PIX 5.0.x の設定：TACACS+ および RADIUS

内容

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 TCP プロトコルでも、通常は行うことができます。

TACACS+認可がサポートされています。RADIUS 許可はサポートされません。以前のバージョンでのPIX 5.0の認証、許可、アカウンティング(AAA)の変更には、HTTP、FTP、およびTelnet以外のトラフィックに対するAAAアカウンティングが含まれます。

前提条件

要件

このドキュメントに特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内容は、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。

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、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。

たとえば、内部に100人のユーザがあり、これらのユーザのうち6人だけがネットワークの外部でFTP、Telnet、またはHTTPを実行できるようにしたいとします。発信トラフィックを認証し、TACACS+/RADIUSセキュリティサーバ上の6つのユーザIDをすべて付与するようにPIXに指示します。単純な認証を*使用*すると、これら6人のユーザをユーザ名とパスワードで認証してからログアウトできます。他の94人のユーザは外出できません。PIXはユーザにユーザ名/パスワードを求め、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ます。応答に応じて、接続が開かれるか拒否されます。これら6人のユーザは、FTP、Telnet、またはHTTPを実行できます。

一方、これら3人のユーザーの一つである「テリー」は信頼できないと仮定します。Terry に外部 FTP 操作を許可しますが、HTTP と Telnet は許可しないことにします。つまり、承認を追加する*必要があります*。つまり、ユーザが*誰*であるかを認証する以外に、何ができるか*を認可*します。PIXに許可を追加すると、PIXは最初にTerryのユーザ名とパスワードをセキュリティサーバに送信し、次にTerryが何を試みているかをセキュリティサーバに伝える許可要求を送信します"コマンド。サーバを正しく設定すると、Terryは「FTP 1.2.3.4」へのアクセスを許可できますが、任意の場所で「HTTP」または「Telnet」へのアクセスは拒否されます。

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

認証/許可をオンにして内部から外部（またはその逆）に移動しようとすると、次のようになります。

- **Telnet：ユーザ名を求めるプロンプトがユーザに表示された後、パスワードを要求されます**。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：ユーザ名を求める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」をローカルのセキュリティ サーバに送信します。認証（および許可）が PIX/サーバで正常に行われると、「remote_username」と「remote_password」は以降の宛先 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。ブラウザがユーザー名とパスワード**をキャッシュす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のにタイムアウトしない場合、実際にはブラウザによって再認証が行われている傾向があります。キャッシュされたユーザ名とパスワードが PIX へ「送られ」、次に PIX がこれを認証サーバへ転送します。この現象は、PIX の syslog またはサーバのデバッグに示されます。TelnetとFTPが正常に動作しているように見えても、HTTP接続が正常に動作しない場合は、これが理由です。

