PIX、TACACS+ および RADIUS の設定例：4.4.x

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。PIX 4.4.1 認証、認可、およびアカウンティング（AAA）では、旧バージョンから次の点が変更されています：AAA サーバ グループ、フェールオーバー、有効化とシリアル コンソール アクセスのための認証、プロンプト メッセージの受け入れ/拒否が変更されています。

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。

ネットワーク内に 100 ユーザが存在し、そのうち 6 ユーザのみに、ネットワーク外部で FTP、Telnet、HTTP を使用することを許可するとします。発信トラフィックを認証するよう PIX に指示し、TACACS+/RADIUS セキュリティ サーバ上で 6 ユーザ全員に ID を与えます。単純な認証では、この 6 ユーザがユーザ名とパスワードを使って認証された後、外部にアクセスできます。残りの 94 ユーザは外部にアクセスできません。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 ユーザは FTP、Telnet、または HTTP を使用できます。

ここで、3 ユーザのうちの 1 人 Terry を信頼できないとします。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。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。PIX に認可を追加すると、PIX は最初に Terry のユーザ名とパスワードをセキュリティ サーバに送信します。次に、Terry が実行しようとしている「コマンド」をセキュリティ サーバに伝える認可リクエストを送信します。サーバが正しくセットアップされていれば、Terry は「FTP 1.2.3.4」を許可されますが、あらゆる HTTP および Telnet 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、内側から外側、または外側から内側に移動しようとすると、次のように表示されます。

- **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：ウィンドウがブラウザに表示されて、ユーザ名とパスワードが要求されます。認証（および許可）が正常に行われると、宛先の Web サイトおよびその先に到達します。**ブラウザによってユーザ名とパスワードがキャッシュされる**ことに注意してください。PIX が HTTP 接続をタイムアウトする必要がある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 や FTP では「正常に」機能しているようでも HTTP 接続ではそうでない場合は、これが原因です。

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

CiscoSecure 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 .*
}
}
}
```

CiscoSecure UNIX RADIUS サーバの設定

高度なグラフィカル ユーザ インターフェイス (GUI) を使用して、ネットワーク アクセス サーバ (NAS) のリストに PIX IP とキーを追加します。

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

CiscoSecure NT 2.x RADIUS

次に示す手順を実行します。

1. [User Setup] セクションでパスワードを入手します。
2. [Group Setup GUI] セクションから、属性 6 (サービス タイプ) 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. 認可 (authorization) を PIX に追加するには、グループ設定の下部で [Deny unmatched IOS commands] をクリックします。
3. 許可する各コマンド (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. 許可されるコマンド (Telnet、HTTP、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。

CiscoSecure 2.x TACACS+

ユーザは GUI の [User setup] セクションでパスワードを入手します。

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. 許可する各コマンド（Telnet など）ごとに [Add/Edit] を選択します。
4. 特定のサイトへの Telnet を許可するには、引数の四角形に許可 IP を入力します（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。

Livingston 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"
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
```

