

PIX, TACACS+, e configurações de exemplo RADIUS: 4.4.x

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Autenticação vs. Autorização](#)

[O que o usuário visualiza com o modo de autenticação/autorização Ligado](#)

[Configurações de servidor de segurança utilizadas para todos os cenários](#)

[Configuração do servidor CiscoSecure UNIX TACACS](#)

[Configuração do servidor CiscoSecure UNIX RADIUS](#)

[CiscoSecure NT 2.x RADIUS](#)

[EasyACS TACACS+](#)

[CiscoSecure 2.x TACACS+](#)

[Configuração de servidor Livingston RADIUS](#)

[Configuração de servidor Merit RADIUS](#)

[TACACS+ Configuração do programa gratuito de servidor](#)

[Etapas de depuração](#)

[Diagrama de Rede](#)

[Exemplos de debug de autenticação a partir de PIX](#)

[Autorização de adição](#)

[A authentication e autorização debuga exemplos do PIX](#)

[Relatório de adição](#)

[TACACS+](#)

[RADIUS](#)

[Uso do comando Except](#)

[Max-sessions e visualização de usuários que fizeram login](#)

[Autenticação e habilitação no próprio PIX](#)

[Autenticação no console serial](#)

[Alterando o prompt que os usuários visualizam](#)

[Personalizando a mensagem que os usuários visualizam no êxito/na falha](#)

[Tempo ocioso e intervalos absolutos por usuário](#)

[HTTP Virtual](#)

[Telnet Virtual](#)

[Desconexão de Telnet Virtual](#)

[Autorização da porta](#)

[Informações Relacionadas](#)

Introdução

O RAI0 e a autenticação TACACS+ podem ser feitos para o FTP, o telnet, e as conexões de HTTP. A autenticação para outros menos protocolos TCP comuns pode geralmente ser feita para trabalhar.

A autorização TACACS+ é apoiada; A autorização de RADIUS não é. As mudanças no Authentication, Authorization, and Accounting (AAA) PIX 4.4.1 sobre a versão anterior incluem: Os Grupos de servidores AAA e o Failover, autenticação para permitem e acesso do console serial, e aceitam e rejeitam mensagens imediata.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

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.

Supõe que você tem 100 usuários internos e você para querer quer somente 6 destes usuários poder fazer o FTP, o telnet, ou o HTTP fora da rede. Você diria o PIX para autenticar o tráfego de saída e dar a todos os usuários 6 ID no servidor de segurança TACACS+/RADIUS. Com autenticação simples, estes usuários 6 poderiam ser autenticados com nome de usuário e senha, a seguir saem. Outros 94 usuários não poderiam sair. O PIX alerta usuários para o username/senha, a seguir passa seu nome de usuário e senha ao servidor de segurança TACACS+/RADIUS, e segundo a resposta, abre ou nega a conexão. Estes usuários 6 poderiam fazer o FTP, o telnet, ou o HTTP.

Mas 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 ter que adicionar a autorização, isto é, autorizando o que os usuários podem fazer além do que a autenticação de quem são. Quando nós adicionamos a autorização ao PIX, o PIX primeiramente enviaria o nome de usuário e senha de Terry ao servidor de segurança, a seguir envia a um pedido de autorização que diz ao servidor de segurança o que o "comando" Terry está tentando fazer. Com a instalação do server corretamente, Terry poderia ser permitido a "FTP 1.2.3.4" mas negou a capacidade ao HTTP ou ao telnet em qualquer lugar.

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

Quando tentar ir de dentro para fora (ou vice-versa) com a autenticação/autorização ligada:

- **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 na requisição de nome de usuário de navegador e na 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 parecer que o PIX está esgotando uma conexão http mas não estiver, é provável que a re-autenticação esteja de fato ocorrendo com o navegador "disparando" o nome de usuário e a senha em cache para o PIX, que, em seguida, o encaminha ao servidor de autenticação. Syslog de PIX e/ou depuração de servidor mostrarão esse fenômeno. Se o Telnet e o FTP parecerem funcionar "normalmente", mas as conexões http não, esse será o motivo.

Configurações de servidor de segurança utilizadas para todos os cenários

Configuração do servidor CiscoSecure UNIX TACACS

Certifique-se de que você tem o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome e chave de domínio totalmente qualificados PIX no arquivo csu.cfg.

```
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 .*
}
}
}

```

[Configuração do servidor CiscoSecure UNIX RADIUS](#)

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).

```

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

```

[CiscoSecure NT 2.x RADIUS](#)

Termine estas etapas.