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サーバの設定

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サーバの設定

グラフィカルユーザインターフェイス(GUI)を使用して、PIX IP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=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
```

Cisco Secure Windows 2.x RADIUS

手順は以下のとおりです。

1. [User Setup GUI]セクションでパスワードを取得します。
2. [Group Setup GUI]セクションで、属性6(Service-Type)を[Login]または[Administrative]に設定します。
3. NAS 構成 GUI で PIX IP を追加します。

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、（exec 権限を付与するために）[Shell exec] をクリックします。
2. PIX に認可を追加するには、グループ設定の下部で [Deny unmatched IOS commands] をクリックします。
3. 許可するコマンド(Telnetなど)ごとに[Add/Edit new command]を選択します。
4. 特定のサイトへの Telnet を許可するには、引数セクションに "permit ##.#.#" という形式の IP を入力します。 すべてのサイトへの Telnet を許可するには、[Allow all unlisted arguments] をクリックします。
5. [Finish editing command] をクリックします。
6. 許可されたコマンド（Telnet、HTTP、FTPなど）ごとに、ステップ1 ~ 5を実行します。
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]セクションでパスワードを取得します。

1. グループ セクションで、（exec 権限を付与するために）[Shell exec] をクリックします。
2. PIX に認可を追加するには、グループ設定の下部で [Deny unmatched IOS commands] をクリックします。
3. 許可するコマンド(Telnetなど)ごとに[Add/Edit new command]を選択します。
4. 特定のサイトへのTelnetを許可する場合は、引数の四角形に「permit IP(s)」と入力します(たとえば、「permit 1.2.3.4」)。 すべてのサイトへの Telnet を許可するには、[Allow all unlisted arguments] をクリックします。
5. [Finish editing command] をクリックします。
6. 許可された各コマンド（Telnet、HTTP、FTPなど）に対して上記の手順を実行します。
7. [NAS Configuration GUI] セクションで PIX IP を追加します。

Livingston RADIUS サーバの設定

PIX IPとキーをclientsファイルに追加します。

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

Merit RADIUS サーバの設定

PIX IP およびキーをクライアント ファイルに追加します。

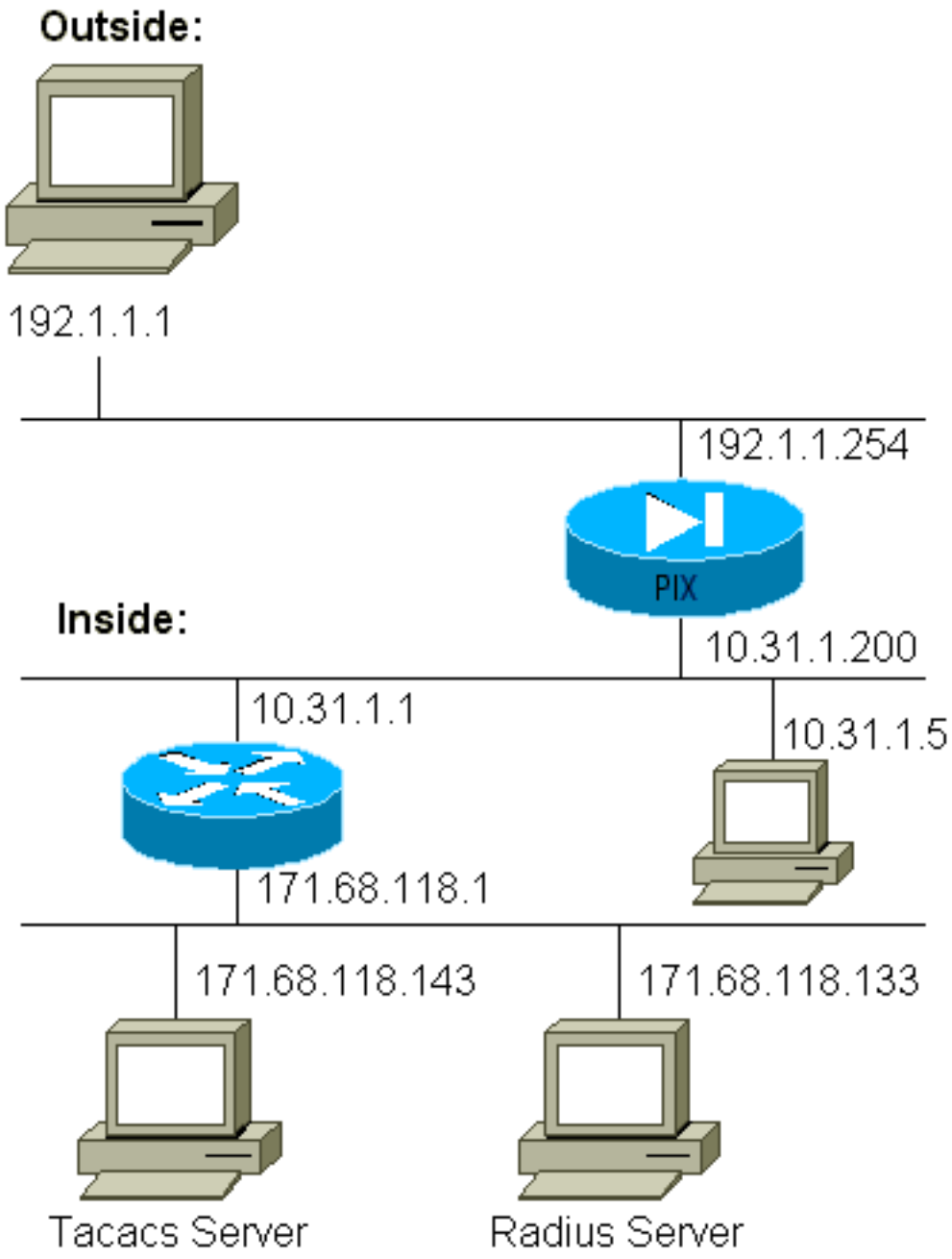
```
adminuser Password="all"
Service-Type = Shell-User
```

```
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

- AAAを追加する前に、PIXの設定が機能していることを確認してください。認証と許可を制定する前にトラフィックを通過させることができないと、結局これらを制定できなくなります。
- PIXでのロギングの有効化logging console debugging コマンドは、負荷の高いシステムでは使用しないでください。logging buffered debugging コマンドは使用できます。**show logging または logging コマンドからの出力を syslog サーバに送信して確認することができます。**
- TACACS+ サーバまたは RADIUS サーバのデバッグがオンになっていることを確認します。このオプションはすべてのサーバで有効です。