TACACS+ フリーウェア サーバの設定

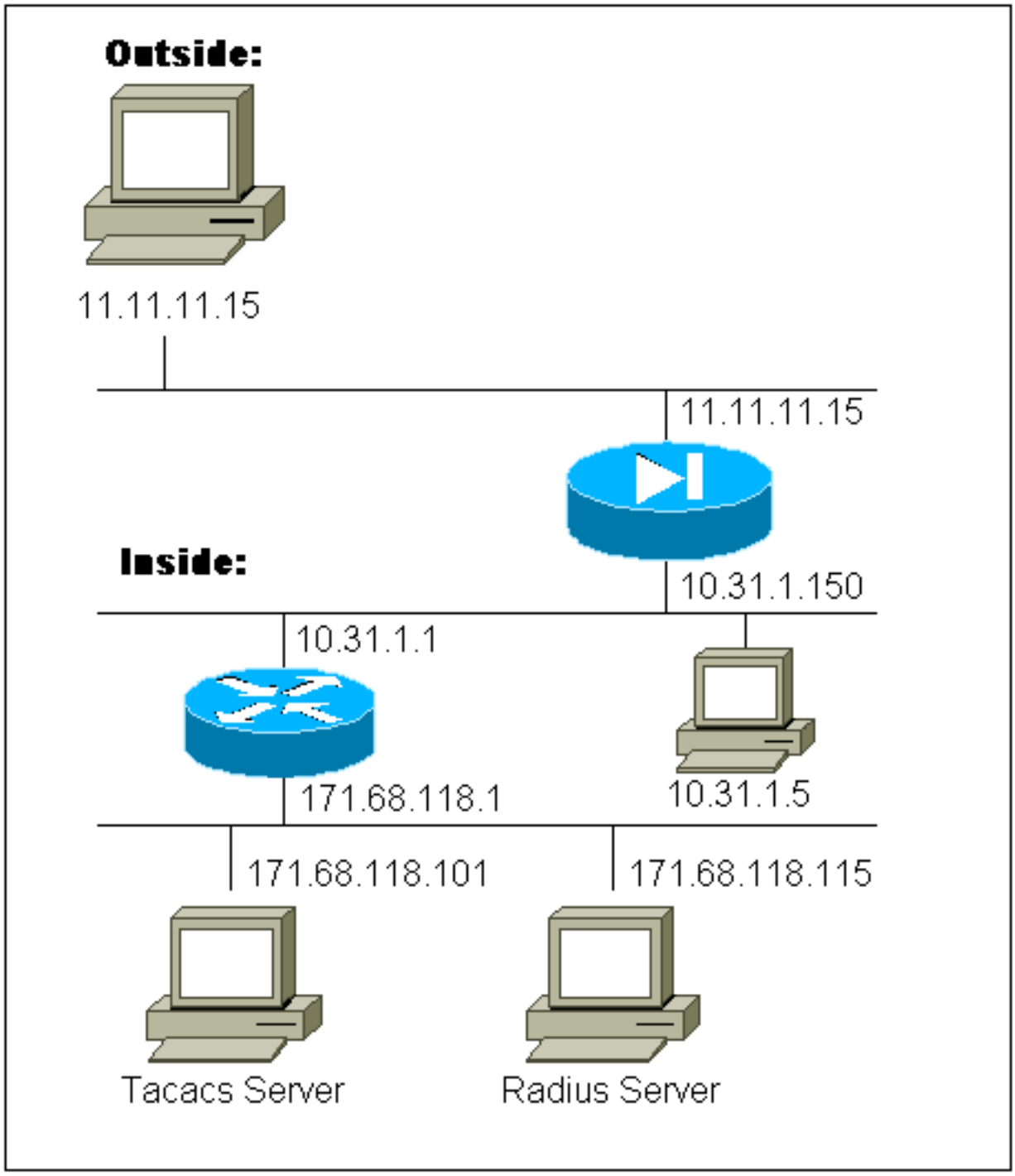
```
key = "cisco"

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

- 認証、認可、およびアカウンティング（AAA）を追加する前に、PIX 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 の口ギングを有効にします：負荷の高いシステムでは **logging console debugging コマンドを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
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 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
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

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 11.11.11.15 への外部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、TACACS サーバ 171.68.118.101 を含むサーバ リスト（発信）を使用します。

Inbound

11.11.11.15 の外部ユーザが 10.31.1.5（11.11.11.22）への内部トラフィックを開始し、RADIUS を介して認証されます。受信トラフィックは、RADIUS サーバ 171.68.118.115 を含むサーバ リスト（受信）を使用します。

PIX デバッグ - 良好な認証 - TACACS+

次の例は、良好な認証の PIX デバッグを示します。

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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、認証（ユーザ名またはパスワード）が失敗した PIX を示します。 4 つのユーザ名/パスワード セットがユーザに表示されます。次のメッセージが表示されます。「Error:max number of tries exceeded"

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX デバッグ - ping できるが応答がない - TACACS+

次の例は、PIX に応答していない ping 可能なサーバの PIX デバッグを示しています。ユーザ名が一度だけ表示され、PIX はパスワードを要求しません（これは Telnet 上です）。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

PIX デバッグ - サーバに ping できない - TACACS+

次の例は、ping できないサーバに対する PIX デバッグを示しています。ユーザに対してユーザ名が一度表示されます。PIX はパスワードを要求しません（これは Telnet 上です）。 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"（この設定例は bogus サーバを表しています）。

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

PIX デバッグ- 良好な認証 - RADIUS

次の例は、良好な認証の PIX デバッグを示しています：

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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、認証（ユーザ名またはパスワード）が失敗した PIX を示します。 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。どちらかが正しくないと、「Incorrect password」というメッセージが 4 回表示されます。次に、ユーザの接続が切断されます。この問題にはバグ ID CSCdm46934 が割り当てられています。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

PIX デバッグ - デーモン停止、PIX と通信できない - RADIUS

次の例は、ping 可能でデーモンが停止しているサーバに対する PIX デバッグを示しています。サーバは PIX と通信しません。ユーザにはユーザ名に続いてパスワードが表示されます。次のメッセージが表示されます。"RADIUS server failed" および "Error:Max number of tries exceeded"

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

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

次の例は、ping できないサーバ、またはキー/クライアントが一致しないサーバの PIX デバッグを示しています。ユーザにはユーザ名とパスワードが表示されます。次のメッセージが表示されます。"Timeout to RADIUS server" および "Error:Max number of tries exceeded"（この設定のサーバは単なる例示用です）。

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

認可の追加

認可は認証なしでは無効なため、同じ送信元/宛先範囲に認可が必要です：

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

発信

着信トラフィックが RADIUS で認証され、RADIUS 認可が無効であるため、「着信」の認可を追加し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

良好な認証、認可が成功した PIX デバッグ - TACACS+

次の例は、認証が良好で認可が成功した PIX デバッグを示します。

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
```

```
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX デバッグ - 良好な認証、認可に失敗 - TACACS+

次の例は、認証が良好で認可に失敗した 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" というメッセージも表示されます。

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

アカウンティングの追加

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

アカウンティングがオン/オフのどちらの場合もデバッグは同じように表示されます。ただし、「Built」時に「開始」アカウンティング レコード送信が存在します。「Teardown」（ティアダウン）時に、「停止」アカウンティング レコード送信が存在します。

TACACS+ アカウンティング レコードは次のようになります（これらは CiscoSecure UNIX のものであり、CiscoSecure NT の場合はカンマ区切りになる可能性があります）：

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming

アカウンティングがオン/オフのどちらの場合もデバッグは同じように表示されます。ただし、「Built」時に「開始」アカウンティング レコードが送信されます。「Teardown」（ティアダウン）時に、「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 レコードは次のようになります（これらは CiscoSecure UNIX のものであり、CiscoSecure NT の場合はカンマ区切りになる可能性があります）：

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

except コマンドの使用

ネットワーク内で、特定の発信元や宛先に認証、認可、アカウンティングが必要ないと判断される場合には、次のような操作を実行できます。

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

認証から IP アドレスを除外するときに認可がオンになっている場合は、認可からもそれ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「開始」レコードが生成されているが「停止」レコードが存在しない場合、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（つまり 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ものの（この時点で）「停止」レコードがないため、サーバは「Telnet」ユーザがログインしていることを示します。認証を必要とする別の接続をこのユーザが（たとえば別の PC から）試みた場合、（最大セッションをサポートする）サーバでこのユーザに対する最大セッションが「1」に設定されていると、接続はサーバによって拒否されます。

ユーザは自分の Telnet や FTP の作業をターゲット ホスト上で続行した後、終了します（ここで 10 分を費やします）。

```
(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。

ただし HTTP は、そのプロトコルの性質上、動作が異なります。次に HTTP の例を示します。

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に投稿されたスタートレコードと16:35:35に投稿されたストップレコード。このダウンロードには1秒(つまり、開始レコードと停止レコードの間は 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、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

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述べました。次の例では、認証を有効にしなくても PIX への Telnet を実行できることを確認します。

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

次に、PIX への Telnet を実行するユーザを認証するコマンドを追加します。

```
aaa authentication telnet console Outgoing
```

ユーザが PIX への Telnet を実行すると、Telnet パスワード (「ww」) を求められます。 また、この場合は PIX が TACACS+ (「発信」サーバ リストが使用されるため) または RADIUS のユーザ名とパスワードも求めます。

```
aaa authentication enable console Outgoing
```

このコマンドでは、TACACS または RADIUS サーバに送信されるユーザ名とパスワードを入力するようユーザに求めます。この場合、「発信」サーバ リストが使用されるため、要求は TACACS サーバに送られます。有効化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、ユーザは同じユーザ名とパスワードを使って TACACS または RADIUS で有効化できます (ただしユーザが TACACS または RADIUS を使って PIX にログインできる場合)。この問題にはバグ ID CSCdm47044 が割り当てられています。

サーバがダウンした場合は、ユーザ名「PIX」および PIX の通常のイネーブル パスワード (enable password whatever) を入力することで、ユーザは PIX イネーブル モードにアクセスできます。 「enable password whatever」が PIX 設定に含まれない場合、ユーザはユーザ名「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ているが不明な場合は、リセットするためにパスワード復旧ディスクが必要です。

シリアル コンソールの認証

PIX のシリアル コンソールにアクセスするために、**aaa authentication serial console コマンドでは認証の検証が必要です。**ユーザがコンソールから設定コマンドを実行すると、 (syslog ホストにデバッグ レベルで syslog を送信するよう PIX が設定されている場合) syslog メッセージが削除されます。 syslog サーバの例を次に示します。

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

プロンプト変更後に表示されるメッセージ

次のコマンドを実行するとします。

```
auth-prompt THIS_IS_PIX_5
```

PIX 処理中に、次のシーケンスがユーザに表示されます。

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

そして、最終的な宛先ボックスに到着すると、「Username:」と「Password:」のプロンプトが宛先ボックスに表示されます。

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/失敗時にユーザに表示されるメッセージのカスタマイズ

次のコマンドを実行するとします。

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

PIX でのログイン失敗/成功時に、次のメッセージがユーザに表示されます。

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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に同じタイムアウト uauth を設定する場合は、これを実装しないでください。ユーザごとに異なる uauth が必要であれば、このまま続行してください。

この PIX の例では、**timeout uauth 3:00:00 コマンドを使用します。**つまり、あるユーザが認証されると、その後 3 時間は再認証する必要がなくなります。ただし、次のプロファイルを使ってユーザを設定し、PIX で TACACS AAA 認可を有効にすると、ユーザ プロファイル内のアイドル タイムアウトと絶対タイムアウトが、そのユーザに関する PIX でのタイムアウト uauth をオーバーライドします。これは、アイドル/絶対タイムアウト後に PIX 経由の Telnet セッションが切断されるという意味ではありません。単に再認証が実行されるかどうかを制御するだけです。

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

```
timeout = 2
idletime = 1
}
}
```

認証後に、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
```

ユーザが同じターゲット ホストに戻ったり別のホストを使用したりするときには、再認証が必要です。

仮想 HTTP

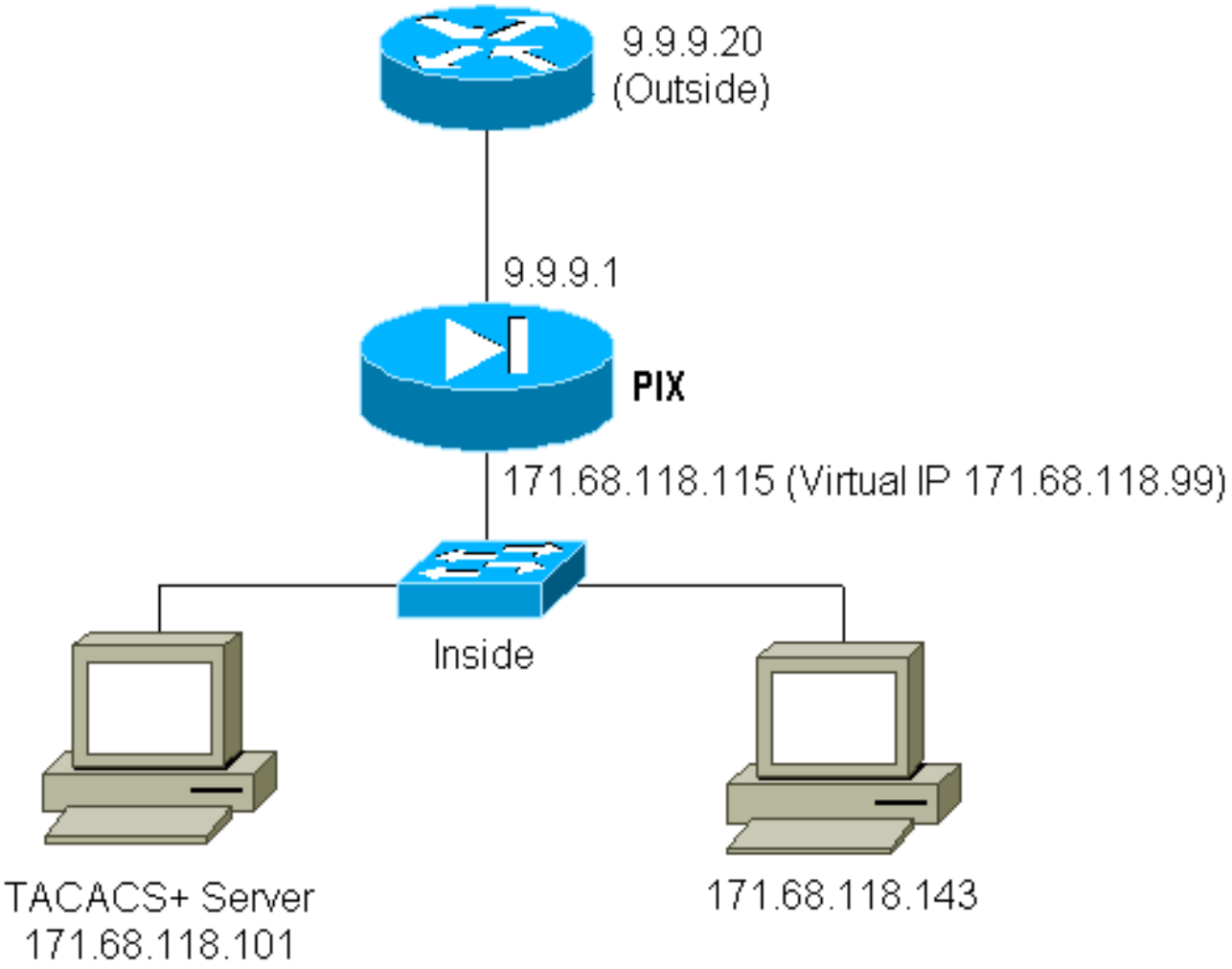
PIX 自体に加えて PIX 外部のサイトでも認証が必要な場合、ブラウザが異常な動作を見せることがあります。これはブラウザがユーザ名とパスワードをキャッシュするためです。

これを回避するには、次のコマンドを使用して、PIX設定にRFC 1918 アドレス (つまり、インターネット上でルーティング不能で、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。

仮想 HTTP 送信の例



仮想 HTTP 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 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

仮想 Telnet

mail などの一部のプロトコルは簡単に認証されないため、すべての着信および発信トラフィックを認証するよう PIX を設定することは推奨できません。PIX を経由するトラフィックがすべて認証される場合、メール サーバとクライアントが PIX を介して通信しようとすると、認証できないプロトコルに関する PIX syslog に次の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
```