1. Obtenha uma senha na seção GUI de instalação de usuário.
2. Da seção gui da instalação de grupo, ajuste o atributo 6 (tipo de serviço) para entrar ou administrativo.
3. Adicionar o IP PIX na configuração de NAS GUI.

[EasyACS TACACS+](#)

A documentação easyacs descreve a instalação.

1. Na seção de grupo, clique sobre o **executivo do shell** (para dar privilégios de exec).
2. A para adicionar a autorização ao PIX, clique **comandos deny unmatched ios** na parte inferior da instalação de grupo.
3. Selecione o **comando add/edit new** para cada comando que você quer permitir (por exemplo, telnet).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP à seção de argumento no formulário "licença #.#.#.#". 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 etapas 1 com 5 para cada um dos comandos permitidos (por exemplo, telnet, HTTP e/ou FTP).
7. Adicionar o IP PIX na seção gui da configuração de NAS.

CiscoSecure 2.x TACACS+

O usuário obtém uma senha na seção de instalação de usuário do GUI.

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. Seletor **adicionar/edite** para cada comando que você quer permitir (por exemplo, telnet).
4. Se você quer permitir o telnet aos locais específicos, incorpore o IP da licença ao retângulo de argumentação (por exemplo, "licença 1.2.3.4"). 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 etapas 1 com 5 para cada um dos comandos permitidos (por exemplo, telnet, HTTP ou FTP).
7. Adicionar o IP PIX na seção gui da configuração de NAS.

Configuração de servidor Livingston RADIUS

Adicionar o IP PIX e a chave aos clientes arquivam.

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

Configuração de servidor Merit RADIUS

Adicionar o IP PIX e a chave aos clientes arquivam.

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

TACACS+ Configuração do programa gratuito de servidor

```
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 .*  
}  
}
```

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 passar o tráfego antes de instituir autenticação e autorização, não conseguirá fazê-lo depois disso.
- 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 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.

Diagrama de Rede

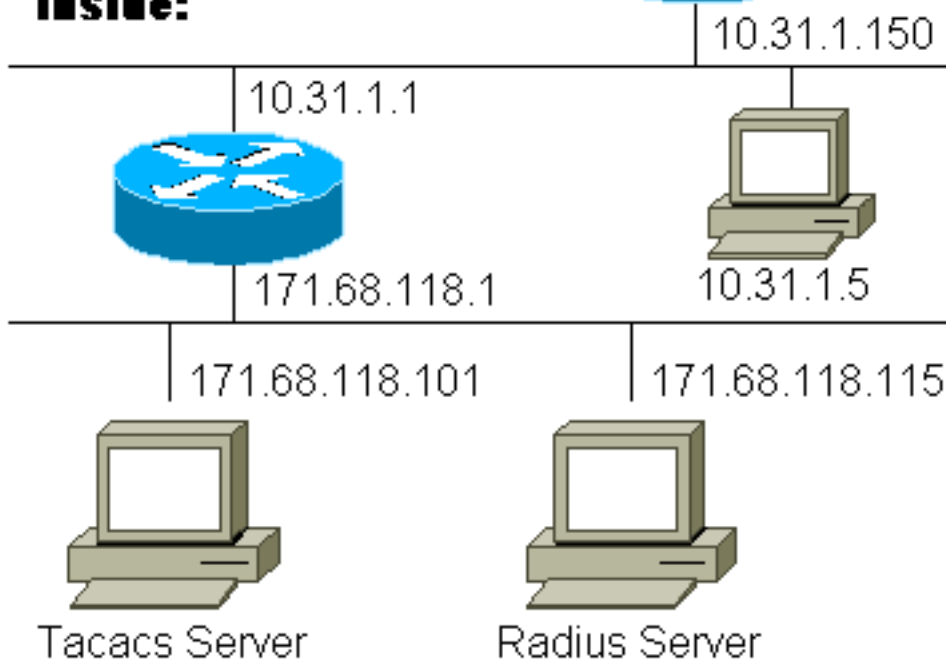
Outside:



11.11.11.15



Inside:



Configuração de PIX

```
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
```

[Exemplos de debug de autenticação a partir de PIX](#)

Nestes debugar exemplos:

Saída

O usuário interno em 10.31.1.5 inicia o tráfego a 11.11.11.15 exterior e é autenticado com o TACACS+ (o tráfego de saída usa a lista de servidor “que parte” que inclui o servidor de TACACS 171.68.118.101).