ネットワーク図



PIX の設定

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
```

```
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

PIXからの認証デバッグ例PIXからの認証デバッグ例

以下のデバッグ例では、

Outbound

10.31.1.5の内部ユーザが外部192.1.1.1へのトラフィックを開始し、TACACS+を介して認証されます。発信トラフィックは、RADIUSサーバ171.68.118.133を含むサーバリスト「AuthOutbound」を使用します。

Inbound

192.1.1.1の外部ユーザが内部10.31.1.5(192.1.1.30)へのトラフィックを開始し、TACACSを介して認証されます。着信トラフィックは、TACACSサーバ171.68.118.143を含むサーバリスト「AuthInbound」を使用します)。

PIX デバッグ - 良好な認証 - TACACS+

次の例は、認証が正常なPIXデバッグを示しています。

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

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

次の例は、不正な認証（ユーザ名またはパスワード）を使用したPIXのデバッグを示しています。 ユーザには4つのユーザ名/パスワードセットと「Error:ま。

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

PIXデバッグ – サーバにpingを実行できる、応答がない – TACACS+

次の例は、サーバにpingを実行できるが、PIXと通信していないPIXのデバッグを示しています。ユーザ名は一度表示されますが、PIXはパスワードの入力を求めません（これはTelnet上にあります）。 「Error:。

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
```

```
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

PIXデバッグ – サーバにpingできない – TACACS+

この例では、サーバにpingできないPIXのデバッグを示します。ユーザにはユーザ名が一度表示されますが、PIXはパスワードを要求しません（これはTelnet上にあります）。 次のメッセージが表示されます。"Timeout to TACACS+ server" および "Error:`Max number of tries exceeded`」（設定で偽のサーバを交換しました）。

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

PIX デバッグ- 良好な認証 - RADIUS

次の例は、認証が正常なPIXデバッグを示しています。

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (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

次の例は、不正な認証（ユーザ名またはパスワード）を使用したPIXのデバッグを示しています。 ユーザ名とパスワードの入力要求がユーザに表示されます。ユーザには、ユーザ名/パスワードの入力に成功するための3つの機会があります。

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Pingデバッグ – Can Ping Server, Daemon Down - RADIUS

次の例は、サーバにping可能だが、デーモンがダウンし、PIXと通信しないPIXデバッグを示しています。ユーザには、ユーザ名、パスワード、「RADIUS server failed」および「Error:。

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

PIXデバッグ – サーバにpingできない、またはキー/クライアントの不一致 – RADIUS

この例では、PIXのデバッグについて説明します。このデバッグでは、サーバにpingできない場合や、キー/クライアントの不一致が見られます。ユーザ名、パスワード、および「Timeout to RADIUS server」および「Error:Max number of tries exceeded」（偽のサーバが設定でスワップされました）。

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

認可の追加

認可を追加する場合は、同じ送信元と宛先の範囲に対する認可が必要です（認証がないと認可は有効ではないため）。

```
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
```

発信トラフィックはRADIUSで認証され、RADIUS認可が無効であるため、「発信」に認可は追加されないことに注意してください。

PIX からの認証および認可のデバッグ例

PIXデバッグ – 正常な認証と正常な認可 – TACACS+

次の例は、正常な認証と正常な認可を使用したPIXデバッグを示しています。

```
109011: Authen Session Start: user 'pixuser', Sid 8
```

```
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

PIX デバッグ - 良好な認証、認可に失敗 - TACACS+

次の例は、認証は正常であるが、認証に失敗したPIXデバッグを示しています。また、ここではユーザに "Error:Authorization Denied」

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

アカウンティングの追加

TACACS+

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

アカウンティングがオンかオフかにかかわらず、デバッグは同じように表示されます。ただし、「Built」の時点では、「start」アカウンティングレコードが送信されます。「ティアダウン」時には、「停止」アカウンティングレコードが送信されます。

TACACS+アカウンティングレコードは次の出力のようになります（これらはCisco Secure NTの出力であり、カンマ区切り形式です）。

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

アカウンティングがオンまたはオフの場合、デバッグは同じように表示されます。ただし、「Built」の時点では、「start」アカウンティングレコードが送信されます。「ティアダウン」時には、「停止」アカウンティングレコードが送信されます。

RADIUSアカウンティングレコードは次の出力のようになります(これらはCisco Secure UNIXのものです。Cisco Secure NTでは、代わりにカンマで区切られる場合があります)。

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

except コマンドの使用

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、次のような出力を行うことができます。

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

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、認証からボックスを除外する必要があります。

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「start」レコードが生成されるが、「stop」レコードがない場合、TACACS+またはRADIUSサーバは、そのユーザがまだログインしていると見なします（PIXを介したセッションがある）。

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。この出力例では、異なるネットワーク設定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 171.68.118.100/12 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
```

サーバは「開始」レコードを認識したが、（この時点では）停止レコードを認識していないため、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ビジネスを続行し、終了します（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（毎回認証）の場合も、0 より大きい（認証を 1 回行い uauth 期間中は再度行わない）場合でも、アクセスされたすべてのサイトでアカウンティング レコードが削除されます。

HTTP は、そのプロトコルの性質によって、動作が異なります。次に、HTTPの出力例を示します。

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。

16:35:34に投稿された開始レコードと16:35:35に投稿された停止レコード。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 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たままで、接続が継続しているでしょうか?いいえ。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すか。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」および「停止」レコードは、1 秒以下です。レコードは実質的に同じ時点

で発生するため、「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送信される「開始」および「停止」レコードはまだ存在します。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。

PIX 自体での認証および有効化

前の説明では、PIXを介したTelnet（およびHTTP、FTP）トラフィックの認証について説明しました。PIXへのTelnetが認証*なし*で動作することを確認します。

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

ユーザがPIXにTelnetすると、Telnetパスワード(**ww**)の入力を求められます。 次に、PIXはTACACS+（この場合は「AuthInbound」サーバリストが使用されるため）またはRADIUSユーザ名とパスワードも要求します。サーバがダウンしている場合は、ユーザ名として**pixを入力して**、アクセス用にイネーブルパスワード(**enable password *whatever)を入力することでPIXにアクセスできます**。

次のコマンドを使用します。

```
aaa authentication enable console AuthInbound
```

ユーザにユーザ名とパスワードの入力を求めるプロンプトが表示され、TACACSに送信されます（「AuthInbound」サーバリストが使用されているため、要求はTACACSサーバに送信されます）。enable用の認証パケットはログイン用の認証パケットと同じであるため、ユーザがTACACSまたはRADIUSを使用してPIXにログインできる場合、TACACSまたはRADIUSを介して同じユーザ名/パスワードでイネーブルにできます。この問題には、Cisco Bug ID CSCdm47044(登録ユーザ専用)が割り当てられています。

シリアル コンソールの認証

aaa authentication serial console AuthInboundコマンド*は、PIXのシリアルコンソールにアクセスするために認証検証を必要とします。*

ユーザがコンソールから設定コマンドを実行すると、syslogメッセージがカットされます（PIXがデバッグレベルでsyslogをsyslogホストに送信するように設定されていると仮定）。 syslogサーバに表示される内容の例を次に示します。

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

ユーザに表示されるプロンプトの変更

auth-prompt PIX_PIX_PIXコマンドを使用すると、PIXを通過するユーザに次のシーケンスが表示されます。

```
PIX_PIX_PIX [at which point one would enter the username]
Password:[at which point one would enter the password]
```

最終宛先ボックスに到着すると、「Username:」および「Password:」プロンプトが表示されます。このプロンプトは、PIXを通過するユーザーにのみ影響を与え、PIXを通過するユーザには影響しません。

注：PIXにアクセスするためのアカウンティングレコードは削除されません。

成功/失敗時にユーザが表示するメッセージのカスタマイズ

次のコマンドがある場合：

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

ユーザは、PIXを経由したログインの失敗または成功で、次のシーケンスを確認できます。

```
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

uauth のアイドル タイムアウトと絶対タイムアウトを、ユーザごとに TACACS+ サーバから送信できます。ネットワーク内のすべてのユーザが同じ「timeout uauth」を使用する場合は、これを実装しないでください。ただし、ユーザごとに異なるUAUTHが必要な場合は、読み続けます。

この例では、**timeout uauth 3:00:00コマンド**を使用します。一度認証を行うと、3時間の再認証は不要になります。ただし、このプロファイルを使用してユーザを設定し、PIXでTACACS AAA認証を有効にしている場合、ユーザプロファイルのアイドルタイムアウトと絶対タイムアウトは、そのユーザのPIXのタイムアウトuauthを上書きします。これは、PIXを経由するTelnetセッションが、アイドル/絶対タイムアウト後に切断されることを意味するものではありません。再認証が実行されるかどうかを制御するだけです。

このプロファイルは、TACACS+フリーウェアから取得したものです。

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

