PIX, TACACS+, e configurações de exemplo RADIUS: 4.2.x

Índice

Introdução

O RAIO e a autenticação TACACS+ podem ser feitos para o FTP, o telnet, e as conexões de HTTP. A autorização TACACS+ é apoiada; A autorização de RADIUS não é.

A sintaxe para autenticação mudada levemente no software de PIX 4.2.2. Este documento usa a

sintaxe para as versões de software 4.2.2.

Pré-requisitos

Requisitos

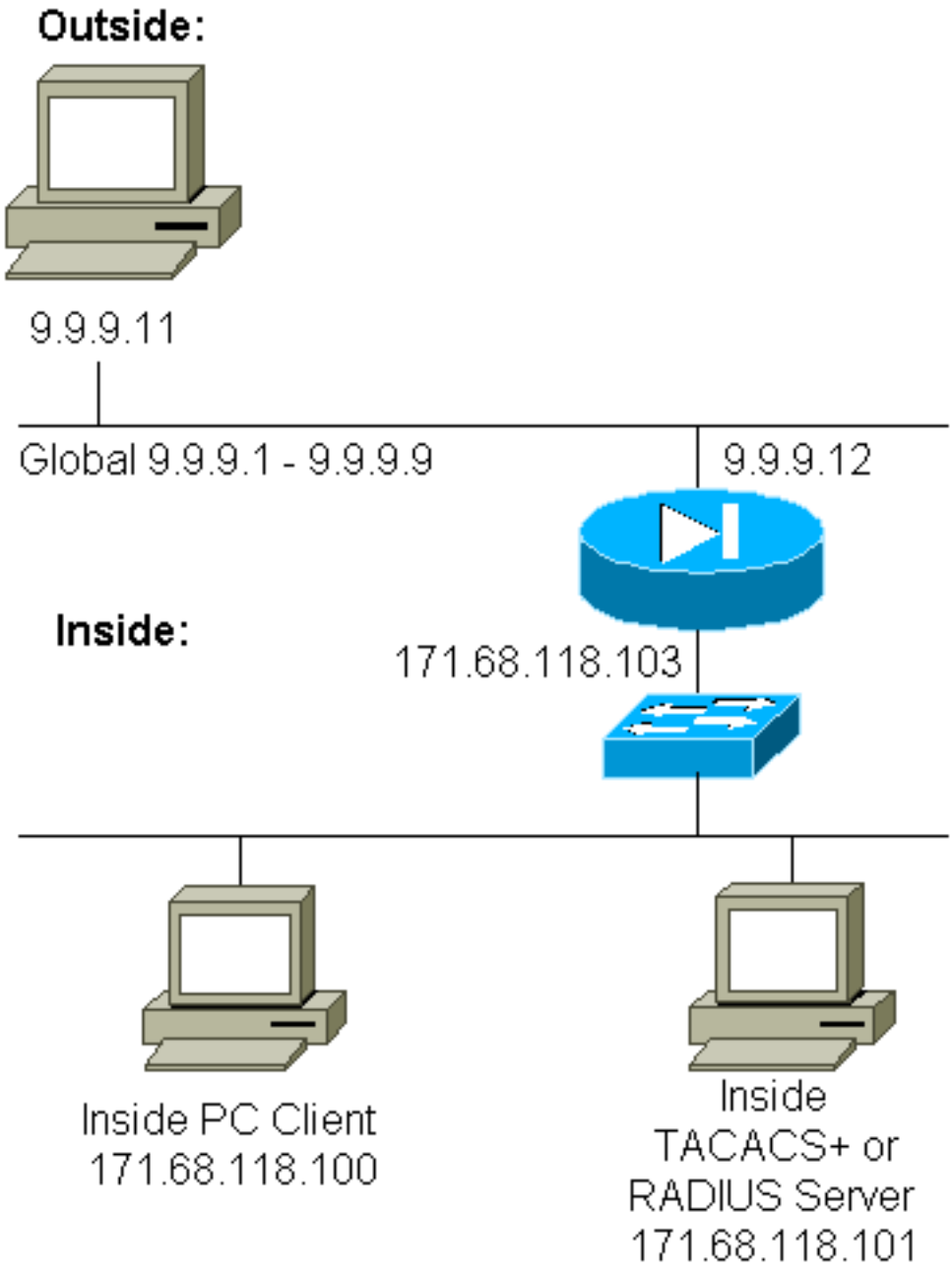
Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração de PIX

```
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]
```

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Autenticação vs. Autorização

- A autenticação é *quem o* usuário é.
- A autorização é *o que o* usuário pode fazer.