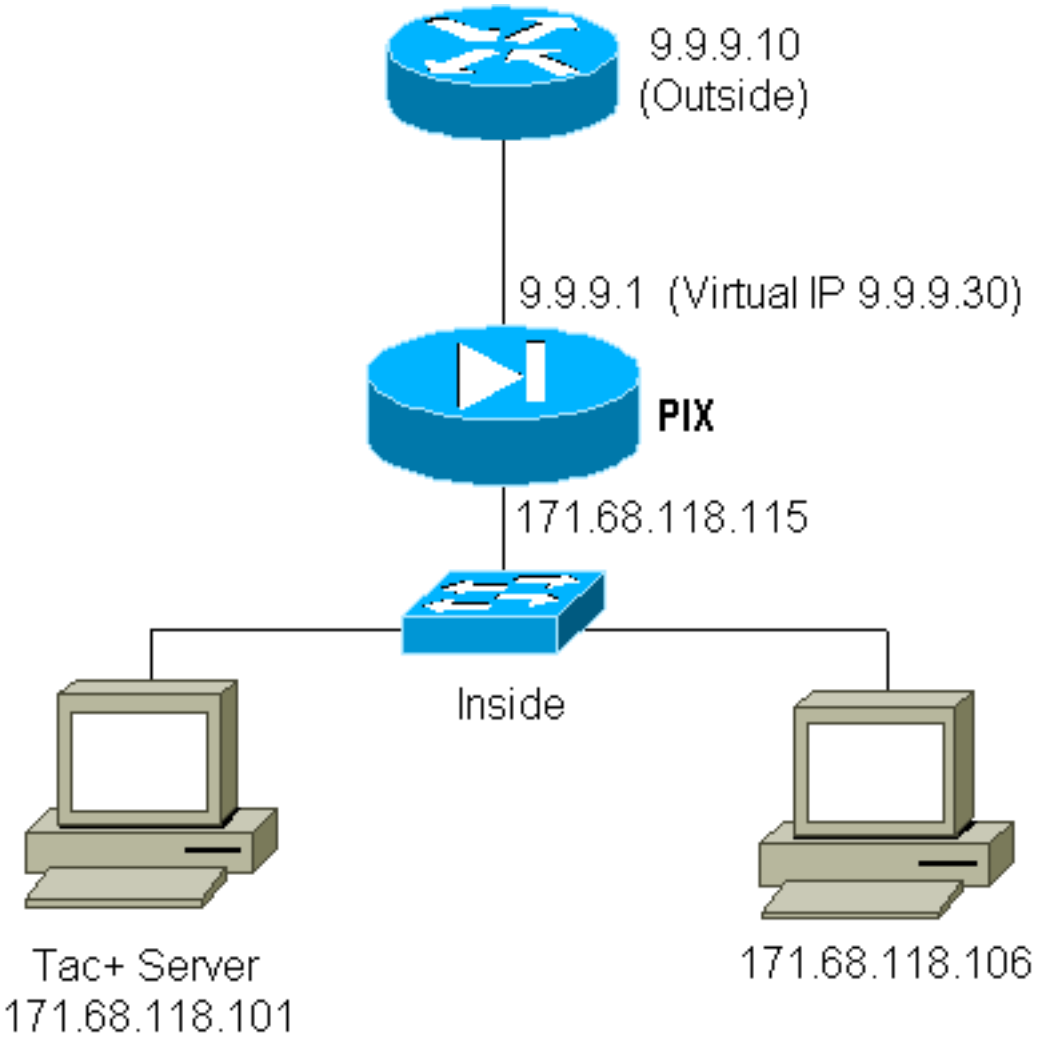
メールなどの一部のサービスは、認証できるほど十分に対話的ではありません。1 つの解決策として、認証/認可用に **except コマンドを使用できます (メール サーバ/クライアントの送信元/宛**

先を除くすべてを認証します) 。

ただし、何らかの特殊なサービスを確実に認証する必要がある場合は、**virtual telnet コマンドを使用できます。**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、特殊なサービスのトラフィックは、仮想 IP に関連付けられた実際のサーバに送られます。

この例では、TCPポート49トラフィックが外部ホスト9.9.9.10から内部ホスト171.68.118.106に流れることを許可します。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。

仮想 Telnet 受信：



仮想 Telnet 受信の 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
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

仮想 Telnet 受信の TACACS+ サーバ ユーザ設定：

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

仮想 Telnet 受信の PIX デバッグ：

9.9.9.10 のユーザは PIX 上の 9.9.9.30 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 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

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          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

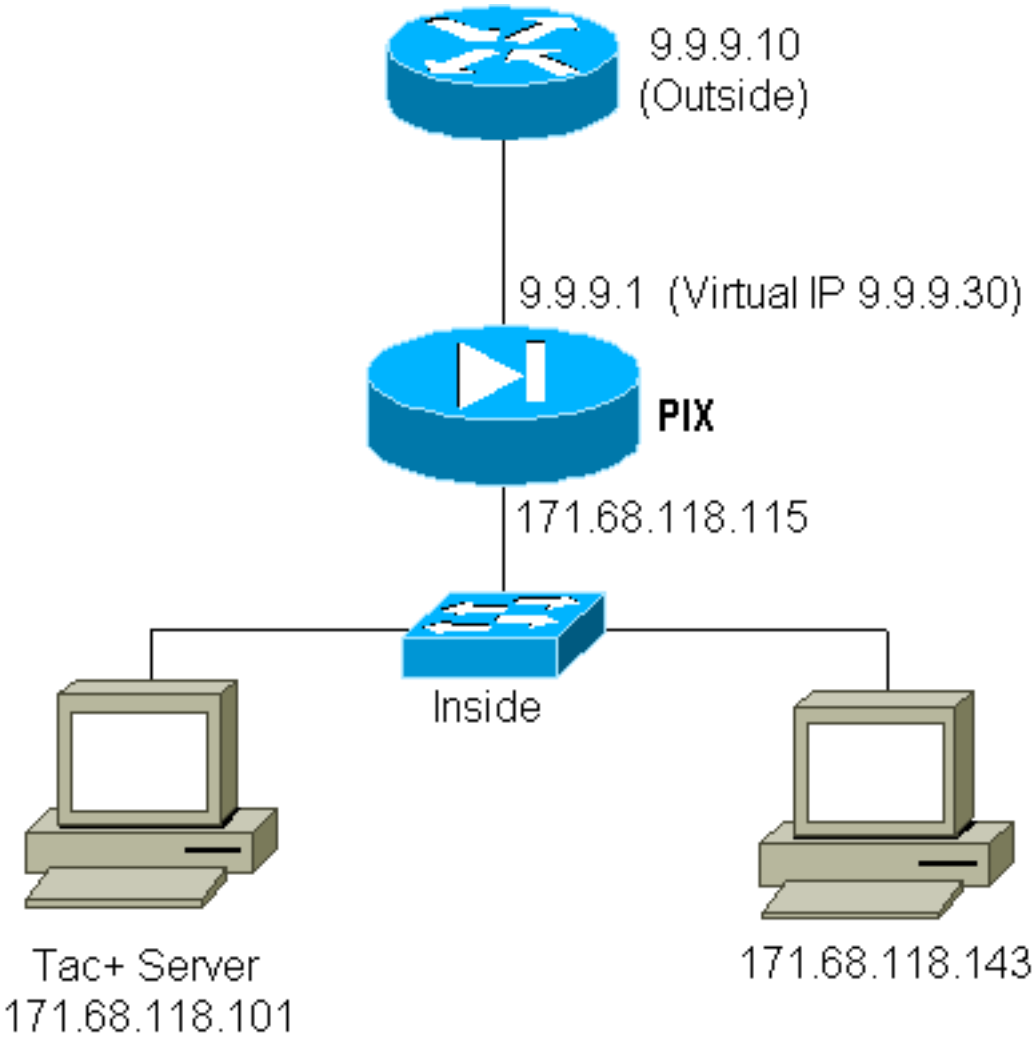
9.9.9.10 のデバイスが 171.68.118.106 のデバイスに TCP/49 トラフィックを送信する場合は、

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 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。次の例では、171.68.118.143 の内部ユーザが仮想 9.9.9.30 に Telnet 接続し、認証されます。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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual telnet 9.9.9.30
```

仮想 Telnet 送信の 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 接続する場合、**show uauth コマンドによってその uauth が表示されます。**（uauth の時間が残っている場合）セッション終了後にトラフィックの通過を防止することを希望するユーザは、仮想 Telnet IP に再び Telnet 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。

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。次の例では、すべての送信で認証が引き続き必要ですが、認可は TCP ポート 23 ~ 49 でのみ必要です。

PIX の設定：

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

この場合、Telnet ポート 23 が 23 ~ 49 の範囲に含まれるため、171.68.118.143 から 9.9.9.10 への Telnet 接続で認証と認可が発生します。171.68.118.143 から 9.9.9.10 への HTTP セッションを実行する場合もやはり認証が必要ですが、80 は 23 ~ 49 の範囲でないため、PIX は TACACS+ サーバに HTTP 認可を求めません。

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 が TACACS+ サーバに「cmd=tcp/23-49」および「cmd-arg=9.9.9.10」を送信していることに注意してください。

PIX でのデバッグ：

```
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)
```

関連情報

- Cisco PIX Firewall Software に関する製品サポート
- Cisco Secure PIX ファイアウォール コマンド リファレンス