Entrada

O usuário externo em 11.11.11.15 inicia o tráfego a 10.31.1.5 interno (11.11.11.22) e é autenticado através do RADIUS (o tráfego de entrada usa a lista de servidor “entrante” que inclui o servidor Radius 171.68.118.115).

[PIX debug - Boa autenticação - TACACS+](#)

O exemplo abaixo do PIX debug das mostras com boa autenticação:

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

O exemplo abaixo do PIX debug das mostras com autenticação inválida (username ou senha). O usuário vê quatro conjuntos de nome de usuário/senha. Os indicadores de seguinte mensagem: “Erro: número máximo de tentativas excedidas”.

```

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 debug - Pode sibilar, mas nenhuma resposta - TACACS+](#)

O exemplo abaixo do PIX debug das mostras para um servidor que aceita ping que não esteja falando ao PIX. O usuário vê o username uma vez, e o PIX nunca pede uma senha (este está no telnet).

```
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 debug - Não pode sibilar o server - TACACS+](#)

O exemplo abaixo do PIX debug das mostras para um server que não seja processo de ping. O usuário vê o username uma vez. O PIX nunca pede uma senha (este está no telnet). Os indicadores de seguinte mensagem: “Intervalo ao server TACACS+” e ao “erro: Número máximo de tentativas excedidas” (a configuração neste exemplo reflete um servidor falso).

```

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 debug - Boa autenticação - RAI0](#)

O exemplo abaixo do PIX debug da mostra com boa autenticação:

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 debug - Autenticação inválida (username ou senha) - RAI0

O exemplo abaixo do PIX debug das mostras com autenticação inválida (username ou senha). O usuário vê um pedido para o nome de usuário e senha. Se qualquer um é errado, a mensagem “senha incorreta” indica quatro vezes. Então, o usuário é desligado. Este problema foi atribuído o Bug ID #CSCdm46934.

```

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 debug - Daemon para baixo, não se comunicará com o PIX - RAI0](#)

O exemplo abaixo do PIX debug das mostras com um servidor que aceita ping, mas o demônio está para baixo. O server não se comunicará com o PIX. O usuário vê o username, seguido pela senha. O indicador de seguintes mensagens: “Servidor Radius falhado” e “erro: Número máximo de tentativas excedidas”.

```

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 debug - Não pode sibilar o server ou a incompatibilidade de chave/cliente - RAI0](#)

O exemplo abaixo do PIX debug das mostras para um server que não seja processo de ping ou onde lá é uma incompatibilidade de chave/cliente. O usuário vê o nome de usuário e senha. O indicador de seguintes mensagens: "Intervalo ao servidor Radius" e ao "erro: Número máximo de tentativas excedidas" (o server na configuração é por exemplo finalidades somente).

```
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

```

Autorização de adição

Porque a autorização é inválida sem autenticação, nós exigiremos a autorização para o mesmo intervalo de origem e de destino:

```

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

```

Que parte

Note que nós não adicionamos a autorização para “entrante” porque o tráfego de entrada é autenticado com RAIO, e a autorização RADIUS é inválida

A authentication e autorização debuga exemplos do PIX

PIX debug com boa autenticação e autorização bem sucedida - TACACS+

O exemplo abaixo do PIX debug da mostra com boa autenticação e autorização bem sucedida:

```

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

```

PIX debug - Boa autenticação, autorização falha - TACACS+

O exemplo abaixo do PIX debug das mostras com boa autenticação, mas autorização falha:

Aqui o usuário igualmente vê erro da mensagem “: Autorização negada”

```
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
```

Relatório de adição

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Debug olhará o mesmos se explicar é de ligar/desligar. Contudo, na altura “construído”, haverá do registro de contabilidade do “começo” enviado. Na altura “Teardown”, haverá do registro de contabilidade da “parada” enviado.

Os registros de contabilidade TACACS+ olham como o seguinte (estes são do CiscoSecure UNIX; esses no CiscoSecure NT podem ser delimitados por vírgula pelo contrário):

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

Debug olhará o mesmos se explicar é de ligar/desligar. Contudo, na altura “construiu”, do registro de contabilidade do “começo” é enviado. Na altura o “Teardown”, do registro de contabilidade da “parada” é enviado:

Os registros de contabilidade do RAIO olham como o seguinte: (estes são do CiscoSecure UNIX; esses no CiscoSecure NT podem ser delimitados por vírgula pelo contrário):

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

Uso do comando Except

Em nossa rede, se nós decidimos que um origem específica e/ou um destino não precisam a autenticação, a autorização, ou explicar, nós podemos fazer algo como o seguinte:

```
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

Se você é “com exceção” dos endereços IP de Um ou Mais Servidores Cisco ICM NT da autenticação e tem a autorização sobre, você deve igualmente excetuá-los da autorização!

Max-sessions e visualização de usuários que fizeram login

Alguns servidores de TACACS+ e RADIUS possuem recursos “max-session” ou “visualizar usuários que fizeram 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 (isto é, tem uma sessão com o PIX).

Isto funciona bem para conexões Telnet e FTP devido à natureza das conexões. Isso não funciona bem para HTTP devido à natureza da conexão. No exemplo seguinte, uma configuração de rede diferente é usada mas os conceitos são os mesmos.

Os telnet do usuário com o PIX, autenticando na maneira:

```
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
```

Porque o server não viu um registro do “começo” mas nenhum registro da “parada” (neste momento), o server mostrará 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 (que supõe as sessões máx. dos suportes de servidor), a conexão será recusada pelo server.

O usuário vai sobre com seu telnet ou negócio FTP no host de destino, a seguir nas saídas (passa os minutos 10 lá):

```
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
```

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

Contudo, o HTTP trabalha diferentemente devido à natureza do protocolo. Está abaixo um exemplo de HTTP.

O usuário consulta de 171.68.118.100 a 9.9.9.25 com o PIX:

```
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
```

O usuário lê a página da Web baixada.

O registro inicial afixado em 16:35:34, e o registro da parada afixado em 16:35:35. Esta transferência tomou o segundo (de que é; 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 quando estão lendo o página da web? No. Max-sessions ou visualizar usuários que fizeram login funcionará aqui? Não, porque o tempo de conexão (o tempo entre “Built” (Construção) e Teardown (Destrução)) em HTTP é muito curto. O registro “start” (iniciar) e “stop” (parar) é sub-segundo. Não haverá um registro do “começo” sem um registro da “parada”, desde que os registros ocorrem virtualmente no mesmo instante. Ainda haverá um “começo” e “pare” o registro enviado ao server para cada transação, se o uauth está ajustado para 0 ou algo maior. Entretanto, os usuários que efetuaram logon em visualização e máximo de sessões não funcionarão devido à natureza das conexões de HTTP.

Autenticação e habilitação no próprio PIX

A discussão anterior era do tráfego de autenticação do telnet (e o HTTP, o FTP) com o PIX. No exemplo abaixo, nós certificamo-nos de que o telnet ao pix trabalha sem autenticação sobre:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Então, nós adicionamos o comando autenticar usuários Telnetting ao PIX:

```
aaa authentication telnet console Outgoing
```

Quando os usuários Telnet ao PIX, eles forem alertados para a senha telnet (“ww”). O PIX igualmente pede o TACACS+ neste caso (desde que a lista de servidor “que parte” é usada) ou nome de usuário RADIUS e senha.

```
aaa authentication enable console Outgoing
```

Com este comando, o usuário é alertado para um nome de usuário e senha que seja enviado ao TACACS ou ao servidor Radius. Neste caso, desde que a lista de servidor “que parte” é usada, o pedido vai ao servidor de TACACS. Desde que o pacote de autenticação para permite é o mesmo que o pacote de autenticação para o início de uma sessão, o usuário pode permitir através do TACACS ou do RADIUS com o mesmo nome de usuário/senha, supor o usuário pode entrar ao PIX com TACACS ou RADIUS. Este problema foi atribuído o Bug ID #CSCdm47044.

Caso o server estiver para baixo, o usuário pode aceder ao modo enable PIX incorporando o “PIX” para o username e o normal permite a senha do PIX (“permita a senha o que quer que”). Se “permita a senha o que quer que” não está na configuração de PIX, o usuário deve incorporar o “PIX” para o username e pressionar a tecla ENTER. Se a senha da possibilidade é ajustada mas não sabida, um disco de recuperação de senha estará exigido a fim restaurar.

Autenticação no console serial

O comando `aaa authentication serial console` exige a verificação de autenticação a fim alcançar o console serial do PIX. Quando os comandos `user performs configuration` do console, mensagens do `syslog` serão cortados (se o PIX é configurado para enviar o `Syslog` a nível de `debug` a um `syslog host`). Está abaixo um exemplo do servidor de `SYSLOG`:

```
aaa authentication enable console Outgoing
```

Alterando o prompt que os usuários visualizam

Se tivermos o comando:

```
auth-prompt THIS_IS_PIX_5
```

os usuários que atravessam o PIX veem a sequência:

```
auth-prompt THIS_IS_PIX_5
```

e então, na chegada na máquina de destino final, o “`username:` ” e “`senha:` ” alerta a máquina de destino é apresentado.

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.

Personalizando a mensagem que os usuários visualizam no êxito/na falha

Se tivermos os comandos:

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

Os usuários verão o seguinte em um login bem-sucedido/falha no login com o PIX:

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

Tempo ocioso e intervalos absolutos por usuário

A quietude e os uauth timeout absolutos podem ser enviados para baixo do server TACACS+ em uma base do usuário per. Se todos os usuários em sua rede devem ter o mesmo "timeout uauth," então não execute isto! Mas, se você precisa uauths diferentes por usuário, leia sobre.

Em nosso exemplo no PIX, nós usamos o **comando timeout uauth 3:00:00**. Isto significa que uma vez que uma pessoa autentica, não terão que reauthenticate por 3 horas. Mas se nós estabelecemos um usuário com o seguinte perfil e temos a autorização de AAA TACACS sobre no PIX, a quietude e os timeouts absolutos no perfil de usuário cancelam o timeout uauth no PIX para esse usuário. Isto não significa que a sessão de Telnet com o PIX obtém desligado após a quietude/timeout absoluto. Apenas controla mesmo se a reautenticação ocorre.

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

Após a autenticação, emita um comando **show uauth** no PIX:

```
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
```

Depois que o usuário senta a quietude para um minuto, debugar no PIX mostra:

```
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
```

O usuário terá que autenticar novamente ao retornar ao mesmo host de destino ou a um host diferente.

[HTTP Virtual](#)

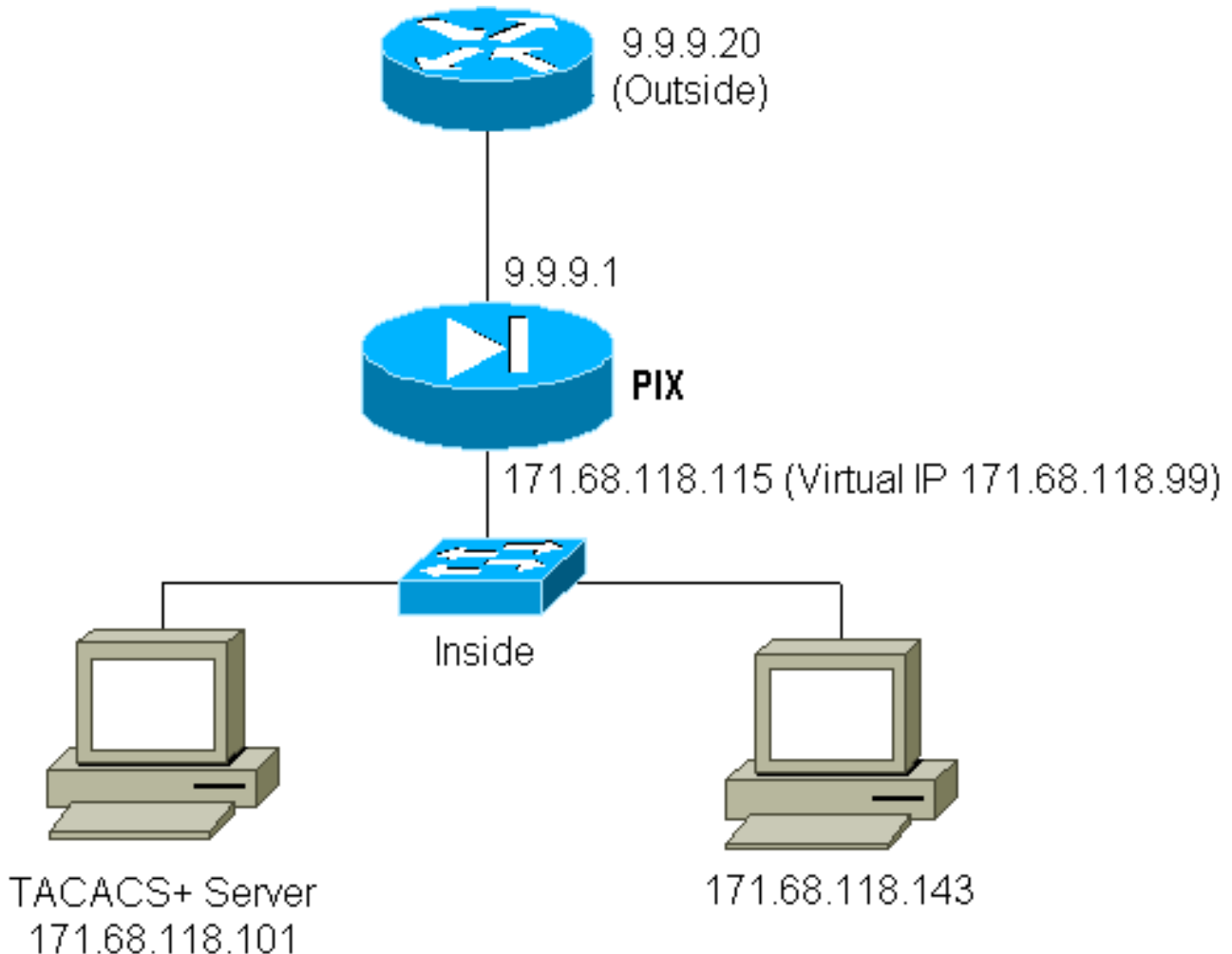
Se a autenticação é exigida em locais fora do PIX, assim como no PIX próprio, o comportamento incomum do navegador pode às vezes ser observado desde que os navegadores põem em esconderijo o nome de usuário e senha.