- A autenticação é válida sem autorização.
- A autorização não é válida sem autenticação.

Como como o exemplo, supõe que você o manda cem usuários internos e somente querer seis destes usuários poder fazer o FTP, o telnet, ou o HTTP fora da rede. Diga o PIX para autenticar o tráfego de saída e dar a todos os seis usuários ID no servidor de segurança TACACS+/RADIUS. Com autenticação simples, estes seis usuários podem ser autenticados com nome de usuário e senha, a seguir saem. Os outros usuários da noventa-quatro não podem sair. O PIX alerta usuários para o username/senha, a seguir passa seu nome de usuário e senha ao servidor de segurança TACACS+/RADIUS. Também, segundo a resposta, abre ou nega a conexão. Estes seis usuários poderiam fazer o FTP, o telnet, ou o HTTP.

Contudo, supõe um destes três usuários, “Terry”, não é ser confiado. Você gostaria de permitir que Terry façam o FTP, mas não o HTTP ou o telnet à parte externa. Isto significa-o necessidade de adicionar a autorização. Isto é, autorizando o que os usuários podem fazer além do que a autenticação de quem são. Quando você adiciona a autorização ao PIX, o PIX primeiramente envia o nome de usuário e senha de Terry ao servidor de segurança, a seguir envia um pedido de autorização que diga ao servidor de segurança o que o “comando” Terry está tentando fazer. Com a instalação do server corretamente, Terry pode ser permitido a “FTP 1.2.3.4” mas é negado a capacidade ao “HTTP” ou ao “telnet” em qualquer lugar.

O que o usuário visualiza com o modo de autenticação/autorização Ligado

Quando você tentar ir do interior à parte externa (ou vice versa) com autenticação/autorização sobre:

- **Telnet** - O usuário vê uma exibição de alerta de nome de usuário, seguida por um pedido para a senha. Se a autenticação (e autorização) for bem-sucedida no PIX/servidor, o usuário está pronto para obter nome de usuário e senha pelo host de destino.
- **FTP** - O usuário vê uma alerta de nome de usuário vir acima. O usuário precisa inserir local_username@remote_username para nome de usuário e local_password@remote_password para senha. O PIX envia "local_username" e "local_password" para o servidor de segurança local e, se a autenticação (e autorização) for bem-sucedida no PIX/servidor, "remote_username" e "remote_password” vão mais além do servidor FTP de destino.
- **HTTP** - Um indicador é indicado no navegador que pede um nome de usuário e senha. Se a autenticação (e autorização) for concluída com sucesso, o usuário chega ao web site de destino. Mantenha na mente que os **navegadores põem em esconderijo nomes de usuário e senha**. Se parece que o PIX deve cronometrar para fora uma conexão de HTTP mas não está fazendo assim, é provável que a reautenticação realmente está ocorrendo com o navegador “tiro” o nome de usuário oculto e a senha ao PIX. Ele então para a frente isto ao Authentication Server. O Syslog e/ou o server PIX debugam a mostra este fenômeno. Se o telnet e o FTP parecem trabalhar normalmente, mas as conexões de HTTP não fazem, esta é a razão.

Configurações do servidor utilizadas para todos os cenários

Nos exemplos de configuração de servidor TACACS+, se somente a autenticação está ligada, os

usuários “tudo”, “telnetonly”, “httponly”, e “ftponly” todos trabalham. Nos exemplos da configuração de servidor RADIUS, o usuário “tudo” trabalha.