```
}
}
```
認証後、PIXでshow uauthコマンドを実行します。

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```
ユーザが 1 分間アイドル状態になった後、PIX のデバッグは次のようになります。

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```
ユーザは、同じターゲットホストまたは別のホストに戻ったときに再認証する必要があります。

仮想 HTTP

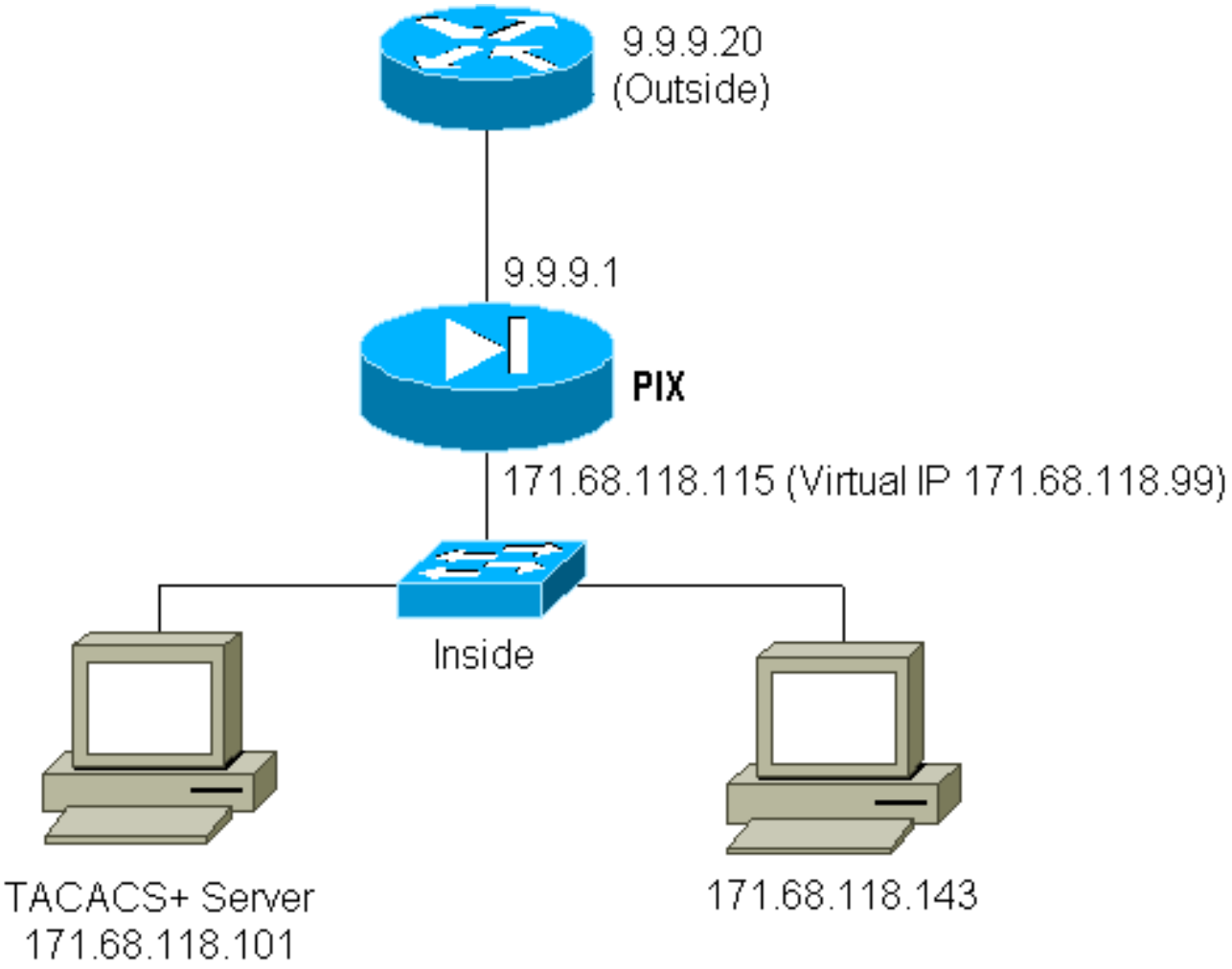
PIX 自体に加えて PIX 外部のサイトでも認証が必要な場合、ブラウザが異常な動作を見せることがあります。これはブラウザがユーザ名とパスワードをキャッシュするためです。

これを避けるためには、次のコマンドを使用して、PIX設定にRFC 1918 アドレス (インターネット上でルーティング不可能であるが、PIX内部ネットワークに対して有効で一意なアドレス) を追加することで、仮想HTTPを実装できます。

```
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。

仮想HTTPアウトバウンド図



仮想HTTPアウトバウンドのPIX設定

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

仮想 Telnet

すべての着信および発信トラフィックを認証するようにPIXを設定することは可能ですが、設定することは推奨できません。これは、「mail」などの一部のプロトコルが簡単に認証されないためです。メールサーバとクライアントが、PIXを経由するすべてのトラフィックが認証されるときにPIXを経由して通信しようとすると、PIX syslog for unauthenticatable protocolsに次のようなメッセージが表示されます。

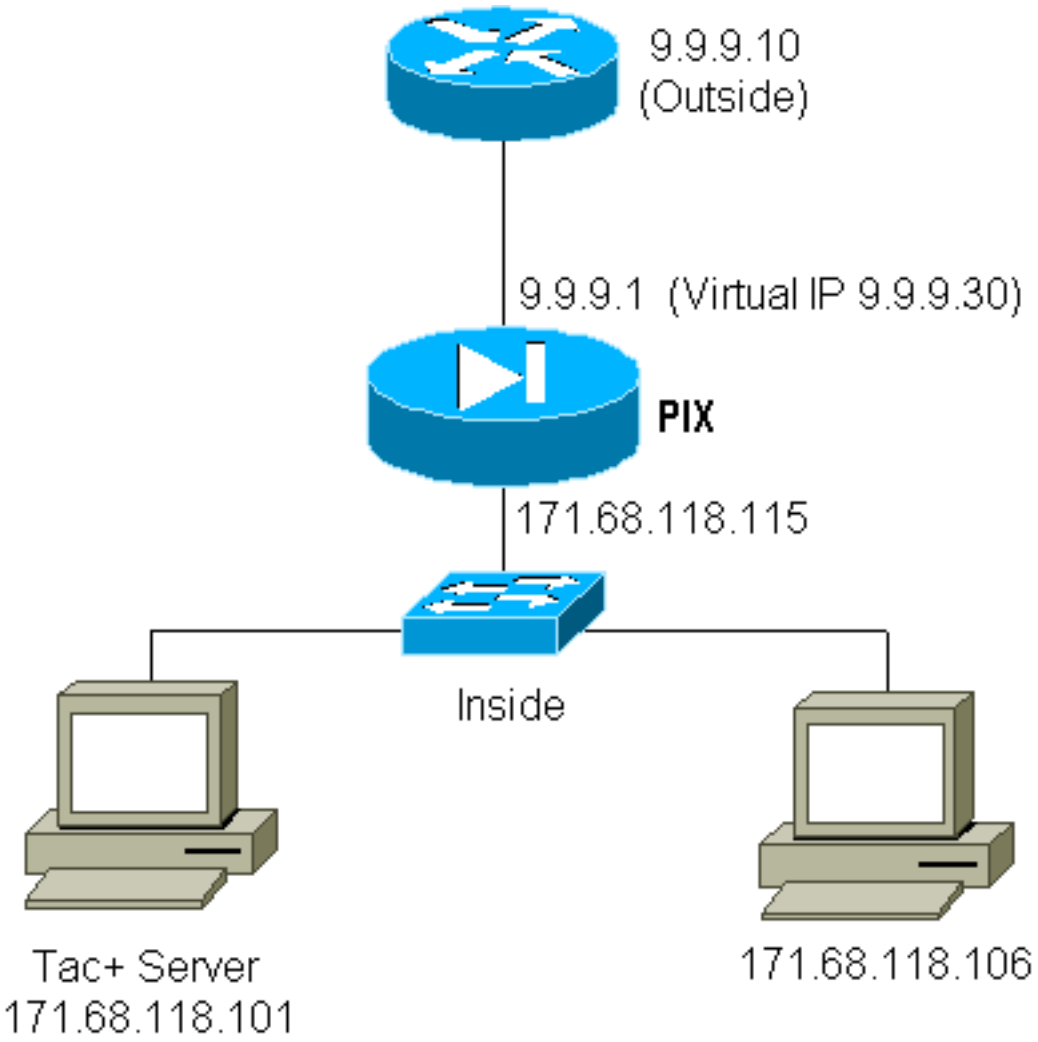
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

メールなどの一部のサービスは、認証できるほど十分に対話的ではありません。1 つの解決策として、認証/認可用に **except コマンドを使用できます (メール サーバ/クライアントの送信元/宛先を除くすべてを認証します) 。**

ある種の異常なサービスを認証する必要がある場合は、**virtual telnetコマンドを使用して行えます**。このコマンドにより、仮想 Telnet IP での認証が可能になります。この認証後、異常なサービスのトラフィックは実サーバに送られます。

