Configurando PIX 5.1.x: TACACS+ e RADIUS

Índice

Introdução

O RAIO e a autenticação TACACS+ podem ser feitos para o FTP, o telnet, e as conexões de HTTP. Em geral, é possível implementar autenticação para outros protocolos menos comuns. A autorização TACACS+ é apoiada; A autorização de RADIUS não é. As mudanças no Authentication, Authorization, and Accounting (AAA) PIX 5.1 sobre a versão anterior incluem a autenticação extendida (XAUTH)-- autenticação dos túneis de IPsec do Cisco Secure VPN Client 1.1.

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

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

Informações de Apoio

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.
- A contabilidade é o que o usuário fez.

Supõe que você tem cem usuários internos e você para querer quer somente seis 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 seis usuários a identificação no servidor de segurança TACACS+/RADIUS. Com autenticação simples, estes seis usuários poderiam ser autenticados com nome de usuário e senha, a seguir saem. Os outros usuários da noventa-quatro 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 seis usuários poderiam fazer o FTP, o telnet, ou o HTTP.

Mas supõe *um d*estes seis usuários, “Festus,” não é ser confiado. Você gostaria de permitir que

Festus 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. Isto é somente válido com TACACS+. Quando nós adicionamos a *autorização ao* PIX, o PIX primeiramente envia o nome de usuário e senha de Festus ao servidor de segurança, a seguir envia a um pedido de autorização que diz ao servidor de segurança o que o "*comando*" Festus está tentando fazer. Com a instalação do server corretamente, Festus podia ser permitido a "ftp 1.2.3.4" mas seria negado 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 um prompt de nome de usuário ativado e, em seguida, a solicitação 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 de entrar em **local_username@remote_username** para o username e em **local_password@remote_password** para a senha. O PIX envia o local_username e o local_password ao servidor de segurança local, e se a autenticação (e a autorização) são bem sucedidas no PIX/server, o remote_username e o remote_password é passado ao servidor FTP de destino além.
- **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 que dispara no nome de usuário oculto e na senha ao PIX, que então para a frente isto ao Authentication Server. O Syslog e/ou o server PIX debugam mostras este fenômeno. Se o telnet e o FTP parecem trabalhar normalmente, mas as conexões de HTTP não fazem, eis porque.
- **Túnel** - Ao tentar escavar um túnel sobre o tráfego de IPSec na rede com o cliente VPN e o Xauth, uma caixa cinzenta para a "autenticação de usuário para a nova conexão" é indicada para o username/senha.**Nota:** Esta autenticação é começo apoiado com o Cisco Secure VPN Client 1.1. Se o menu do **ajuda > sobre** não mostra a versão 2.1.x ou mais recente, este não trabalha.

Configurações de servidor de segurança utilizadas para todos os cenários

Configuração de servidor de TACACS segura de Cisco UNIX

Nesta seção, você é presentado com a informação para configurar seu servidor de segurança.

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 segura dos RADIUS UNIX de Cisco

Use o GUI para adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT e a chave PIX à lista do servidor do acesso de rede (NAS).

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

RAIO do Cisco Secure ACS for Windows 2.x

Use estas etapas para configurar o RAIO do Cisco Secure ACS for Windows 2.x.

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 endereço IP de Um ou Mais Servidores Cisco ICM NT PIX na seção de configuração de NAS GUI.

EasyACS TACACS+

A documentação easyacs descreve a instalação.

1. Na seção de grupo, **executivo do shell do** clique para dar privilégios de exec.
2. Para adicionar a autorização ao PIX, clique sobre **comandos deny unmatched ios na** parte inferior da instalação de grupo.
3. Selecione o **comando add/edit new** para cada comando que você deseja permitir, por exemplo, o **telnet**.
4. Se Telnetting aos locais específicos é permitido, preencha o endereço IP de Um ou Mais Servidores Cisco ICM NT na seção de argumento no formulário “licença #.#.#.#”. Se não, permitam Telnetting, o clique **permite que 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.

Cisco 2.x seguro TACACS+

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

1. Na seção de grupo, clique sobre o **executivo do shell** para dar privilégios de exec.
2. Para adicionar a autorização ao PIX, na parte inferior da instalação de grupo, clica **comandos deny unmatched ios**.
3. **Comando add/edit new** seleto para cada comando que você deseja permitir (por exemplo, **telnet**).
4. Para permitir Telnetting aos locais específicos, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT à seção de argumento no formulário “licença #.#.#.#”. Para permitir Telnetting a todo o local, 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. Assegure-se de que o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX esteja adicionado na seção gui da configuração de NAS.

Configuração de servidor Livingston RADIUS

Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX e a chave aos clientes arquiva.

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

Configuração de servidor Merit RADIUS

Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT PIX e a chave aos clientes arquiva.