Quando a autorização é adicionada ao PIX, além do que a emissão o nome de usuário e senha ao server da autenticação TACACS+, o PIX envia os comandos (telnet, HTTP, ou FTP) ao server TACACS+. O server TACACS+ verifica então para ver se esse usuário é autorizado para esse comando.

Em um exemplo mais atrasado, o usuário em 171.68.118.100 emite o comando telnet **9.9.9.11**. Quando isto é recebido no PIX, o PIX passa o username, senha, e comanda ao server TACACS+ para processar.

Assim com a autorização sobre além do que a autenticação, o usuário “telnetonly” pode executar operações telnet com o PIX. Contudo, os usuários “httponly” e “ftponly” não podem executar operações telnet com o PIX.

(Outra vez, a autorização não é apoiada com o RADIUS devido à natureza da especificação de protocolo).

Configuração do servidor segura de Cisco UNIX TACACS+

Cisco 2.x seguro

- As estâncias do usuário são indicadas aqui.
- Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome e chave de domínio totalmente qualificados PIX ao CSU.cfg.

```
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 .*
}
}
}
```

Configuração do servidor segura dos RADIUS UNIX de Cisco

Use a interface de usuário gráfica avançada (GUI) para adicionar o IP PIX e a chave à lista do servidor do acesso de rede (NAS). A estância do usuário aparece como considerado aqui:

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

RAIO do Cisco Secure NT 2.x

A seção de configurações da amostra do 2.1 do CiscoSecure em linha e da documentação da web descreve a instalação; o atributo 6 (tipo de serviço) seria início de uma sessão ou administrativo.

Adicionar o IP do PIX na seção de configuração de NAS usando o GUI.

EasyACS TACACS+

A documentação easyacs fornece a informação do instalação.

1. Na seção de grupo, **executivo do shell do** clique (para dar privilégios de exec).
2. Para adicionar a autorização ao PIX, **comandos deny unmatched ios do** clique na parte inferior da instalação de grupo.
3. Seleto **adicionar/edite** para cada comando que você quer permitir (telnet, por exemplo).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP à seção de argumento. Para permitir o telnet a todos os locais, o clique **permite todos os argumentos não listados**.
5. **Comando editing do revestimento do** clique.
6. Execute as etapas 1through 5 para cada um dos comandos permitidos (telnet, HTTP e/ou FTP, por exemplo).
7. Adicionar o IP do PIX na seção de configuração de NAS usando o GUI.

Cisco Secure NT 2.x TACACS+

A documentação 2.x segura de Cisco fornece a informação do instalação.

1. Na seção de grupo, **executivo do shell do** clique (para dar privilégios de exec).
2. Para adicionar a autorização ao PIX, **comandos deny unmatched ios do** clique na parte inferior da instalação de grupo.
3. Selecione a caixa de seleção do **comando na** parte inferior e incorpore o comando que você quer permitir (telnet, por exemplo).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP à seção de argumento (por exemplo, “licença 1.2.3.4"). Para permitir o telnet a todos os locais, clique **argumentos não listados da licença**.
5. Clique em Submit.
6. Execute as etapas 1through 5 para cada um dos comandos permitidos (telnet, FTP, e/ou HTTP, por exemplo).
7. Adicionar o IP do PIX na seção de configuração de NAS usando o GUI.

Configuração de servidor Livingston RADIUS

Adicionar o IP PIX e a chave aos clientes arquivam.

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

Configuração de servidor Merit RADIUS

Adicionar o IP PIX e a chave aos clientes arquivam.

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

TACACS+ Configuração do programa gratuito de servidor

```
# 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 .*
}
}
```

Etapas de depuração

- Certifique-se de que as configurações de PIX estão trabalhando antes de adicionar o Authentication, Authorization, and Accounting (AAA).Se você não pode passar o tráfego antes de instituir o AAA, você não poderá fazer tão mais tarde.
- Enable que entra o PIX:**O comando logging console debugging** não deve ser usado pesadamente em um sistema carregado.O comando logging buffered debugging poder ser utilizado. A saída dos **comandos show logging ou logging** pode então ser enviada a um servidor de SYSLOG e ser examinada.
- Certifique-se de que debugar está ligada para o TACACS+ ou os servidores Radius. Todos os servidores possuem esta opção.

