. 許可されたコマンドのそれぞれのためのステップ 1 〜 5 を実行して下さい (たとえば、Telnet、HTTP、または FTP)。
7. PIX IP アドレスを追加されます NAS Configuration GUI セクションに確認して下さい。

Livingston RADIUS サーバの設定

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。

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

Merit RADIUS サーバの設定

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。

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

TACACS+ フリーウェア サーバの設定

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

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

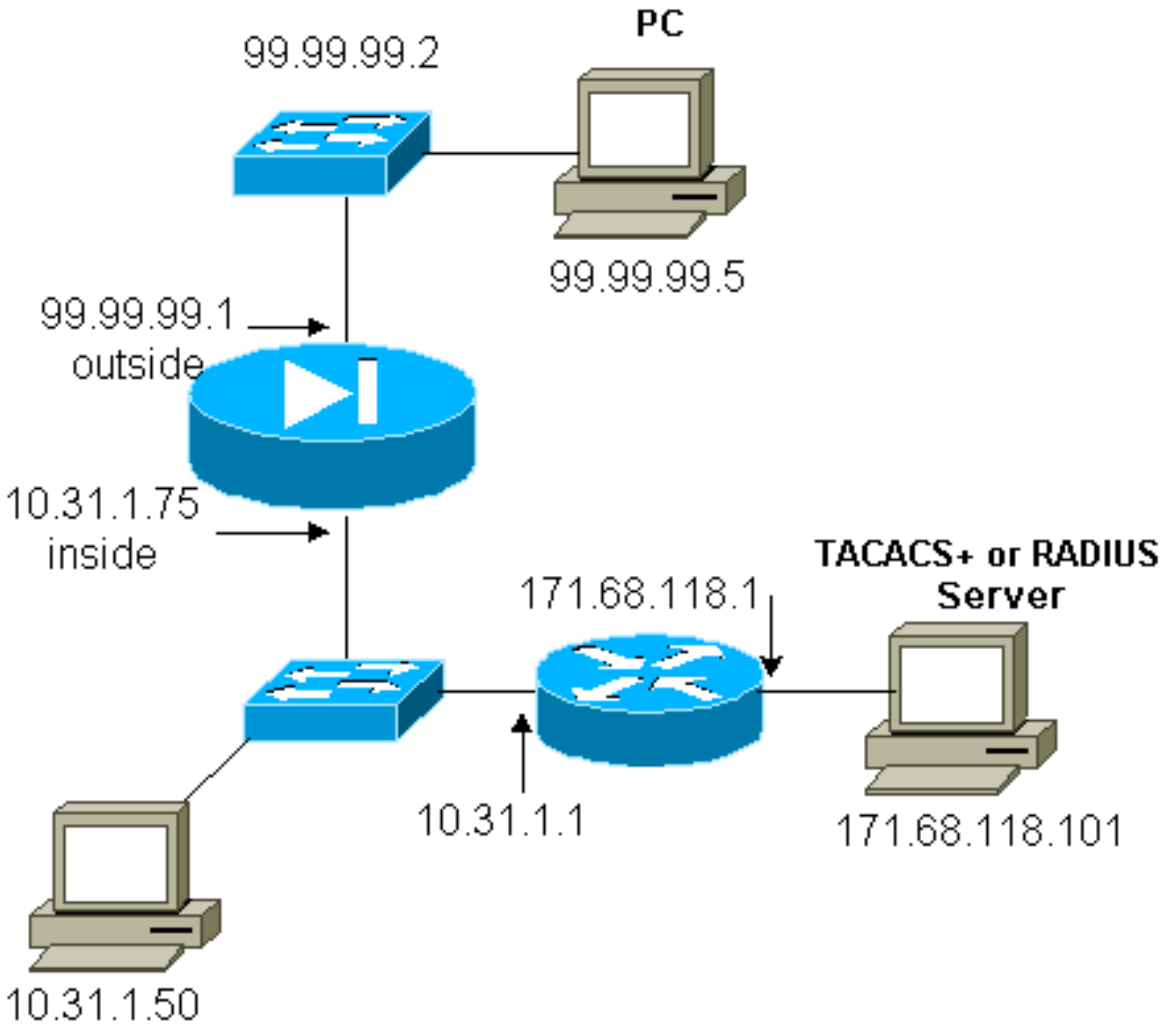
```
user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

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

デバッグの手順

注: 特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- PIX 設定が AAA をことを追加する前に機能していることを確かめて下さい。 認証 および 権限を実施する前にトラフィックを通過できない場合そうその後されません。
- PIX をログオンするイネーブル。Logging console debugging はでロードされたシステム重く使用するべきではありません。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+ か RADIUSサーバ（すべてのサーバにこのオプションがあります）のデバッグを回して下さい。

ネットワーク図



PIX の設定

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby
logging console debugging no logging monitor no logging
buffered no logging trap no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu pix/intf2
1500 ip address outside 99.99.99.1 255.255.255.0 ip
address inside 10.31.1.75 255.255.255.0 ip address
pix/intf2 127.0.0.1 255.255.255.255 no failover failover
timeout 0:00:00 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 failover ip address
pix/intf2 0.0.0.0 arp timeout 14400 global (outside) 1
```

```
99.99.99.7-99.99.99.10 netmask 255.255.255.0 nat
(inside) 1 10.31.1.0 255.255.255.0 0 0 static
(inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0 conduit permit icmp any any conduit
permit tcp any any conduit permit udp any any route
outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 route inside
171.68.120.0 255.255.255.0 10.31.1.1 1 timeout xlate
3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00 timeout uauth 0:05:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.101 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.101 cisco timeout 5 aaa authentication
include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include telnet inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location no snmp-server contact snmp-
server community public no snmp-server enable traps
floodguard enable telnet timeout 5 terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca : end
[OK]
```