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

TACACS+ Configuração do programa gratuito de servidor

```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
```

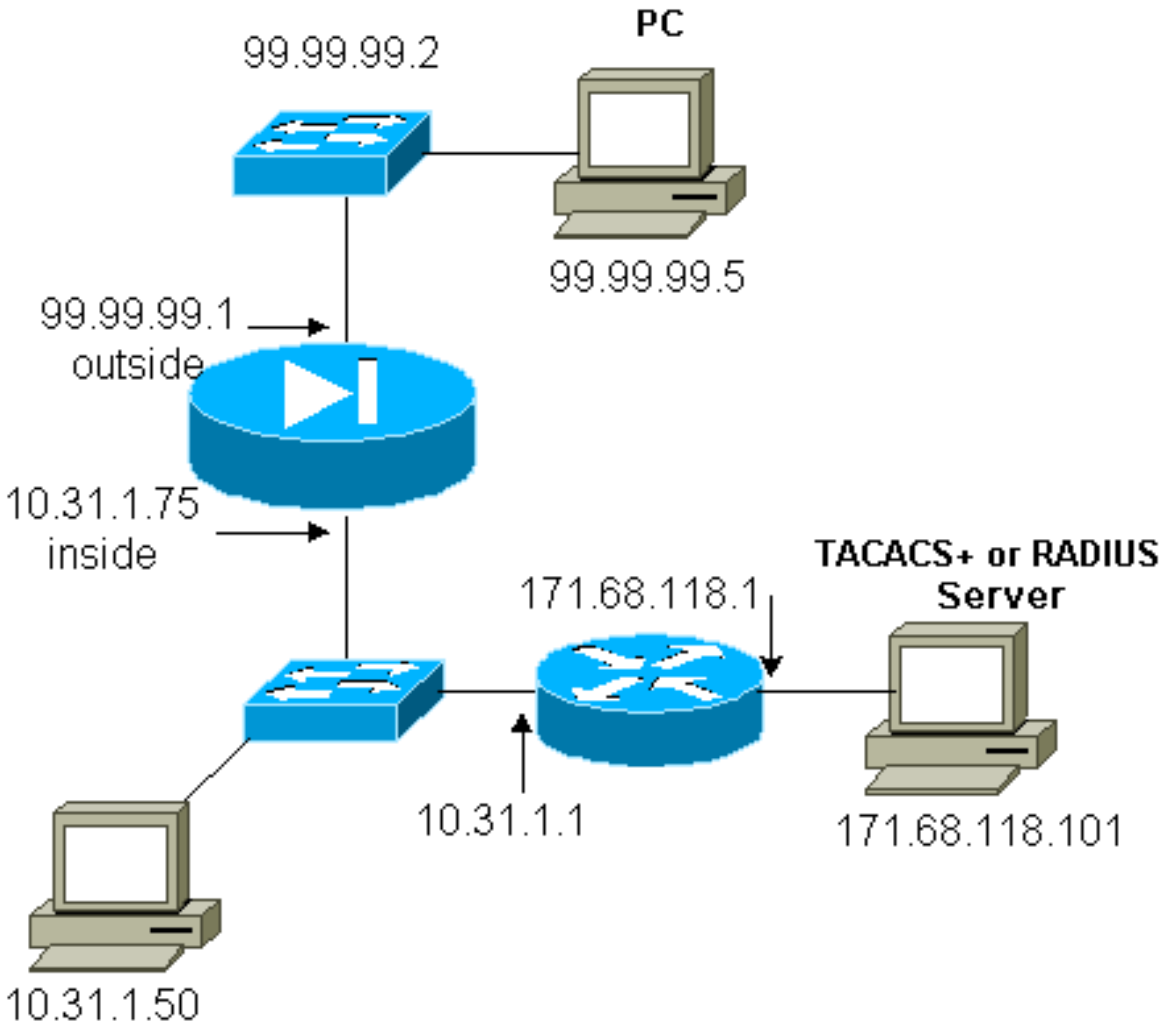
```
}

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

Nota: A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- Certifique-se que a configuração de PIX está trabalhando antes de adicionar o AAA. Se você não pode passar o tráfego antes de instituir a authentication e autorização, você não poderá fazer tão mais tarde.
- Enable que entra o PIX.A eliminação de erros do console de registro não deve ser usada pesadamente em um sistema carregado.A depuração de registro colocado em buffer pode ser usada; em seguida, execute o comando show logging.O registro também pode ser enviado a um servidor syslog e examinado lá.
- Gire sobre debugar no TACACS+ ou nos servidores Radius (todos os server têm esta opção).

Diagrama de Rede



Configuração de PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
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
no logging standby
logging console debugging no logging monitor no logging
buffered no logging trap no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu pix/intf2
1500 ip address outside 99.99.99.1 255.255.255.0 ip
address inside 10.31.1.75 255.255.255.0 ip address
pix/intf2 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 arp timeout 14400 global (outside) 1
```

```
99.99.99.7-99.99.99.10 netmask 255.255.255.0 nat
(inside) 1 10.31.1.0 255.255.255.0 0 0 static
(inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0 conduit permit icmp any any conduit
permit tcp any any conduit permit udp any any route
outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 route inside
171.68.120.0 255.255.255.0 10.31.1.1 1 timeout xlate
3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00 timeout uauth 0:05:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.101 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.101 cisco timeout 5 aaa authentication
include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include telnet inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
no snmp-server location no snmp-server contact snmp-
server community public no snmp-server enable traps
floodguard enable telnet timeout 5 terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca : end
[OK]
```