Exemplos de debug de autenticação a partir de PIX

PIX debug - Boa autenticação - RAIO

Este é um exemplo de um PIX debug com boa autenticação:

```
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 debug - Autenticação inválida (username ou senha) - RAIO

Este é um exemplo de um PIX debug com autenticação inválida (username ou senha). O usuário vê quatro conjuntos de nome de usuário/senha. O “erro: o número máximo de” mensagem excedida novas tentativas é indicado.

Nota: Se esta é uma tentativa FTP, uma tentativa está permitida. Para o HTTP, as novas tentativas infinitas são permitidas.

```
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 debug - Server para baixo - RAIO

Este é um exemplo de um PIX debug com o server para baixo. O usuário vê o username uma vez. O server então “pendura” e pede uma senha (três vezes).

```
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 debug - Boa autenticação - TACACS+

Este é um exemplo de um PIX debug com boa autenticação:

```
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 debug - Autenticação inválida (username ou senha) - TACACS+

Este é um exemplo de um PIX debug com autenticação inválida (username ou senha). O usuário vê quatro conjuntos de nome de usuário/senha. O “erro: o número máximo de” mensagem excedida novas tentativas é indicado.

Nota: Se esta é uma tentativa FTP, uma tentativa está permitida. Para o HTTP, as novas tentativas infinitas são permitidas.

```
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 debug - Server para baixo - TACACS+

Este é um exemplo de um PIX debug com o server para baixo. O usuário vê o username uma vez. Imediatamente, o “erro: O número máximo de” mensagem excedida tentativas é indicado.

```
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
```

Autorização de adição

Porque a autorização é inválida sem autenticação, a autorização é exigida para a mesmos fonte e destino:

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

Ou, se todos os três serviços externos foram autenticados originalmente:

```
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
```

Exemplos de depuração de autenticação e de autorização do PIX

PIX debug - Boa autenticação e autorização - TACACS+

Este é um exemplo de um PIX debug com boa autenticação e autorização:

```
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 debug - Boa autenticação, mas falha na autorização - TACACS+

Este é um exemplo de um PIX debug com boa autenticação mas falha na autorização:

```
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 debug - Autenticação inválida, autorização não tentada - TACACS+

Este é um exemplo de um PIX debug com authentication e autorização, mas não tentado da

autorização devido à autenticação inválida (username ou senha). O usuário vê quatro conjuntos de nome de usuário/senha. O “erro: número máximo de novas tentativas excedidas.” a mensagem é indicada

Nota: Se esta é uma tentativa FTP, uma tentativa está permitida. Para o HTTP, as novas tentativas infinitas são permitidas.

```
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 - Autenticação/autorização, server para baixo - TACACS+

Este é um exemplo de um PIX debug com authentication e autorização. O server está para baixo. O usuário vê o username uma vez. Imediatamente, o “erro: Número máximo de tentativas excedidas.” é indicado.

```
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
```

Adicionar relatório

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+

Debugar olhares o mesmos se explicar é de ligar/desligar. Contudo, na altura do “construiu, registro de contabilidade do “começo”” a é enviado. Também, na altura do “Teardown, o registro de contabilidade da “parada”” a é enviado:

```
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
```

Os registros de contabilidade TACACS+ olham como esta saída (estes são do CiscoSecure UNIX; os registros em Cisco Windows seguro podem ser delimitados por vírgula pelo contrário):

```
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
```

Os campos dividem como considerado aqui:

```
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

Debugar olhares o mesmos se explicar é de ligar/desligar. Contudo, na altura do “construiu, registro de contabilidade do “começo”” a é enviado. Também, na altura do “Teardown, o registro de contabilidade da “parada”” a é enviado:

```
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
```

Os registros de contabilidade do RAIO olham como esta saída (estes são de Cisco UNIX seguro; esses em Cisco Windows seguro são delimitados por vírgula):