PIX からの認証デバッグ例

このセクションはさまざまなシナリオのための認証デバッグのサンプルを示します。

着信

99.99.99.2 の外部ユーザは内部 10.31.1.50 にトラフィックを初期化します（すなわち、99.99.99.99）TACACS によって認証され、（TACACSサーバが 171.68.118.101）含まれている着信 トラフィックは Server リスト「AuthInbound」を使用します。

PIX デバッグ - 良好な認証 - TACACS+

下記の例は良好な認証を用いる PIX デバッグを示します:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX デバッグ - 失敗した認証（ユーザ名またはパスワード）- TACACS+

下記の例は認証不良を用いる PIX デバッグを示します（ユーザ名かパスワード）。 ユーザはこのメッセージに先行している 3 つのユーザネーム/パスワードセットを見ます: `Error:` 。

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX デバッグ-サーバを ping できます無応答- TACACS+

下記の例はサーバが ping 可能である、しかし PIX に話さないことを示します PIX デバッグ。 ユーザはユーザ名を一度見ますが、PIX はパスワードの決して入力を求めません（これは Telnet にあります）。 ユーザは見ます：。

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX デバッグ-サーバ ping することが不可能- TACACS+

下記の例はサーバが ping 可能どこにではないか PIX デバッグに示します。 ユーザはユーザ名を一度見ますが、PIX はパスワードの決して入力を求めません（これは Telnet にあります）。 次の メッセージは表示する: TACACS+ および：（偽サーバは設定交換されました）。

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX デバッグ- 良好な認証 - RADIUS

下記の例は良好な認証を用いる PIX デバッグを示します:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

PIX デバッグ - 失敗した認証（ユーザ名またはパスワード）- RADIUS

下記の例は認証不良を用いる PIX デバッグを示します（ユーザ名かパスワード）。 ユーザはユーザ名 および パスワードについては要求を見、これらを入力する 3 つの機会があります。 エント

リが不成功なとき、次 の メッセージは表示する: Error: 。

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX デバッグ-サーバを、デーモンは ping できます- RADIUS

下記の例はサーバが ping 可能どこにであるが、デーモンはダウンし、PIX と通信しませんか PIX デバッグに示します。 ユーザはユーザ名を、そしてパスワード、RADIUS および見ます: 。 というエラー メッセージが表示されます。

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX デバッグ-サーバかキー/クライアントミスマッチ ping することが不可能- RADIUS

下記の例はサーバがどこに ping 可能ではないか、またはクライアント/キー ミスマッチがあるか PIX デバッグに示します。 ユーザは RADIUS メッセージユーザ名、パスワード、、および見ます: メッセージ偽サーバ 設定交換されました) 。