Para evitar isto, você pode executar o HTTP virtual adicionando um endereço do [RFC 1918](#) (isto é, um endereço que seja não-rroteável no Internet, mas válido e original para a rede interna PIX) à configuração de PIX usando o comando seguinte:

```
virtual http #.#.#.# [warn]
```

Quando o usuário tenta sair do PIX, a autenticação é necessária. Se o parâmetro de advertência estiver presente, o usuário recebe uma mensagem redirecionada. A autenticação é boa para a duração do uauth. Como indicado na documentação, não ajuste a duração do **comando timeout uauth aos segundos 0** com HTTP virtual; isso evita conexões de HTTP ao servidor da Web real.

Exemplo de saída HTTP virtual:



Saídas HTTP Virtual da configuração de PIX:

```
virtual http #.#.#.# [warn]
```

Telnet Virtual

Configurar o PIX para autenticar todo o tráfego de entrada e de saída não é uma boa ideia porque alguns protocolos, tais como o "correio," não são autenticados facilmente. Quando um mail server e um cliente tentam se comunicar com o PIX quando todo o tráfego com o PIX está sendo autenticado, o Syslog PIX para protocolos não autenticáveis mostrará mensagens como:

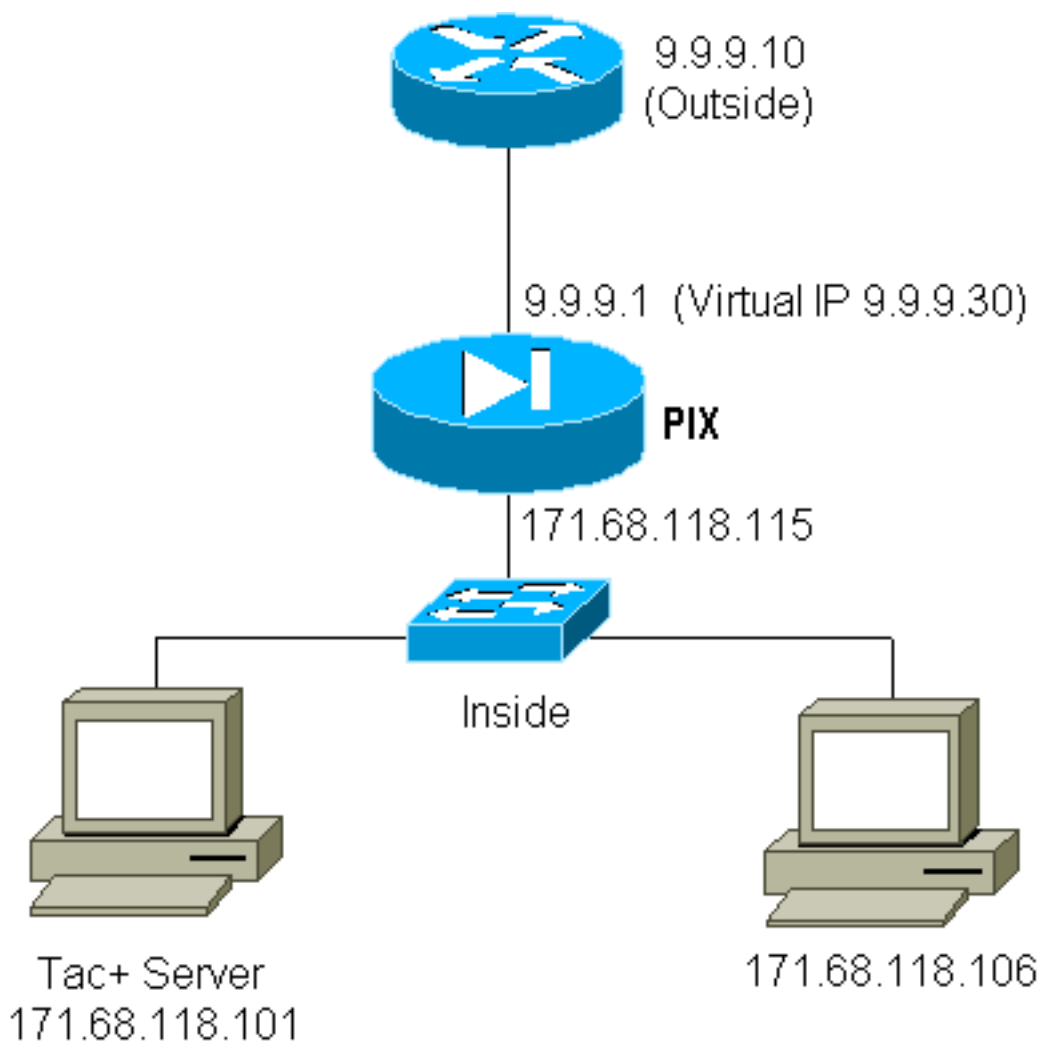
```
virtual http #.#.#.# [warn]
```