Exemplos de debug de autenticação a partir de PIX

Esta seção mostra que as amostras de autenticação debugam para várias encenações.

Entrada

O usuário externo em 99.99.99.2 inicia o tráfego a 10.31.1.50 interno (99.99.99.99) e é autenticado com o TACACS (isto é, o tráfego de entrada usa a lista de servidor “AuthInbound” que inclui o servidor de TACACS 171.68.118.101).

PIX debug - Boa autenticação - TACACS+

O exemplo abaixo mostra um PIX debug com boa autenticação:

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

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

O exemplo abaixo mostra um PIX debug com autenticação inválida (username ou senha). O usuário vê três conjuntos de nome de usuário/senha, seguidos por esta mensagem: `Erro: número`

```
máximo de tentativas excedidas.

109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX debug - Pode sibilar o server, nenhuma resposta - TACACS+

O exemplo abaixo mostra um PIX debug onde o server seja processo de ping, mas o discurso ao PIX. O usuário vê o username uma vez, mas o PIX nunca pede uma senha (este está no telnet). O usuário vê o `erro: Número máximo de tentativas excedidas.`

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX debug - Incapaz de sibilar o server - TACACS+

O exemplo abaixo mostra a um PIX debug onde o server não é processo de ping. O usuário vê o username uma vez, mas o PIX nunca pede uma senha (este está no telnet). Os seguintes mensagens são indicados: `Intervalo ao server` e ao `erro TACACS+: Número máximo de tentativas excedidas` (um servidor falso foi trocado dentro a configuração).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX debug - Boa autenticação - RAIO

O exemplo abaixo mostra um PIX debug com boa autenticação:

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

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

O exemplo abaixo mostra um PIX debug com autenticação inválida (username ou senha). O usuário vê o pedido para um nome de usuário e senha, e tem três oportunidades de entrar nestes. Quando a entrada é mal sucedida, o seguinte mensagem está indicado: `Erro: número máximo de tentativas excedidas.`

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX debug - Pode sibilar o server, o demônio para baixo - RAIO

O exemplo abaixo mostra a um PIX debug onde o server é processo de ping, mas o demônio está para baixo e não se comunicará com o PIX. O usuário vê o username, então senha, a `falha de mensagem do servidor Radius`, e o `erro: Número máximo de tentativas excedidas`. mensagem de erro.

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX debug - Incapaz de sibilar o server ou a incompatibilidade de chave/cliente - RAIO

O exemplo abaixo mostra a um PIX debug onde o server não é processo de ping ou há um cliente/incompatibilidade de chave. O usuário vê um username, a senha, o `intervalo à` mensagem do `servidor Radius`, e o `erro: O número máximo de` mensagem `excedida tentativas um` servidor falso foi trocado dentro a configuração).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Autorização de adição

Se você decide adicionar a autorização, desde que a autorização é inválida sem autenticação, você precisa de exigir a autorização para o mesmo intervalo de origem e de destino.

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Note que você não adiciona a autorização para que parte porque o tráfego de saída é autenticado com RAIO, e a autorização RADIUS é inválida.

A authentication e autorização debuga exemplos do PIX

PIX debug - Boa autenticação e autorização bem sucedida - TACACS+

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

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX debug - Boa autenticação, autorização falha - TACACS+

O exemplo abaixo mostra o PIX debug com boa autenticação mas autorização falha. Aqui o usuário igualmente vê o erro de mensagem：`Autorização negada.`

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Relatório de adição

TACACS+

aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

Freeware TACACS+ output:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

Radius da merit output:

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Uso do comando Exclude

Se nós adicionamos uma outra parte externa do host (em 99.99.99.100) a nossa rede, e este host está confiado, você pode exclui-los da authentication e autorização com os comandos seguintes:

aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound

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 “start" (de relatório gerado, mas não há um registro "stop", o servidor TACACS+ ou RADIUS admite que a pessoa ainda está conectada (ou seja, o usuário tem uma sessão no 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.

Usuário estabelece um Telnet por meio do PIX, autenticando no caminho:

```
   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 inicial 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. estão ajustadas a **1 no** server para este usuário (que supõe as sessões máx. dos suportes de servidor), a conexão está recusada pelo server.

O usuário vai aproximadamente seu telnet ou negócio FTP no host de destino, a seguir nas saídas (passa dez minutos 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
```

Seja o uauth 0 (isto é, autenticar sempre) ou mais (autenticar uma vez e não mais durante o período de uauth), um registro de contabilidade será cortado para cada local acessado.

O HTTP trabalha de forma diferente 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:

```
(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 a página da Web baixada.

O registro de início foi lançado às 16:35:34, e o registro de interrupção, às 16:35:35. Esse download levou um segundo (ou seja, houve menos de um segundo entre o início e o término da gravação). O usuário continua conectado ao site e a conexão continua aberta quando o usuário está lendo a página da Web? Não. Max-sessions ou visualizar usuários que fizeram login funcionará aqui? Não, porque o tempo de conexão (o tempo entre “Built” (Construção) e Teardown (Destruição)) em HTTP é muito curto. O registro de início e de parada é secundário-segundo. Não há um registro inicial sem um registro da parada desde que os registros ocorrem virtualmente no mesmo instante. Ainda haverá um registro de início e de parada 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 refere-se ao tráfego de autenticação do telnet (e o HTTP, o FTP) com o PIX. Assegure o telnet aos trabalhos PIX sem autenticação sobre:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

Adicionar então o comando autenticar usuários Telnetting ao PIX:

```
aaa authentication telnet console AuthInbound
```

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. Neste caso desde que a lista de servidor do AuthInbound é usada, o PIX pede o nome de usuário e senha TACACS+.

Se o server está para baixo, você pode alcançar o PIX incorporando o **pix** para o username, e então a senha da possibilidade (**permita a senha** *o que quer que*). Com o comando:

```
aaa authentication enable console AuthInbound
```

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 do AuthInbound é usada, o PIX pede o nome de usuário e senha TACACS+.

Desde que o pacote de autenticação para permite é o mesmo que o pacote de autenticação para o início de uma sessão, se o usuário pode entrar ao PIX com TACACS ou RAIO, eles pode permitir através do TACACS ou do RAIO com o mesmo nome de usuário/senha. Este problema foi atribuído a identificação de bug Cisco CSCdm47044 (clientes registrados somente).

Se o server está para baixo, você pode alcançar o modo enable PIX entrando o **pix** para o username e o normal permite a senha do PIX (**permita a senha** *o que quer que*). Caso a habilitação de senha não esteja na configuração PIX, digite pix como nome de usuário e pressione Enter. Se a senha da possibilidade é ajustada mas não sabida, um disco de recuperação de senha precisa de ser construído para restaurar a senha.

Alterando o prompt que os usuários visualizam

Se você tem o comando:

```
auth-prompt PIX_PIX_PIX
```

os usuários que atravessam o PIX veem a seguinte sequência:

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

Na chegada no destino final, os usuários veriam o username: e senha: alerta indicada pela máquina de destino. 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 o youh tem os comandos:

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

então os usuários veem a seguinte sequência em um login bem-sucedido/falha no login com o PIX:

```
PIX_PIX_PIX
   Username: asjdkl Password: "BAD_AUTH" "PIX_PIX_PIX" Username: cse Password: "GOOD_AUTH"
```

Tempo ocioso e intervalos absolutos por usuário

Esta função atualmente não está trabalhando e o problema foi atribuído a identificação de bug Cisco CSCdp93492 (clientes registrados somente).

HTTP Virtual

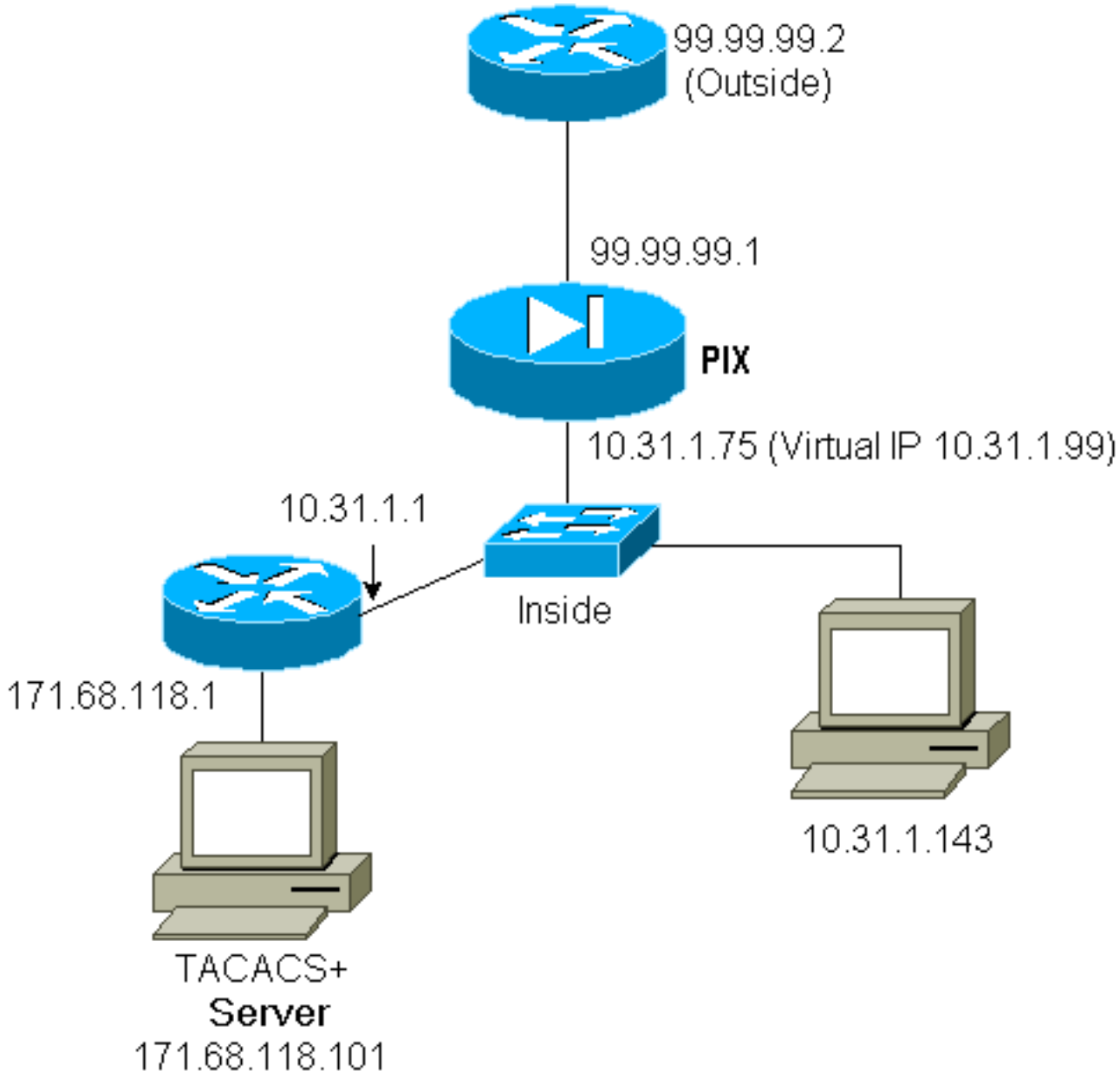
Se a autenticação for necessária em locais fora do PIX, bem como no próprio PIX, um comportamento incomum do navegador poderá ser observado algumas vezes, uma vez que os navegadores armazenam o nome do usuário e a senha em cache.

Para evitar isto, você pode executar o HTTP virtual adicionando um endereço do RFC 1918 (isto é, um endereço que seja não-roteável 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 durante o tempo 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:

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 01:00:00 aaa
authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa-server
RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound (inside)
host 171.68.118.101 cisco timeout 5 virtual http 10.31.1.99
```

Telnet Virtual

Épossível configurar o PIX para autenticar toda de entrada e de partida, mas 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 autenticável mostra mensagens como:

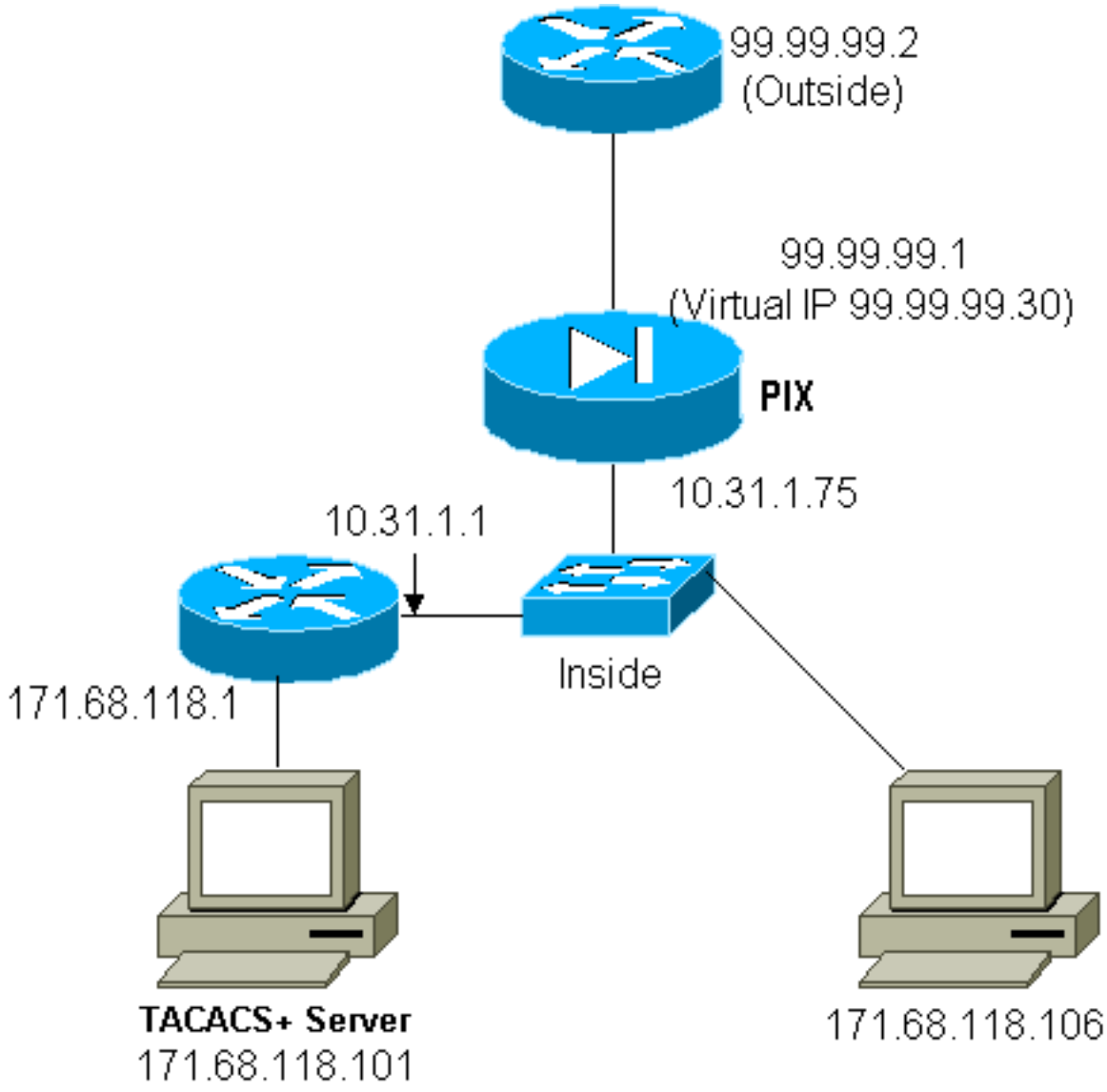
```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Contudo, se há realmente uma necessidade de autenticar algum tipo do serviço incomun, isto

pode ser feito por meio do **comando virtual telnet**. Este comando permite que a autenticação ocorra ao endereço IP telnet virtual. Após esta autenticação, o tráfego para o serviço incomun pode ir ao servidor real.

Neste exemplo, você quer o tráfego da porta TCP 49 fluir do host exterior 99.99.99.2 ao host interno 171.68.118.106. Desde que este tráfego não é realmente authenticatable, estabelecer um telnet virtual. Para o telnet virtual, deve haver uma estática associada. Aqui, 99.99.99.20 e 171.68.118.20 são endereços virtuais.

Entrada de Telnet Virtual



Entrada de telnet virtual da configuração de PIX

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 static
(inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0 static (inside,outside)
99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.20 eq
telnet any conduit permit tcp host 99.99.99.30 eq tacacs any aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+ aaa-server Incoming (inside) host 171.68.118.101 cisco
timeout 5 aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming virtual telnet
99.99.99.20
```

Entrada de telnet virtual do PIX debug

O usuário em 99.99.99.2 deve primeiramente autenticar por Telnetting ao endereço de 99.99.99.20 no PIX:

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

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 2 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

E quando o dispositivo em 99.99.99.2 quiser enviar o tráfego TCP/49 ao dispositivo em 171.68.118.106:

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

A autorização pode ser adicionada:

```
aaa authorization include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

de modo que quando o tráfego TCP/49 for tentado com o PIX, o PIX igualmente envie a pergunta da autorização ao server:

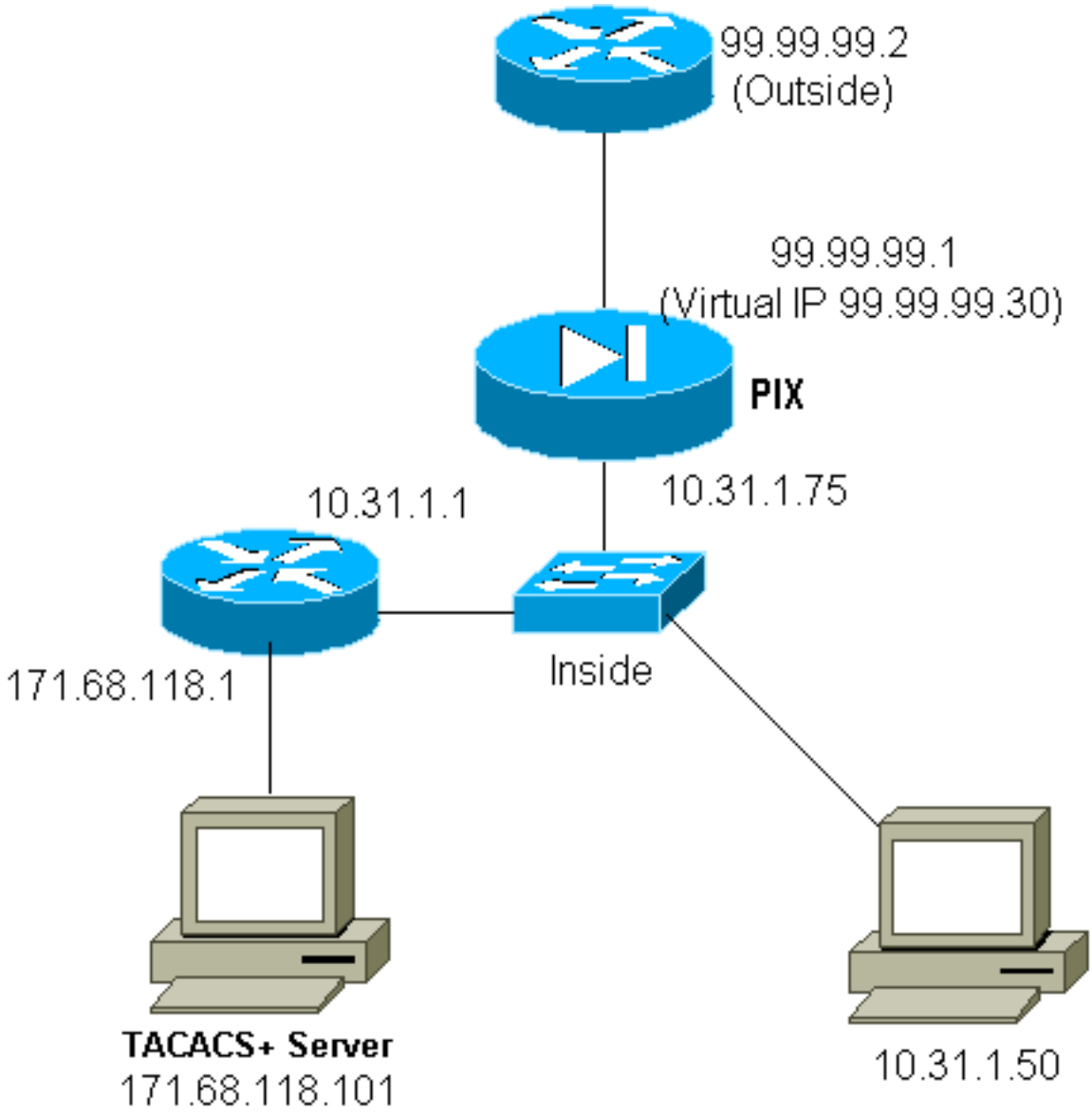
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

No server TACACS+, isto é visto como:

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

Saída Telnet Virtual

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 10.31.1.50 Telnets a 99.99.99.30 virtual e autentica; a conexão Telnet é deixada cair imediatamente. Uma vez que autenticado, o tráfego TCP é permitido de 10.31.1.50 ao server em 99.99.99.2:



Saídas telnet virtuais da configuração de PIX:

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 0:05:00 absolute aaa-
server RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 171.68.118.101 cisco timeout 5 aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound virtual telnet 99.99.99.30
```

Nota: Não há nenhuma autorização desde que este é RAIO.

Saídas telnet virtuais do PIX debug:

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
```

```
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

Desconexão de Telnet Virtual

Quando os usuários Telnet ao endereço IP telnet virtual, o **comando show uauth** mostrarem seu uauth. Se os usuários querem impedir que o tráfego vá completamente depois que suas sessões estão terminadas quando há um tempo deixado no uauth, precisam o telnet ao endereço IP telnet virtual outra vez. Esta ação desliga a sessão.

Após a primeira autenticação:

```
 pix3# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'pixuser' at 10.31.1.50, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 109005:
Authentication succeeded for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 on interface
inside
```

Após a segunda autenticação (isto é, o furo é fechado firmado):

```
 pix3# show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

Autorização da porta

A autorização é permitida intervalos de porta (como o TCP/30-100). Se o telnet virtual está configurado no PIX e na autorização para uma faixa de porta, uma vez que o furo está aberto com telnet virtual, o PIX emite um **comando tcp/30-100 ao** servidor para autorização TACACS+:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0 conduit permit tcp
host 99.99.99.75 host 99.99.99.2 static (inside,outside) 99.99.99.75 10.31.1.50 netmask
255.255.255.255 0 0 virtual telnet 99.99.99.75 aaa authentication include any inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound virtual telnet 99.99.99.30
```

Programa gratuito de configuração de servidor TACACS+:

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

Relatório de AAA para tráfego diferente de HTTP, FTP e Telnet

Após ter-se certificado do telnet virtual trabalhado para permitir o tráfego TCP/49 ao host dentro da rede, nós decidimos que nós quisemos esclarecer isto, assim que nós adicionamos:

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

Isto conduz a ter um registro de contabilidade cortado quando o tráfego tcp/49 vai completamente (este exemplo é do freeware TACACS+):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Autenticação estendida (Xauth)

Configurações de exemplo

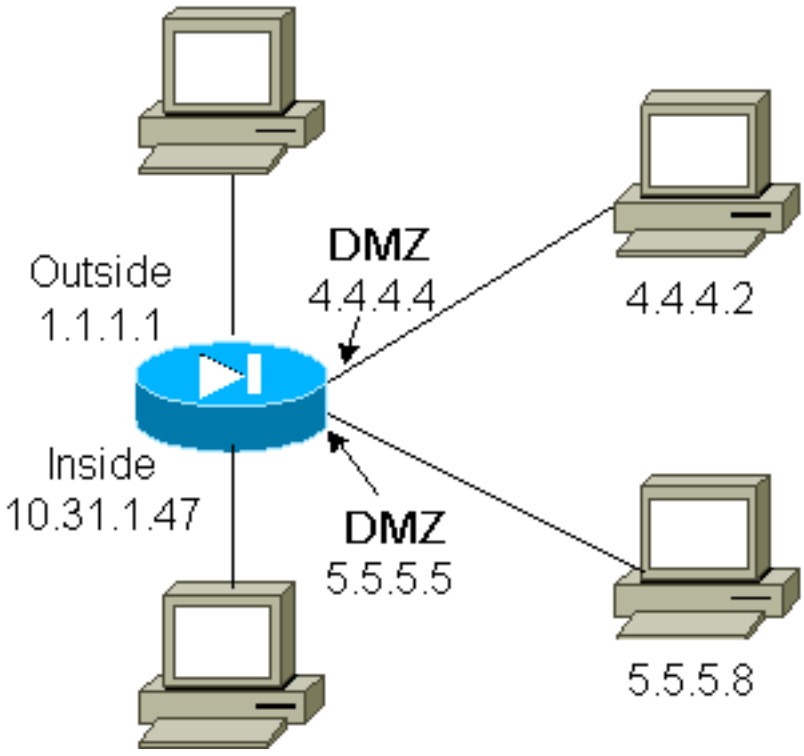
- Terminando os túneis de IPSec de várias interfaces de firewall de PIX do Cisco Secure com Xauth
- IPsec entre o firewall PIX segura Cisco e um cliente VPN com autenticação extendida

Autenticação no DMZ

Para autenticar os usuários que vão de uma relação DMZ a outra, diga o PIX para autenticar o tráfego para as interfaces nomeada. Em nosso PIX o arranjo é:

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

Diagrama de Rede



Configuração de PIX

Nós queremos autenticar o tráfego do telnet entre pix/intf4 e pix/intf5:

```
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3 security15) nameif ethernet4 pix/intf4
security20 nameif ethernet5 pix/intf5 security25 ip address outside 1.1.1.1 255.255.255.0 ip
address inside 10.31.1.47 255.255.255.0 (ip address pix/intf2 127.0.0.1 255.255.255.255 ip
address pix/intf3 127.0.0.1 255.255.255.255) ip address pix/intf4 4.4.4.4 255.255.255.0 ip
address pix/intf5 5.5.5.5 255.255.255.0 static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask
255.255.255.255 0 0 aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa-server TACACS+ protocol tacacs+ aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Relatório Xauth

Se o **comando sysopt connection permit-ipsec**, não o **comando sysopt ipsec pl-compatible**, é configurado no PIX com Xauth, explicar é válido para conexões de TCP, mas não ICMP ou UDP.

Informações Relacionadas

- Página de Suporte do Produto PIX
- Referências de comando PIX
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Página de suporte de UNIX Cisco Secure
- Cisco Secure ACS para página de suporte do Windows
- Suporte Técnico - Cisco Systems