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

認可の追加

認証を追加することにする場合許可が認証なしで無効であるので、同じ送信元範囲 および 宛先範囲のために許可を求める必要があります。

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

アウトゴーイングトラフィックが RADIUS と認証され、RADIUS認証が無効であるので発信のための認証を追加しないことに注目して下さい。

PIX からの認証および認可のデバッグ例

PIX デバッグ-良好な認証および認証の成功- TACACS+

下記の例は良好な認証および認証の成功の PIX デバッグを示します:

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX デバッグ - 良好な認証、認可に失敗 - TACACS+

下記の例は良好な認証 認証失敗の PIX デバッグを示します。 ここにユーザはまた Message エラーを見ます: 。

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

アカウンティングの追加

TACACS+

aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

出力される TACACS+ フリーウェア:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

出力される Merit RADIUS:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
```

```
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

exclude コマンドの使用

付け加えれば別のホスト外部（99.99.99.100）でネットワークに、このホストは信頼され、次のコマンドで認証 および 権限からそれらを除くことができます:

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
255.255.255.255 AuthInbound
```

最大セッションとログイン ユーザの表示

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。 HTTP では接続の性質上、十分に機能しません。 次の例では、別のネットワーク構成が使用されていますが、概念は同じです。

ユーザが PIX を通して Telnet を実行し、途中で認証を行っています。

```
   171.68.118.100/1200 to 9.9.9.25 /23
  (pix) 109011: Authen Session Start: user
     'cse', Sid 3
  (pix) 109005: Authentication succeeded for user
     'cse' from 171.68.118.100/12 00 to 9.9.9.25/23
  (pix) 302001: Built TCP connection 5 for faddr
     9.9.9.25/23 gaddr 9.9.9.10/12 00
     laddr 171.68.118.100/1200 (cse)
  (server start account) Sun Nov 8 16:31:10 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100 cmd=telnet
```

サーバが開始レコード停止レコードを、この時点で見なかったが、ので、サーバは Telnet ユーザがログオンされることを示します。 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。 HTTPの例は下記にあります:

ユーザが 171.68.118.100 から PIX を経由して 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)。 さて、ユーザが Web ページを読んでいるとき、ユーザは Web サイトにログインして接続はまだ開いているでしょうか? いいえ。 最大セッションまたはログイン ユーザの表示は機能するでしょうか? 答えはいいえ、です。HTTP の接続時間 (「開始」と「終了」の間の時間) が短すぎるため、機能できません。 開始レコード と 停止レコードは計測秒です。 レコードが殆ど同時に発生するので開始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 されるかどうかまだ各トランザクションのためのサーバに送信 された 開始レコード と停止レコードがあります。 ただし、最大セッションとログイン ユーザの表示は、HTTP 接続の性質により機能しません。

PIX 自体での認証および有効化

PIX によって Telnet (および HTTP、FTP) トラフィックを認証する前の説明問題。 認証なしで PIX 作業に Telnet を確認して下さい:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```
それから PIX に Telnet で接続しているユーザを認証するためにコマンドを追加して下さい:

```
aaa authentication telnet console AuthInbound
```
ユーザが PIX に Telnet で接続するとき、Telnetパスワード（**WW**）のためにプロンプト表示されます。 PIX はまた TACACS+ か RADIUSユーザ名およびパスワード要求します。 この場合 AuthInbound Server リストが使用されるので、PIX は TACACS+ ユーザ名 および パスワードを要求します。

次にサーバがダウンしている場合、ユーザ名のための **PIX の**入力によって PIX、およびイネーブルパスワード（**enable password whatever**）にアクセスできます。 次のコマンドを使用すると

```
aaa authentication enable console AuthInbound
```
ユーザは TACACS か RADIUSサーバに送信 される ユーザ名 および パスワードのためにプロンプト表示されます。 この場合 AuthInbound Server リストが使用されるので、PIX は TACACS+ ユーザ名 および パスワードを要求します。

イネーブルのための認証パケットがログオンのための認証パケットと同じであるので、ユーザが TACACS または RADIUS の PIX にログインできる場合、それらは同じ ユーザ名/パスワードで TACACS か RADIUS によって有効に なることができます。 この問題は Cisco バグ ID CSCdm47044 （登録ユーザのみ）を割り当てられました。

サーバがダウンしている場合、PIX（**enable password whatever**）からユーザ名および正常なイネーブルパスワードのための **PIX の**入力によって PIX イネーブル モードにアクセスできます。 enable password whatever が PIX 設定に含まれていない場合は、ユーザ名として pix を入力して Enter キーを押します。 イネーブルパスワードが設定 されるが、知られない場合パスワードを変えるために、パスワード回復 の ディスクは構築される必要があります。

ユーザに表示されるプロンプトの変更

コマンドがあれば:

```
auth-prompt PIX_PIX_PIX
```
PIX を通過しているユーザは次のシーケンスを見ます:

```
PIX_PIX_PIX [at which point one would enter the username]
   Password:[at which point one would enter the password]
```
最終デスティネーションの到達で、ユーザはユーザ名を見ます: そしてパスワード: 宛先ボックスによって表示するプロンプト。 このプロンプトは PIX を経由するユーザにのみ影響し、PIX には影響しません。

注: PIX へのアクセスでアカウンティング レコードが削除されることはありません。

成功/失敗時にユーザに表示されるメッセージのカスタマイズ

youh にコマンドがあれば:

```
auth-prompt accept "GOOD_AUTH" auth-prompt reject "BAD_AUTH"
```

それからユーザは PIX によって失敗した/成功したログインの次のシーケンスを見ます:

```
PIX_PIX_PIX
   Username: asjdkl Password: "BAD_AUTH" "PIX_PIX_PIX" Username: cse Password: "GOOD_AUTH"
```

ユーザごとのアイドル/絶対タイムアウト

この機能は現在はたらかなくて、問題は Cisco バグ ID CSCdp93492 （登録ユーザのみ）を割り当てられました。

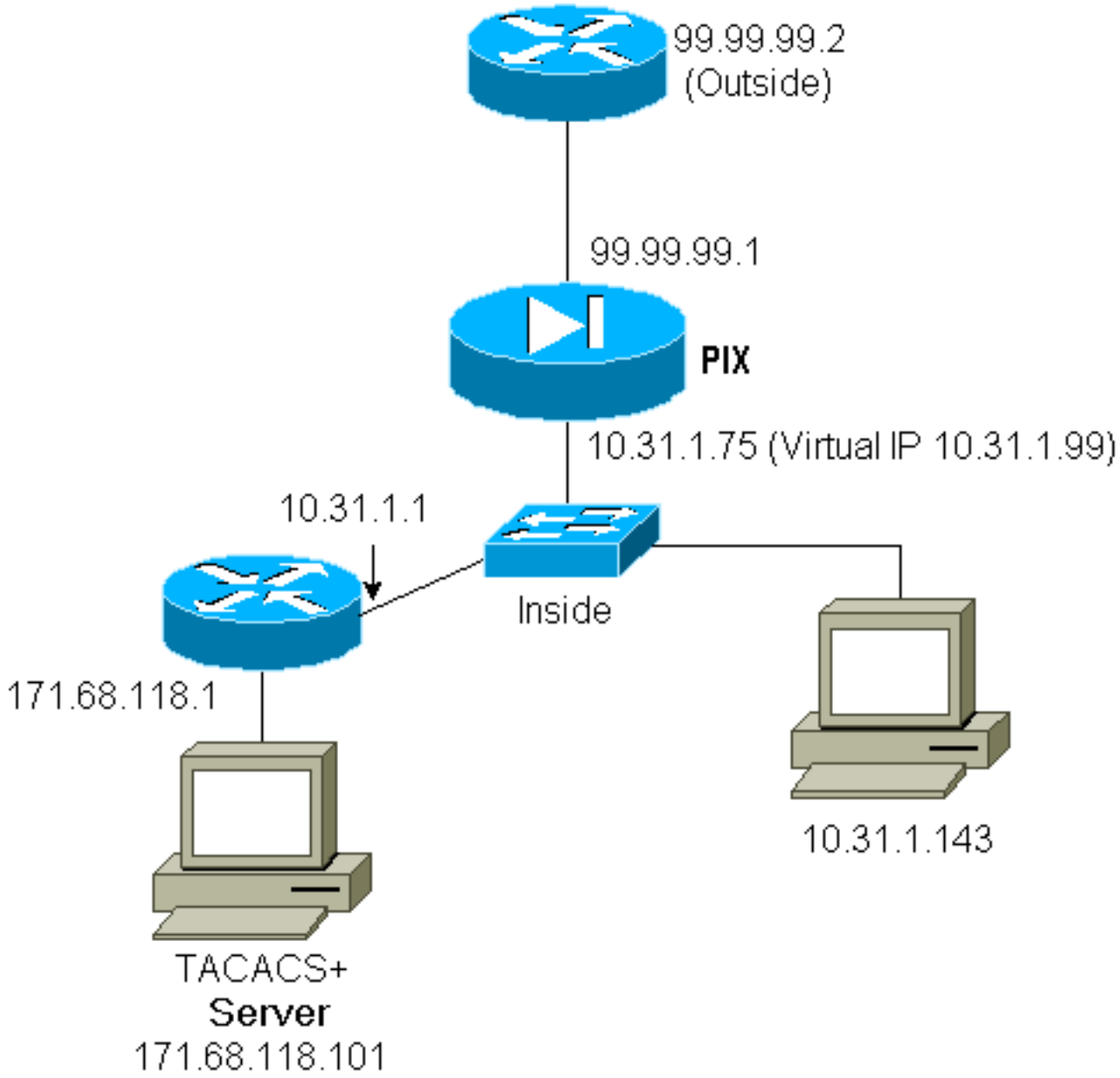
仮想 HTTP

認証が PIX 外部のサイトと同様 PIX そのものでも必要となる場合、ブラウザは異常な動作を見せることがありますが、これ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です。

これを避けるために仮想 HTTP を実装できます。そうするには、次のコマンドを使用して、RFC 1918 アドレス (つまりインターネット上ではルーティングできず、しかも PIX 内部ネットワークでは有効かつ一意のアドレス) を PIX 設定に追加します。

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。 ドキュメントに示しているように、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。

バーチャルHTTP送信の例



仮想 HTTP 送信の PIX 設定：

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 01:00:00 aaa
authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa-server
RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound (inside)
host 171.68.118.101 cisco timeout 5 virtual http 10.31.1.99
```

仮想 Telnet

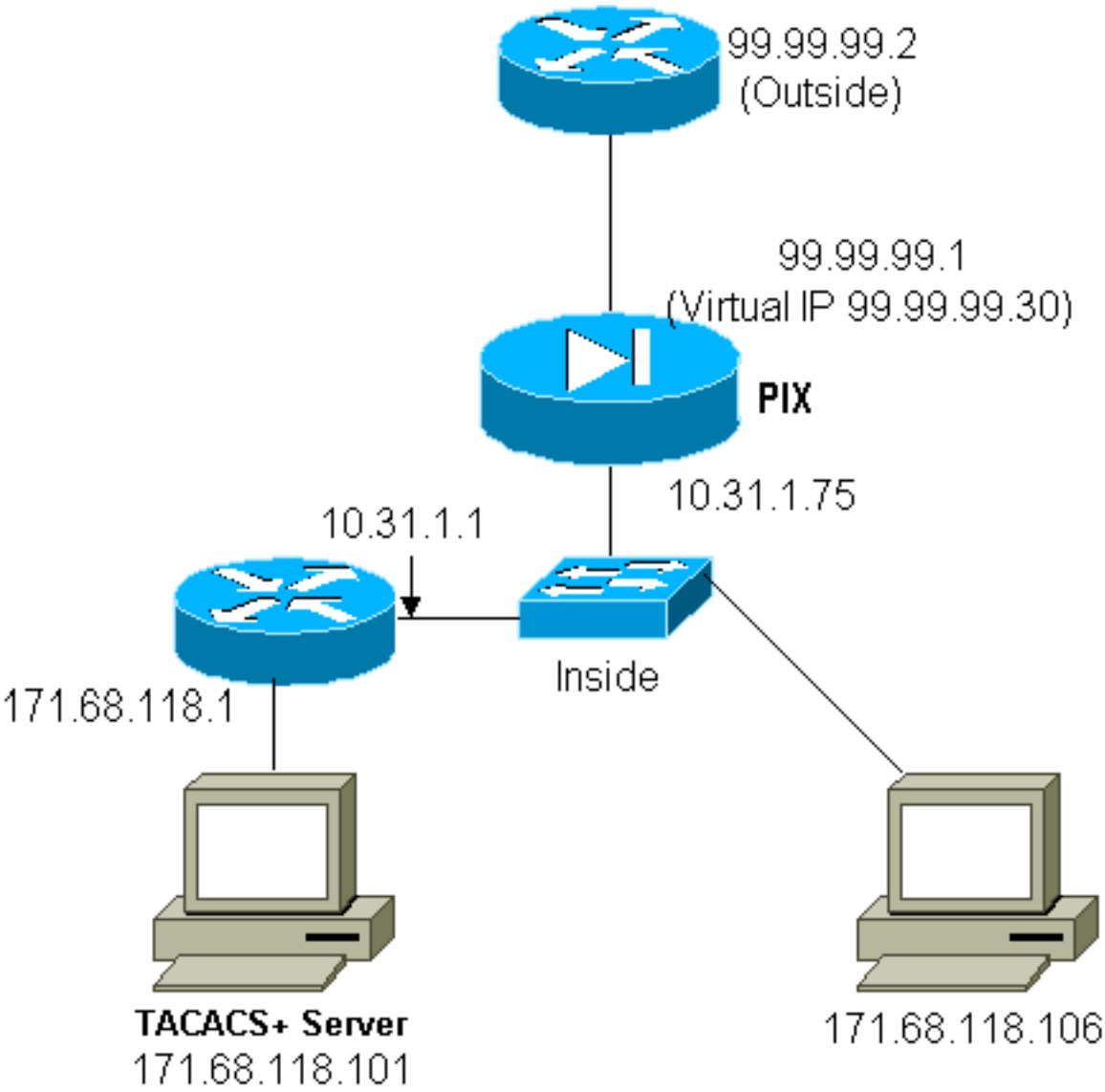
PIX をすべての受信および送信認証するために設定することは可能性のあるですがいくつかのプロトコルが、メールのような、簡単に認証されないのでよい概念ではないです。 PIX によるすべてのトラフィックが認証されているときメール サーバおよびクライアントが PIX によって通信することを試みるとき、認証できないプロトコルのための PIX syslog はメッセージを表示します（以下を参照）：