```
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
```

Os campos dividem como considerado aqui:

```
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 = #>
```

Max-sessions e visualização de usuários que fizeram login

Alguns TACACS e servidores Radius têm o " sessão máxima " ou “veja características dos usuários que fez login”. A habilidade de realizar max-sessions ou verificar usuários que fizeram login depende dos registros de contabilidade. Quando há um registro do “começo” da contabilidade gerado mas nenhum registro da “parada”, o TACACS ou o servidor Radius supõem que a pessoa está entrada ainda (que é; tem uma sessão com o PIX). Isto funciona bem para conexões Telnet e FTP devido à natureza das conexões. Como um exemplo:

O usuário Telnets de 171.68.118.100 a 9.9.9.25 com o PIX, autenticando na maneira:

```
(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
```

Porque o server não viu um registro do “começo” mas nenhum registro da “parada” (neste momento), o server mostra que o usuário do “telnet” está entrado. Se o usuário tenta uma outra conexão que exija a autenticação (talvez de um outro PC) e se as sessões máx. são ajustadas a "1" no server para este usuário, a conexão é recusada pelo server.

O usuário vai aproximadamente negócio no host de destino, a seguir nas saídas (passa os minutos 10 lá).

```
(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
```

Se o uauth é 0 (que é; autentique todas as vezes) ou mais (autentique uma vez e não outra vez durante o período de uauth), haverá um corte do registro de contabilidade para cada local alcançado.

Mas o HTTP trabalha diferentemente devido à natureza do protocolo. Este é um exemplo:

O usuário consulta de 171.68.118.100 a 9.9.9.25 com o PIX.

```
(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
```

O usuário lê um página da web transferido.

Note o tempo. Esta transferência tomou o segundo (havia menos do que o segundo entre o começo e o registro da parada). O usuário é entrado ainda ao site e à conexão ainda abertos? Não.

Max-sessions ou visualizar usuários que fizeram login funcionará aqui? Não, porque o tempo de conexão no HTTP é demasiado curto. O tempo entre “construído” e o “Teardown” (o registro do “começo” e da “parada”) é secundário-segundo. Não haverá um registro do “começo” sem um registro da “parada”, desde que os registros ocorrem virtualmente no mesmo instante. Ainda haverá o registro de "start" e "stop" enviado ao servidor em cada transação se uauth for definido como 0 ou um número superior. Contudo, as sessões máx. e os usuários que fez login da vista não trabalharão devido às naturezas da conexão de HTTP.

Usar o comando de exceção

Em nossa rede, se nós decidimos que um usuário de saída (171.68.118.100) não precisa de ser autenticado, nós podemos fazer este:

```
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+
```

Autenticação para o próprio PIX

A discussão anterior é do tráfego de autenticação do telnet (e o HTTP, o FTP) com o PIX. Com 4.2.2, as conexões Telnet ao PIX podem igualmente ser autenticadas. Aqui, nós definimos o IPs das caixas que podem telnet ao PIX:

```
telnet 171.68.118.100 255.255.255.255
```

Forneça então a senha telnet: **passwd ww**.

Adicionar o comando new autenticar usuários Telnetting ao PIX:

```
aaa authentication telnet console tacacs+|radius
```

Quando os usuários Telnet ao PIX, eles forem alertados para a senha telnet (“ww”). O PIX igualmente pede o TACACS+ ou o nome de usuário RADIUS e a senha.

Alterando o prompt visto pelos usuários

Se você adiciona o comando: **a autêntico-alerta YOU_ARE_AT_THE_PIX**, os usuários que atravessam o PIX verá a sequência:

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter
the password]
```

Em cima da chegada no destino final, o “username: ” e “senha: as” alertas serão indicadas. Esta alerta afeta somente os usuários que vão com o PIX, não ao PIX.

Nota: Não há nenhum registro de contabilidade cortado para o acesso ao PIX.

Informações Relacionadas

- Sustentação do produto do Software do firewall Cisco PIX
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems