PIX、TACACS+ および RADIUS の設定例：4.2.x

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。 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。

認証のための構文は PIX Software 4.2.2 でわずかに変更されました。 この資料はソフトウェア バ

ージョン 4.2.2 のために構文を使用します。

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。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

PIX の設定

```
pix2# write terminal Building configuration : Saved :
PIX Version 4.2(2) nameif ethernet0 outside security0
nameif ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr
encrypted hostname pix2 fixup protocol http 80 fixup
protocol smtp 25 no fixup protocol ftp 21 no fixup
protocol h323 1720 no fixup protocol rsh 514 no fixup
protocol sqlnet 1521 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 0.0.0.0 names
pager lines 24 logging console debugging no logging
monitor logging buffered debugging logging trap
debugging logging facility 20 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto ip
address outside 9.9.9.12 255.255.255.0 ip address inside
171.68.118.103 255.255.255.0 ip address 0.0.0.0 0.0.0.0
arp timeout 14400 global (outside) 1 9.9.9.1-9.9.9.9
netmask 255.0.0.0 static (inside,outside) 9.9.9.10
171.68.118.100 netmask 255.255.255.255 0 0 conduit
permit icmp any any conduit permit tcp host 9.9.9.10 eq
telnet any no rip outside passive no rip outside default
no rip inside passive no rip inside default timeout
xlate 3:00:00 conn 1:00:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:00:00 absolute ! !-
-- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5 radius-server (inside) host
171.68.118.101 cisco timeout 10 ! !--- The focus of
concern is with hosts on the inside network !---
accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11 255.255.255.255 tacacs+|radius ! !--- It is
possible to be less granular and authenticate !--- all
outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
```

```
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

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、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。

例としてように、内部百人のユーザおよびネットワークの外部の FTP、Telnet、または HTTP をされるこれらのユーザの 6 にほしくてもらうことをただ仮定して下さい。 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 を与えるように言って下さい。 シンプル認証を使うと、この 6 人のユーザはユーザ名 および パスワードを使うと認証することができましたりそして出かけます。 他の 94 人のユーザは出かけることができません。 PIX は username/password のためのユーザをプロンプト表示しましたり、そして TACACS+/RADIUS セキュリティサーバにユーザ名 および パスワードを渡します。 また、応答によって、それは接続を開くか、または否定します。 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。

ただし、この 3 人のユーザの 1 人を、「テリー」、ではないです信頼されること仮定して下さい。 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。 これは認証を追加する必要意味します。 すなわち、ユーザがだれのあるか認証に加えてすることができるものを承認します。 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」がテリー試みているものをテリーのユーザ名 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を使うと、テリーは「FTP 1.2.3.4」に許可することができますが、「HTTP」または「Telnet」への能力をどこでも否定されます。

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/許可と内部から外部へ（または逆に）行くことを試みる時:

- **Telnet**：ユーザ名を求めるプロンプトがユーザに表示された後、パスワードを要求されます。 PIX/サーバで認証（および認可）に成功すると、外部の宛先ホストからユーザ名とパスワードの入力を求められます。
- **FTP**： ユーザ名を求めるプロンプトがユーザに表示されます。 ユーザ名に「local_username@remote_username」を、パスワードに「local_password@remote_password」を入力する必要があります。 PIX は「local_username」と「local_password」をローカル セキュリティ サーバに送信します。

PIX/サーバ間で認証（および認可）に成功すると、「remote_username」と「remote_password」が外部の宛先 FTP サーバに渡されます。
- 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 PIX にブラウザ「射撃」と実際にキャッシュされたユーザ名およびパスワード起こっている可能性が高いといえます。 それは認証サーバにそれからこれを転送します。 PIX syslog やサーバ デバッグはこの現象を示します。 Telnet および FTP が正常に働くようであるが HTTP 接続が場合、これは原因です。

すべてのシナリオに適用できるサーバ設定

TACACS+ サーバコンフィギュレーション例では、認証だけオンになっていれば、ユーザは「すべて」、「telnetonly」、「httponly」、および「ftponly」すべて機能しています。 RADIUSサーバ設定例では、ユーザは「すべて」機能しています。

認証が TACACS+ 認証 サーバへユーザ名 および パスワードを、PIX 送信コマンド（Telnet、HTTP、または TACACS+ サーバへ FTP）送信 することに加えて PIX に、追加される時。 TACACS+ サーバはそれからそのユーザがそのコマンドのために許可されるかどうか確認します。

より遅い例では、171.68.118.100 のユーザはコマンド **telnet 9.9.9.11 を**発行します。 これが PIX で受け取られるとき、PIX は処理のための TACACS+ サーバにユーザ名、パスワードおよびコマンドを渡します。

従って認証に加える許可と、ユーザは「PIX によって telnetonly」Telnet オペレーションを行うことができます。 ただし、ユーザは「PIX によって httponly」および「ftponly」Telnet オペレーションを行うことができません。

（再度、許可はプロトコル 仕様の性質による RADIUS でサポートされません）。

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

Cisco Secure 2.x

- ユーザ スタンザはここに表示する。
- CSU.cfg に PIX IP アドレスか完全修飾ドメイン名 および キーを追加して下さい。`user = all`