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

ただし、実際にある種の一般的でないサービスを認証する必要性があればこれは **virtual telnet コマンド**を使用してすることができます。 このコマンドは認証が仮想Telnet IPアドレスに発生するようにします。 この認証の後で、一般的でないサービスのためのトラフィックは実サーバに行くことができます。

この例では、TCPポート 49 トラフィックに外部ホスト 99.99.99.2 から内部ホスト 171.68.118.106 にフローしてほしいです。 このトラフィックが実際に認証可能ではないので、仮想Telnet を設定して下さい。 仮想Telnet に関しては、関連するスタティックがある必要があります。 ここでは、99.99.99.20 および 171.68.118.20 は両方仮想アドレスです。

仮想 Telnet 受信



受信 PIX コンフィギュレーション仮想Telnet

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 static
(inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0 static (inside,outside)
99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.20 eq
telnet any conduit permit tcp host 99.99.99.30 eq tacacs any aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+ aaa-server Incoming (inside) host 171.68.118.101 cisco
timeout 5 aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming virtual telnet
```

99.99.99.20

PIX デバッグ仮想 Telnet 受信

99.99.99.2 のユーザは PIX の 99.99.99.20 アドレスへ Telnet で接続することによって最初に認証を受ける必要があります:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

認証が成功した後、**show uauth** コマンドによって、ユーザの有効時間が表示されます :

```
pixfirewall# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

そして 99.99.99.2 のデバイスが 171.68.118.106 でデバイスに TCP/49 トラフィックを送信 したいと思う時:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