この例では、TCPポート49トラフィックを外部ホスト9.9.9.10から内部ホスト171.68.118.106に流します。このトラフィックは実際には認証可能ではないため、仮想Telnetを設定します。インバウンド仮想Telnetの場合、関連付けられたスタティックが必要です。ここでは、9.9.9.20と171.68.118.20の両方が仮想アドレスです。

仮想Telnetインバウンド図



仮想TelnetインバウンドのPIX設定

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
```

```
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

TACACS+サーバユーザ設定の仮想Telnetインバウンド

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

PIXデバッグ仮想Telnetインバウンド

9.9.9.10 のユーザは PIX 上の 9.9.9.20 アドレスに Telnet することで、まず認証される必要があります。

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

認証が成功した後、**show uauth**コマンドを実行すると、ユーザに「時間がメーターに表示されます」と表示されます。

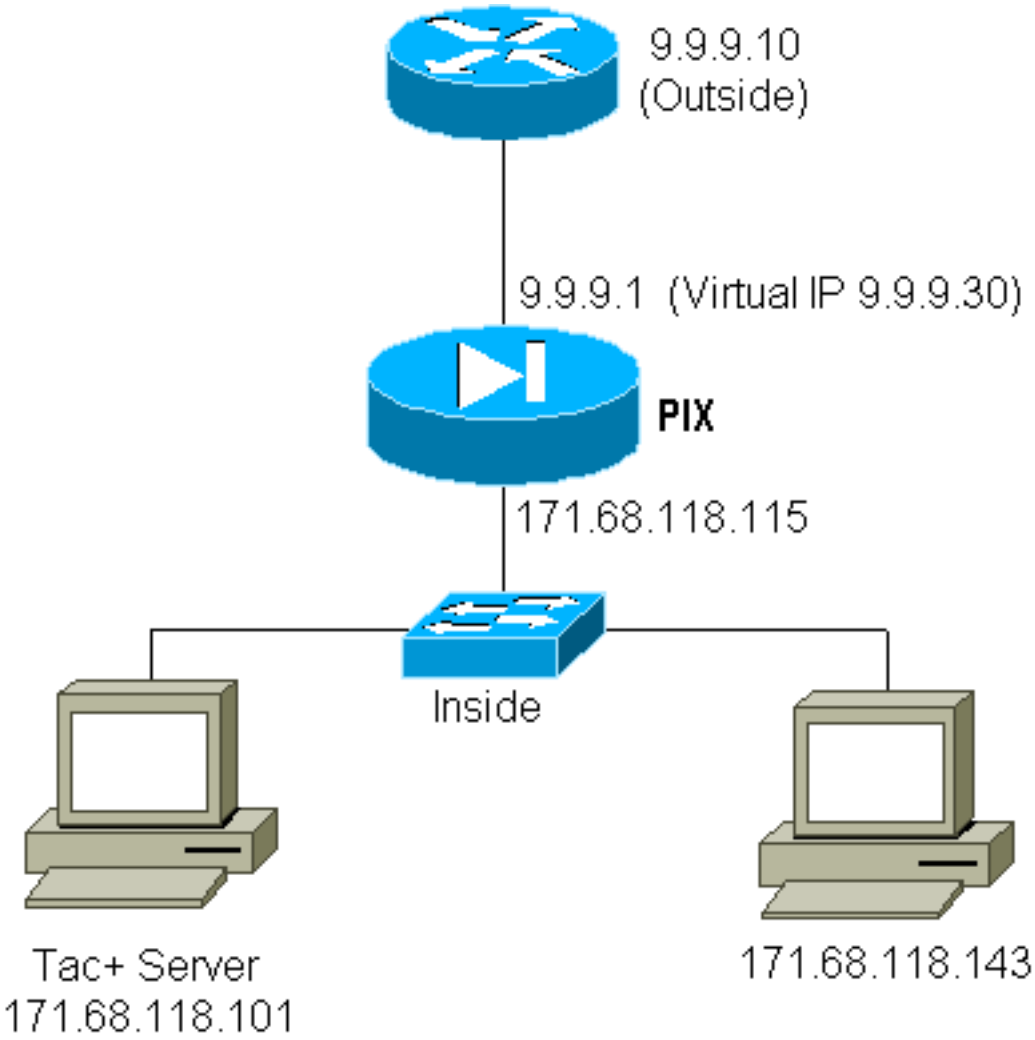
```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

ここでは、9.9.9.10のデバイスが171.68.118.106のデバイスにTCP/49トラフィックを送信しようとしています。

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

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。この例では、171.68.118.143の内部ユーザが仮想9.9.9.30にTelnetし、認証します。Telnet 接続はただちにドロップされます。認証されると、171.68.118.143 から 9.9.9.10 のサーバへの TCP トラフィックが許可されます。



仮想Telnet送信のPIX設定

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

仮想Telnet発信のPIXデバッグ

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', Sid 25
 109005: Authentication succeeded for user 'timeout_143' from
    171.68.118.143/1536 to 9. 9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
```

```
   bytes 625 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
   9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
   bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

仮想 Telnet ログアウト

ユーザが仮想Telnet IPにTelnetすると、**show uauth**コマンドでuauthが表示されます。

ユーザが（uauthに時間が残っている場合に）セッションが終了した後にトラフィックが通過するのを防止するには、ユーザは仮想Telnet IP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。

ポートの認可

ポート範囲に対して認可を要求することができます。この例では、すべての発信に対して認証が必要でしたが、TCPポート23 ~ 49に対しては許可だけが必要でした。

PIX の設定

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

171.68.118.143から9.9.9.10へのTelnetが実行されると、Telnetポート23が23 ~ 49の範囲にあるため、認証と認可が行われました。

171.68.118.143から9.9.9.10へのHTTPセッションが完了しても、認証は必要ですが、80が23 ~ 49の範囲にないため、PIXはTACACS+サーバにHTTPを許可するように要求しません。

TACACS+ フリーウェア サーバの設定

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

PIXは「`cmd=tcp/23-49`」と「`cmd-arg=9.9.9.10`」をTACACS+サーバに送信することに注意してください。

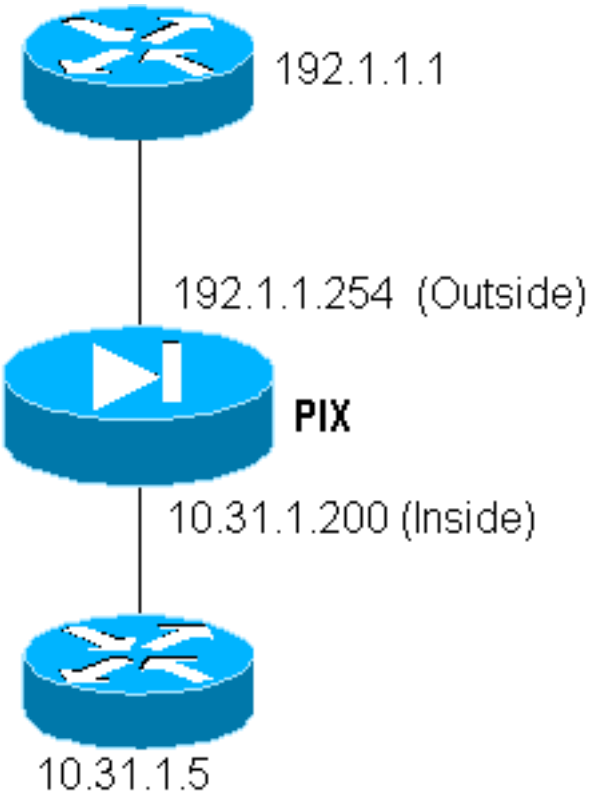
PIXのデバッグ

```
109001: Auth start for user '???' from 171.68.118.143/1051
   to 9.9.9.10/23
109011: Authen Session Start: user 'telnetrange', Sid 0
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1051 to 9. 9.9.10/23
```

```
109011: Authen Session Start: user 'telnetrange', Sid 0
109007: Authorization permitted for user 'telnetrange'
   from 171.68.118.143/1051 to 9.9 .9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23
   gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105
   to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110
   to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', Sid 1
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1110 to 9. 9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

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

PIXソフトウェアバージョン5.0では、トラフィックアカウンティング機能が変更されています。認証が完了すると、HTTP、FTP、およびTelnet以外のトラフィックのアカウンティングレコードを削除できます。



外部ルータ(192.1.1.1)から内部ルータ(10.31.1.5)にファイルをTFTPコピーするには、仮想Telnetを追加してTFTPプロセスの穴を開けます。

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

次に、192.1.1.1の外部ルータから仮想IP 192.1.1.30にTelnetし、UDPがPIXを通過できるようにする仮想アドレスに認証します。次の例では、**copy tftp flashプロセス**がoutsideからinsideに開始されています。

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

PIX上の**copy tftp flash**（このIOSコピー中に3つあった）ごとに、アカウンティングレコードがカットアンド送信されます。Cisco Secure WindowsでのTACACSレコードの例を次に示します)。

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

関連情報

- PIX コマンド リファレンス
- PIX 製品のサポートページ