Desde que o correio e alguns outros serviços não são interativos bastante autenticar, uma solução é usar o **comando except** para a autenticação/autorização (autentique tudo à exceção da fonte/destino do mail server/cliente).

Mas se há realmente uma necessidade de autenticar algum tipo do serviço incomum, isto pode ser feito por meio do **comando virtual telnet**. Este comando permite que a autenticação ocorra ao IP de Telnet virtual. Após esta autenticação, o tráfego para o serviço incomum pode ir ao servidor real que é amarrado ao IP virtual.

Em nosso exemplo, nós queremos permitir que o tráfego da porta TCP 49 flua do host exterior 9.9.9.10 ao host interno 171.68.118.106. Porque este tráfego não é realmente authenticatable, nós estabelecemos o telnet virtual.

Entrada de telnet virtual:



Entrada de telnet virtual da configuração de PIX:

```
virtual http #.#.#.# [warn]
```

Telnet virtual de configuração de usuário do servidor TACACS+ de entrada:

```
virtual http #.#.#.# [warn]
```

Entrada de telnet virtual do PIX debug:

O usuário em 9.9.9.10 deve primeiramente autenticar telnetting ao endereço de 9.9.9.30 no PIX:

```
virtual http #.#.#.# [warn]
```

Após a autenticação bem sucedida, o comando **show uauth** mostra que o usuário tem o “tempo no medidor”:

```
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
```

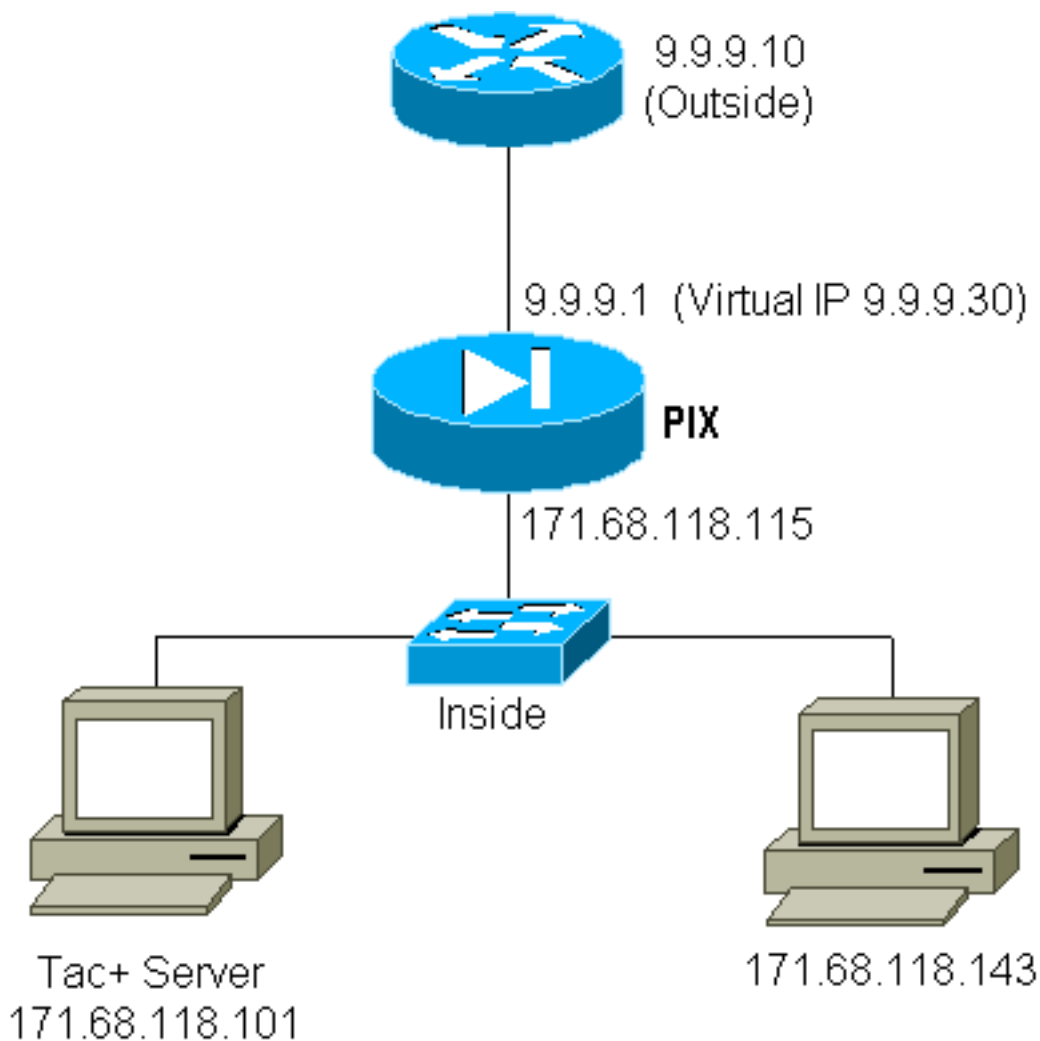
E quando o dispositivo em 9.9.9.10 quiser enviar o tráfego TCP/49 ao dispositivo em 171.68.118.106:

```
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
```

Saídas telnet virtuais:

Desde que o tráfego de saída é permitido à revelia, não estático é exigido para o uso das saídas telnet virtuais. No exemplo seguinte, o usuário interno em 171.68.118.143 quer o telnet a 9.9.9.30 virtual e autentica-o. A conexão Telnet é deixada cair imediatamente.

Uma vez que autenticado, o tráfego TCP é permitido de 171.68.118.143 ao server em 9.9.9.10:



Saídas telnet virtuais da configuração de PIX:

```
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	

Saídas telnet virtuais do PIX debug:

```
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	

[Desconexão de Telnet Virtual](#)

Quando o usuário Telnets ao IP de Telnet virtual, o comando **show uauth** mostrar seu uauth. Se o usuário quer impedir que o tráfego vá completamente depois que sua sessão está terminada (quando houver um tempo deixado no uauth), precisa o telnet ao IP de Telnet virtual outra vez. Esta ação desliga a sessão.

Autorização da porta

Você pode exigir a autorização em uma faixa de porta. No exemplo seguinte, a autenticação foi exigida ainda para todo o de partida, mas a autorização é exigida somente para portas TCP 23-49.

Configuração de PIX:

```
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
```

Assim, quando nós telnet de 171.68.118.143 a 9.9.9.10, authentication e autorização ocorreremos porque a porta 23 do telnet está na escala 23-49. Quando nós fazemos uma sessão de HTTP de 171.68.118.143 a 9.9.9.10, nós ainda temos que autenticar, mas o PIX não pede o server TACACS+ para autorizar o HTTP porque 80 não estão na escala 23-49.

TACACS+ Configuração do programa gratuito de servidor

```
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
```

Note que o PIX está enviando "cmd=tcp/23-49" e "cmd-arg=9.9.9.10" ao server TACACS+.

Debugar no PIX:

```
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
```

Informações Relacionadas

- [Sustentação do produto do Software do firewall Cisco PIX](#)
- [Referências do comando Cisco Secure PIX Firewall](#)