認証は追加することができます:

```
aaa authorization include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

TCP/49 トラフィックが PIX によって試みられる時、PIX がまたサーバに許可クエリを送るように:

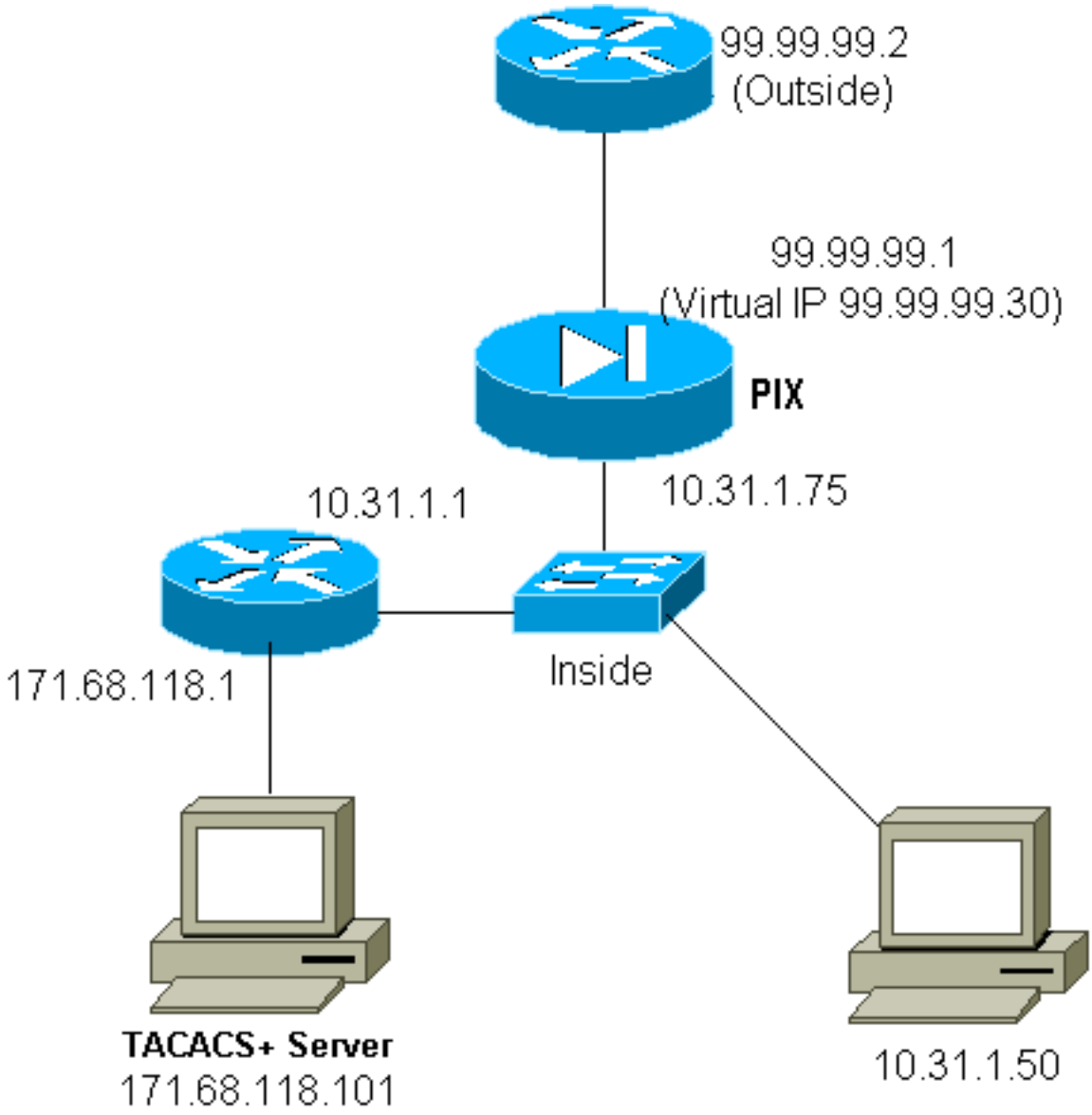
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

TACACS+ サーバで、これはとして見られます:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

仮想 Telnet 送信

発信トラフィックがデフォルトで許可されているため、仮想 Telnet 送信の使用ではスタティックが不要です。 次の例では、10.31.1.50 の内部ユーザは仮想 な 99.99.99.30 に Telnet で接続し、認証を受けます; Telnet接続はすぐに破棄されます。 認証されて、TCPトラフィックは 10.31.1.50 から 99.99.99.2 のサーバへの許可されます:



仮想 Telnet 送信の PIX 設定：

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 0:05:00 absolute aaa-
server RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 171.68.118.101 cisco timeout 5 aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound virtual telnet 99.99.99.30
```

注: これが RADIUS であるので許可がありません。

仮想 Telnet 送信の PIX デバッグ：

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
```

```
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

仮想 Telnet ログアウト

ユーザが仮想Telnet IPアドレスに Telnet で接続するとき、**show uauth コマンドは**ユーザ認証を示します。 ユーザ認証に残っている時間があるときセッションが終了した後ユーザがトラフィックは行くことを防ぎたいと思えば仮想Telnet IPアドレスに再度 Telnet で接続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。

最初認証の後:

```
 pix3# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'pixuser' at 10.31.1.50, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 109005:
Authentication succeeded for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 on interface
inside
```

第 2 認証の後 (すなわち、ホールは閉じる切り替わます) :

```
 pix3# show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

ポートの認可

許可はポート範囲のために許可されます (TCP/30-100 のように) 。 仮想Telnet がポート範囲のための PIX および許可で設定される場合、一度ホールは仮想Telnet と、PIX 問題許可のための TACACS+ サーバへの **tcp/30-100** コマンド開きます:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0 conduit permit tcp
host 99.99.99.75 host 99.99.99.2 static (inside,outside) 99.99.99.75 10.31.1.50 netmask
255.255.255.255 0 0 virtual telnet 99.99.99.75 aaa authentication include any inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound virtual telnet 99.99.99.30
```

TACACS+ フリーウェアサーバコンフィギュレーション:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

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/49 トラフィックを許可するためにはたらいた仮想Telnet を確かめた後これのための会計がほしいと思った、従って付け加えたことを決定しました:

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

これはアカウンティング レコードを切ってもらうことという結果に tcp/49 トラフィックが行くとき終ります (この例は TACACS+ フリーウェアからあります) :

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
```

```
99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
cmd=tcp/49
```

拡大認証(Xauth)

設定例

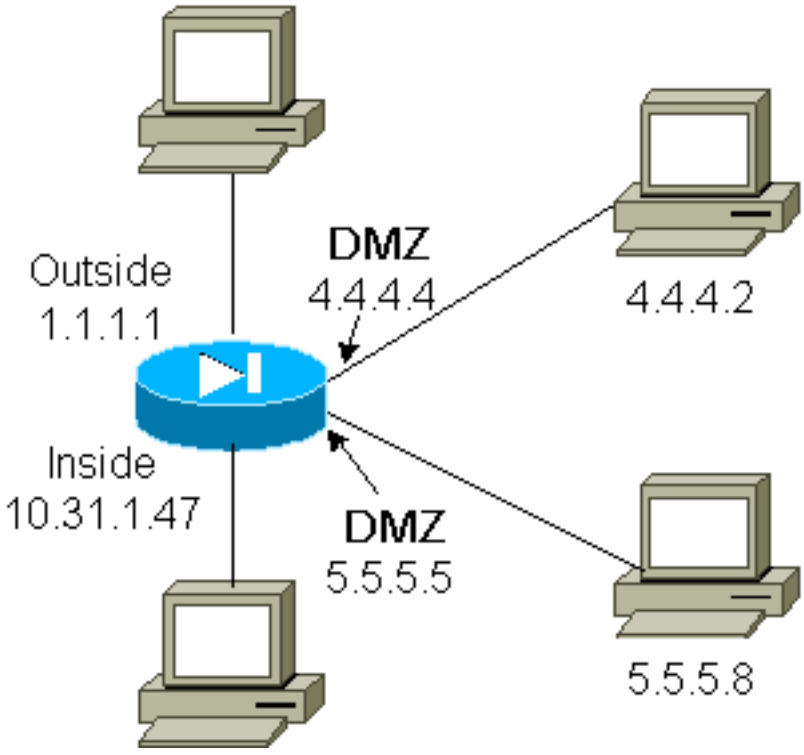
- Xauth を使用する複数の Cisco Secure PIX Firewall インターフェイスで IPSec トンネルを終了させる方法
- 拡張認証を用いる Cisco Secure PIX Firewall と VPN クライアント間の IPSec

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っている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 で配置は次のとおりです:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

ネットワーク図



PIX の設定

pix/intf4 と pix/intf5 間の Telnetトラフィックを認証したいと思います:

```
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 ip address outside 1.1.1.1 255.255.255.0 ip
address inside 10.31.1.47 255.255.255.0 (ip address pix/intf2 127.0.0.1 255.255.255.255 ip
address pix/intf3 127.0.0.1 255.255.255.255) ip address pix/intf4 4.4.4.4 255.255.255.0 ip
address pix/intf5 5.5.5.5 255.255.255.0 static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask
255.255.255.255 0 0 aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa-server TACACS+ protocol tacacs+ aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

xauth アカウンティング

sysopt connection permit-ipsec コマンドが、ない sysopt ipsec pl-compatible コマンド、Xauth で PIX で設定されれば、説明は TCP 接続、しかしない ICMP または UDP のために有効です。

関連情報

- PIX 製品のサポート ページ
- PIX コマンド リファレンス
- RADIUS に関するサポート ページ
- Requests for Comments (RFC)
- Cisco Secure UNIX に関するサポート ページ
- Cisco Secure ACS for Windows に関するサポート ページ
- テクニカルサポート - Cisco Systems