```
{
password = clear "all"
default service = permit
}

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

```
user = ftponly {
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

ネットワーク アクセス サーバ（NAS）リストに PIX IP およびキーを追加するのに高度なグラフィカル ユーザ インターフェイス（GUI）を使用して下さい。 ユーザ スタンザはここに見られるように現われます:

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

Cisco Secure NT 2.x RADIUS

CiscoSecure 2.1 の Sample Configurations セクションはオンラインおよび Web ドキュメント セットアップを記述します; アトリビュート 6（サービス タイプ）はログインまたは管理上です。

GUI を使用して NAS Configuration セクションの PIX の IP を追加して下さい。

EasyACS TACACS+

EasyACSドキュメンテーションはセットアップ情報を提供します。

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. 割り当てたいと思う各コマンドのために『Add/Edit』 を選択 して下さい（Telnet、たとえば）。
4. 特定のサイトに Telnet を許可したいと思う場合引数部分で IP を入力して下さい。 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 して下さい。
6. 許可されたコマンド（Telnet、HTTP や FTP、たとえば）のそれぞれのためのステップ 1through 5 を実行して下さい。
7. GUI を使用して NAS Configuration セクションの PIX の IP を追加して下さい。

Cisco Secure NT 2.x TACACS+

Cisco Secure 2.x ドキュメントはセットアップ情報を提供します。

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. **Command チェックボックスを**下部ので選択し、許可したいと思うコマンドを入力して下さい（Telnet、たとえば）。
4. 特定のサイトに Telnet を許可したいと思う場合引数部分で IP を入力して下さい（たとえば、「割り当て 1.2.3.4"）。 Telnet をすべてのサイトに許可するために、『Permit unlisted arguments』 をクリック して下さい。
5. [Submit] をクリックします。
6. 許可されたコマンド（Telnet、FTP、および/または HTTP、たとえば）のそれぞれのためのステップ 1through 5 を実行して下さい。
7. GUI を使用して NAS Configuration セクションの PIX の IP を追加して下さい。

Livingston RADIUS サーバの設定

PIX IP 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。

```
all 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。

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

TACACS+ フリーウェア サーバの設定

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

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

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

user = ftponly {
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。AAA を設け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 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**から出力は syslog サーバにそして送られ、検査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。

PIX からの認証デバッグ例

PIX デバッグ- 良好な認証 - RADIUS

これは良好な認証を用いる PIX デバッグの例です:

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

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

これは認証不良を用いる PIX デバッグの例です（ユーザ名かパスワード）。 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。 「エラー: 再試行によって超過される」メッセージの最大数は表示する。

注: これが FTP 試みである場合、1 つの試みが割り当てられます。 HTTP に関しては、無限のリトライは許可されます。

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX デバッグ-サーバ- RADIUS

これはサーバの PIX デバッグの例です。 ユーザに対してユーザ名が一度表示されます。 サーバはそして「ハングし」、パスワード（3 回）の入力を求めます。

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX デバッグ - 良好な認証 - TACACS+

これは良好な認証を用いる PIX デバッグの例です:

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
```

```
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

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

これは認証不良を用いる PIX デバッグの例です (ユーザ名かパスワード) 。 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。 「エラー: 再試行によって超過される」メッセージの最大数は表示する。

注: これが FTP 試みである場合、1 つの試みが割り当てられます。 HTTP に関しては、無限のリトライは許可されます。

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX デバッグ-サーバ- TACACS+

これはサーバの PIX デバッグの例です。 ユーザに対してユーザ名が一度表示されます。 すぐに、「エラー: 試みによって超過される」メッセージの最大数は表示する。

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

認可の追加

許可が認証なしで無効であるので、許可は同じ送信元および宛先のために求められます:

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255
tacacs+|radius
```

または、すべての 3 人のアウトバウンド サービスが最初に認証された場合:

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization
ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization telnet outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
```

PIX からの認証および認可のデバッグ例

PIX デバッグ-良好な認証および許可- TACACS+

これは良好な認証および許可の PIX デバッグの例です:

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
```

```
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX デバッグ-許可の良好な認証、しかし失敗- TACACS+

これは良好な認証しかし許可の失敗との PIX デバッグの例です:

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX デバッグ-認証不良、試みられない許可- TACACS+

これは認証 および 権限を用いる PIX デバッグの例、認証不良が許可試みられなかった原因であり (ユーザ名かパスワード) ではない。 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。 「エラー: 超過する再試行の最大数」。 メッセージは表示する

注: これが FTP 試みである場合、1 つの試みが割り当てられます。 HTTP に関しては、無限のリトライは許可されます。

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX Debug authentication/許可、サーバ- TACACS+

これは認証 および 権限を用いる PIX デバッグの例です。 サーバはダウンしています。 ユーザはユーザ名を一度見ます。 すぐに、「エラー: 超過する試みの最大数」。 表示する。

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

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: tacacs+
デバッグは説明がオン/オフであるかどうか同じを検知 します。 ただし、の時に「」、a「開始する」アカウンティング レコード 送信 されます構築しました。 また、「ティアダウンの時に」、a「停止」アカウンティング レコードは送信 されます:

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
```

```
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

この出力のように TACACS+ アカウンティング レコード見え（これらは CiscoSecure UNIX からあります; Cisco Secure Windows のレコードは代りにコンマで区切られるかもしれません）:

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

フィールドはここに見られるように破壊します:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

デバッグは説明がオン/オフであるかどうか同じを検知 します。 ただし、の時に「」、a「開始する」アカウンティング レコード 送信 されます構築しました。 また、「ティアダウンの時に」、a「停止」アカウンティング レコードは送信 されます:

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

この出力のように RADIUS アカウンティング レコード見え（これらは Cisco Secure UNIX からあります; Cisco Secure Windows の物はコンマで区切られって います）:

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
```

```
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```
フィールドはここに見られるように破壊します:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

最大セッションとログインユーザを確認する方法

いくつかの TACACS におよび RADIUSサーバに" max-session "か「view logged-in users」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。 作成される会計「開始する」レコード「停止」レコードがないが、とき、（ある人がまだログオンされることを TACACS か RADIUSサーバは仮定します; PIX によってセッションを持っています）。 これは Telnet や FTP 接続では接続の性質上うまく機能します。 たとえば、次のようになります。

ユーザは 171.68.118.100 にから 9.9.9.25 方法で認証を受ける PIX によって Telnet で接続します:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
   to 9.9.9.25/23
(pix) 109011: Authen Session Start: user 'cse', sid 3
(pix) 109005: Authentication succeeded for user 'cse' from 171.68.118.100/12
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
```
「開始する」は記録するが、ことをサーバが見たので「停止」レコードは（この時点で）、サーバ「Telnet」ユーザがログオンされることを示しません。 最大セッション数がこのユーザ向けのサーバの "1" に設定 される試みれば場合ユーザが認証を必要とする別の接続を（多分別の PC から）、そして、接続はサーバによって拒否されます。

ユーザはビジネス ターゲットホスト、そして終了の歩き回ります（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
```
ユーザ認証は（ある 0 であるかどうか; 認証する毎回）または多く（ユーザ認証期間の間の一度および再度認証する）、アクセスされた各サイトのためのアカウンティング レコード切り取りがあります。

しかし HTTP はプロトコルの性質が別様に原因ではたらかせます。 次に例を示します。

ユーザは 171.68.118.100 にから 9.9.9.25 PIX によってブラウズします。

```
(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ウェブページを読みます。

時間に注意して下さい。 このダウンロードは 1秒を奪取 しました (開始すると停止レコード間の 1秒より小さかったでした)。 ユーザはまだ開いた Webサイトおよび接続にまだ口グオンされますか。 いいえ。

最大セッションまたは口グイン ユーザの表示は機能するでしょうか? HTTP の接続時間が余りに短いので、いいえ。 」構築される「と「ティアダウン」間の時間は (「開始する」および「停止」レコード) 計測秒です。 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、0 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た「開始」および「停止」レコードはまだ存在しています。 ただし、max-sessions and view logged-in users は HTTP 接続の性質が原因ではたらかせません。

except コマンドの使用

1 人の発信 ユーザことをネットワークでは、決定すれば (171.68.118.100) 認証される必要はありませんこれをすることができます:

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255 tacacs+ aaa
authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11 255.255.255.255 tacacs+
```

PIX 自身への認証

前の説明は認証 Telnet (および HTTP、FTP) トラフィック PIX によってです。 4.2.2 によって、PIX への Telnet接続はまた認証されるかもしれません。 ここでは、PIX に Telnet で接続することができるボックスの IP を定義します:

```
telnet 171.68.118.100 255.255.255.255
```

それから Telnetパスワードを供給して下さい: **passwd ww**。

PIX に Telnet で接続しているユーザを認証するために新しいコマンドを追加して下さい:

aaa authentication telnet console tacacs+|radius
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。 PIX はまた TACACS+ か RADIUSユーザ名およびパスワード要求します。

プロンプト変更後に表示されるメッセージ

コマンドを追加すれば: **auth-prompt YOU_ARE_AT_THE_PIX は**、PIX を通過しているユーザ シーケンスを見ます:

YOU_ARE_AT_THE_PIX [*at which point you enter the username*] Password:[*at which point you enter the password*]
最終デスティネーションの到達に、「ユーザ名:] および [Password: 」プロンプトは表示する。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。

関連情報

- Cisco PIX Firewall ソフトウェア製品サポート
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems