Configurazione di PIX 5.0.x: TACACS+ e RADIUS

Sommario

Introduzione

L'autenticazione RADIUS e TACACS+ può essere eseguita per le connessioni FTP, Telnet e HTTP. In genere, è possibile eseguire l'autenticazione per altri protocolli TCP meno comuni.

L'autorizzazione TACACS+ è supportata. L'autorizzazione RADIUS non è valida. Le modifiche apportate all'autenticazione, all'autorizzazione e all'accounting (AAA) PIX 5.0 rispetto alla versione precedente includono l'accounting AAA per il traffico diverso da HTTP, FTP e Telnet.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Autenticazione e autorizzazione

- L'autenticazione corrisponde all'utente.
- L'autorizzazione è ciò che l'utente può fare.
- L'autenticazione *è* valida senza autorizzazione.
- L'autorizzazione *non* è valida senza autenticazione.

Si supponga, ad esempio, di avere un centinaio di utenti all'interno e che si desideri che solo sei di questi utenti siano in grado di eseguire operazioni FTP, Telnet o HTTP all'esterno della rete. Indicare al PIX di autenticare il traffico in uscita e fornire a tutti e sei gli utenti gli ID sul server di sicurezza TACACS+/RADIUS. Con l'*autenticazione* semplice, questi sei utenti possono essere autenticati con nome utente e password, quindi uscire. Gli altri 94 utenti non sono in grado di uscire. Il PIX chiede all'utente di immettere nome utente/password, quindi passa il nome utente e la password al server di sicurezza TACACS+/RADIUS. A seconda della risposta, apre o nega la connessione. Questi sei utenti possono eseguire operazioni FTP, Telnet o HTTP.

D'altra parte, supponiamo che *uno* di questi tre utenti, "Terry", non debba essere ritenuto affidabile. Si desidera consentire a Terry di eseguire FTP, ma non HTTP o Telnet verso l'esterno. Ciò significa che è necessario aggiungere l'*autorizzazione*. Ciò significa autorizzare *ciò che* gli utenti possono fare oltre ad autenticare *chi* sono. Quando si aggiunge un'*autorizzazione* al PIX, il PIX invia prima il nome utente e la password di Terry al server di sicurezza, quindi invia una richiesta di autorizzazione per comunicare al server di sicurezza il "*comando*" che Terry sta tentando di eseguire. Se il server è configurato correttamente, è possibile consentire a Terry di utilizzare "FTP 1.2.3.4", ma non di utilizzare "HTTP" o "Telnet".

Caratteristiche visualizzate dall'utente con Autenticazione/Autorizzazione attivata

Quando si prova a passare dall'interno all'esterno (o viceversa) con autenticazione/autorizzazione su:

- **Telnet**: l'utente visualizza un prompt con il nome utente seguito da una richiesta di password. Se l'autenticazione (e l'autorizzazione) hanno esito positivo sul PIX/server, all'utente vengono richiesti nome utente e password dall'host di destinazione oltre.
- **FTP** - Viene visualizzato il prompt del nome utente. L'utente deve immettere "local_username@remote_username" come nome utente e "local_password@remote_password" come password. Il PIX invia i valori "local_username" e "local_password" al server di sicurezza locale e, se l'autenticazione (e l'autorizzazione) hanno esito positivo sul PIX/server, "remote_username" e "remote_password" vengono passati al server FTP di destinazione oltre.
- **HTTP** - Finestra visualizzata nel browser che richiede nome utente e password. Se l'autenticazione (e l'autorizzazione) hanno esito positivo, l'utente arriva al sito Web di destinazione dopo. Tenere presente che **i browser memorizzano nella cache i nomi utente e le password.**. Se si ritiene che il PIX debba avere un timeout di una connessione HTTP, ma non lo sta facendo, è probabile che la riautenticazione sia effettivamente in corso con il browser che "riprende" il nome utente e la password memorizzati nella cache al PIX, che

quindi inoltra questo al server di autenticazione. Questo fenomeno viene visualizzato nel syslog PIX e/o nel debug del server. Se le connessioni Telnet e FTP sembrano funzionare normalmente, ma le connessioni HTTP no, è per questo motivo che.

Configurazioni del server di sicurezza utilizzate per tutti gli scenari

Configurazione server TACACS Cisco Secure UNIX

Accertarsi di disporre dell'indirizzo IP PIX o del nome di dominio completo e della chiave nel file 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 .*
}
}
}
```

Configurazione server Cisco Secure UNIX RADIUS

Utilizzare l'interfaccia utente grafica (GUI) per aggiungere l'IP e la chiave PIX all'elenco dei server di accesso alla rete (NAS).

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

```
}
}
```

Cisco Secure Windows 2.x RADIUS

Attenersi alla procedura seguente:

1. Ottenere una password nella sezione User Setup GUI.
2. Dalla sezione GUI di Configurazione gruppo, impostare l'attributo 6 (Service-Type) su Login o Administrative.
3. Aggiungere l'indirizzo IP PIX nell'interfaccia grafica di configurazione NAS.

EasyACS TACACS+

Nella documentazione di EasyACS viene descritta la configurazione.

1. Nella sezione gruppo fare clic su **Shell exec** per assegnare i privilegi di esecuzione.
2. Per aggiungere l'autorizzazione al PIX, fare clic su **Deny unmatched IOS commands** in fondo all'impostazione del gruppo.
3. Selezionare **Aggiungi/Modifica nuovo comando** per ogni comando che si desidera consentire (ad esempio, Telnet).
4. Se si desidera consentire Telnet a siti specifici, immettere gli indirizzi IP nella sezione degli argomenti nel formato "allow #.#.#.#". Per consentire Telnet a tutti i siti, fare clic su **Consenti tutti gli argomenti non in elenco**.
5. Fare clic su **Comando Fine modifica**.
6. Eseguire i passaggi da 1 a 5 per ogni comando consentito, ad esempio Telnet, HTTP o FTP.
7. Aggiungere l'indirizzo IP PIX nella sezione NAS Configuration GUI.

Cisco Secure 2.x TACACS+

L'utente ottiene una password nella sezione User setup GUI.

1. Nella sezione gruppo fare clic su **Shell exec** per assegnare i privilegi di esecuzione.
2. Per aggiungere l'autorizzazione al PIX, fare clic su **Deny unmatched IOS commands** in fondo all'impostazione del gruppo.
3. Selezionare **Aggiungi/Modifica nuovo comando** per ogni comando che si desidera consentire, ad esempio Telnet.
4. Se si desidera consentire Telnet a siti specifici, immettere allow IP(s) nel rettangolo dell'argomento (ad esempio, "allow 1.2.3.4"). Per consentire Telnet a tutti i siti, fare clic su **Consenti tutti gli argomenti non in elenco**.
5. Fare clic sul **comando fine modifica**.
6. Eseguire i passaggi precedenti per ogni comando consentito, ad esempio Telnet, HTTP e/o FTP.
7. Aggiungere l'indirizzo IP PIX nella sezione NAS Configuration GUI.

Configurazione server RADIUS Livingston

Aggiungere l'IP e la chiave PIX al file client.

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

Configurazione server RADIUS di tipo Merit

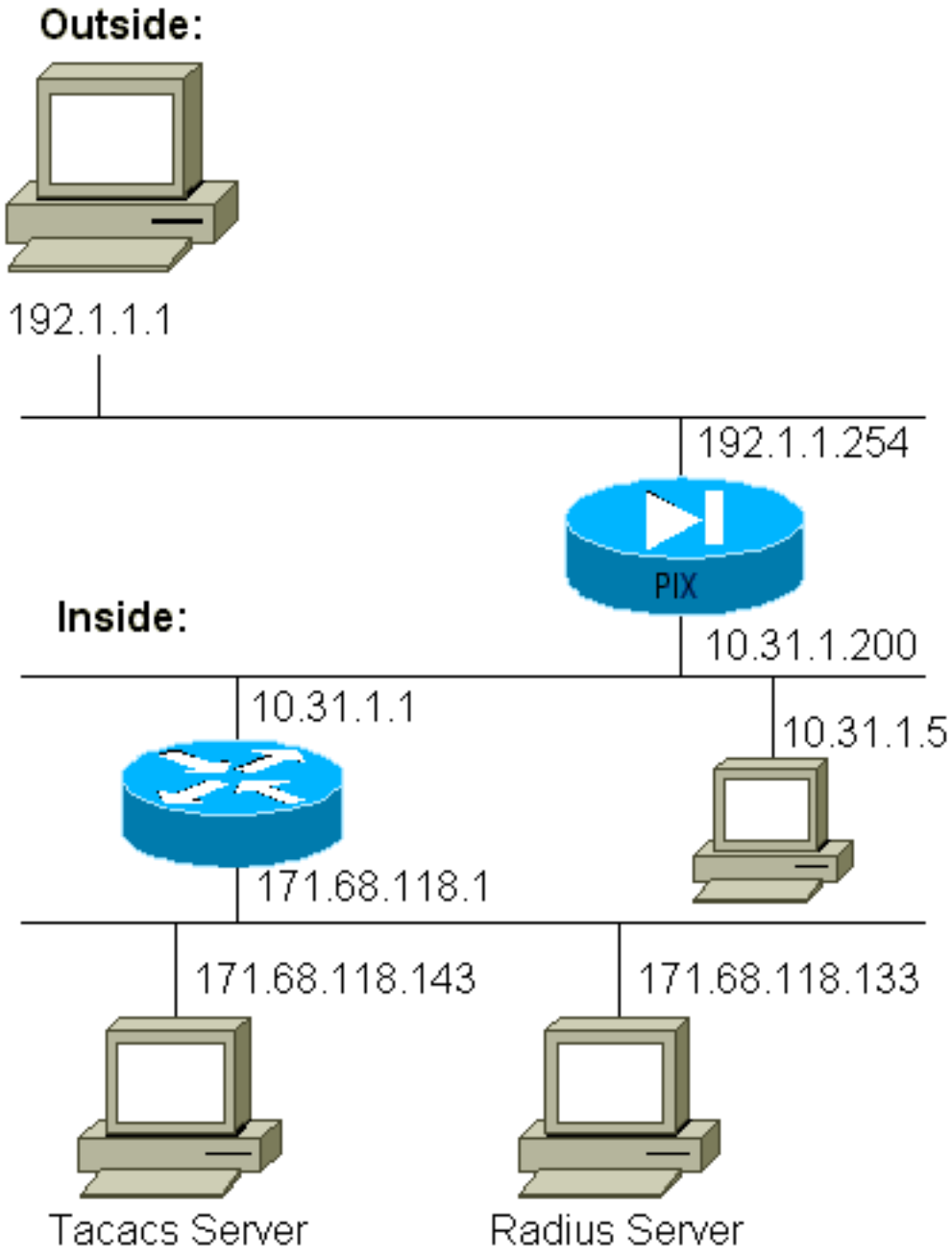
Aggiungere l'indirizzo IP e la chiave PIX al file client.

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

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 .*
}
}
```

Passaggi di debug

- Verificare che le configurazioni PIX funzionino prima di aggiungere il supporto AAA.Se non è possibile trasmettere il traffico prima di richiedere l'autenticazione e l'autorizzazione, non sarà possibile farlo in seguito.
- Abilita accesso a PIXIl comando di **debug della console di registrazione** *non deve* essere utilizzato in un sistema con carico elevato.Èpossibile utilizzare il comando **logging buffered debugging**. L'output del comando **show logging** o **logging** può essere inviato a un server syslog ed esaminato.
- Verificare che il debug sia attivo per i server TACACS+ o RADIUS. Tutti i server dispongono di questa opzione.

Esempio di rete



Configurazione PIX

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
```

```
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication 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
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

Esempi di debug di autenticazione da PIXAuthentication Esempi di debug da PIX

Negli esempi di debug seguenti:

In uscita

L'utente interno alla versione 10.31.1.5 avvia il traffico verso l'esterno della versione 192.1.1.1 ed è autenticato tramite TACACS+. Il traffico in uscita utilizza l'elenco di server "AuthOutbound" che include il server RADIUS 171.68.118.133.

In entrata

L'utente esterno alla versione 192.1.1.1 avvia il traffico verso l'interno della versione 10.31.1.5 (192.1.1.30) ed è autenticato tramite TACACS. Il traffico in entrata utilizza l'elenco di server "AuthInbound" che include il server TACACS (171.68.118.143).

Debug PIX - Buona autenticazione - TACACS+

Nell'esempio viene mostrato un debug PIX con una buona autenticazione:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

Debug PIX - Autenticazione non valida (nome utente o password) - TACACS+

Nell'esempio viene mostrato come eseguire il debug con PIX e un'autenticazione (nome utente o password) errata. L'utente vede quattro set di nome utente/password e il messaggio "`Error: numero massimo di tentativi superato`."

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

PIX debug - Can Ping Server, No Response - TACACS+

Nell'esempio viene mostrato come eseguire il debug PIX quando è possibile eseguire il ping del server, ma questo non sta parlando al PIX. Il nome utente viene visualizzato una sola volta, ma PIX non richiede mai una password (in Telnet). L'utente vede "`Errore: Numero massimo di tentativi superato`."

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
```

```
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

Debug PIX - Impossibile eseguire il ping del server - TACACS+

Nell'esempio viene mostrato un debug PIX in cui il server non è in grado di eseguire il ping. L'utente vede il nome utente una volta, ma il PIX non chiede mai una password (questa è in Telnet). Vengono visualizzati i seguenti messaggi: "`Timeout to TACACS+ server`" e "`Error: Numero massimo di tentativi superato`" (è stato effettuato lo swapping in un server falso nella configurazione).

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

Debug PIX - Buona autenticazione - RADIUS

Nell'esempio viene mostrato un debug PIX con una buona autenticazione:

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

Debug PIX - Autenticazione non valida (nome utente o password) - RADIUS

Nell'esempio viene mostrato un debug PIX con autenticazione (nome utente o password) errata. L'utente vede una richiesta di Nome utente e Password. L'utente ha tre possibilità per immettere correttamente il nome utente/password.

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
```

```
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Debug ping - Può eseguire il ping del server, Daemon inattivo - RADIUS

Nell'esempio viene mostrato un debug PIX in cui è possibile eseguire il ping del server, ma il daemon non è attivo e non comunica con il PIX. Vengono visualizzati il nome utente, la password e i messaggi "`Server RADIUS non riuscito`" e "`Errore: Numero massimo di tentativi superato.`"

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

Debug PIX - Impossibile eseguire il ping di una mancata corrispondenza tra il server o la chiave/il client - RADIUS

In questo esempio viene eseguito un debug PIX quando il server non è in grado di eseguire il ping o la chiave o il client non corrispondono. L'utente visualizza il nome utente, la password e i messaggi "`Timeout to RADIUS server`" e "`Error: Numero massimo di tentativi superato`" (un server falso è stato scambiato nella configurazione).

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

Aggiungi autorizzazione

Se si decide di aggiungere l'autorizzazione, sarà necessario richiedere l'autorizzazione per lo stesso intervallo di origine e di destinazione (poiché l'autorizzazione non è valida senza autenticazione):

```
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
```

Si noti che l'autorizzazione per "in uscita" non viene aggiunta perché il traffico in uscita è autenticato con RADIUS e l'autorizzazione RADIUS non è valida.

Esempi di debug di autenticazione e autorizzazione da PIX

Debug PIX - Buona autenticazione e corretta autorizzazione - TACACS+

Nell'esempio viene mostrato un debug PIX con una buona autenticazione e una corretta autorizzazione:

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

Debug PIX - Buona autenticazione, Autorizzazione non riuscita - TACACS+

Nell'esempio viene mostrato un debug PIX con una buona autenticazione ma con un'autorizzazione non riuscita. Qui l'utente vede anche il messaggio "`Errore: Autorizzazione negata.`"

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

Aggiungi accounting

TACACS+

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

Il debug ha lo stesso aspetto sia quando l'accounting è attivato che quando è disattivato. Tuttavia, al momento della "Creazione", viene inviato un record contabile di "inizio". Al momento del "Teardown", viene inviata una registrazione contabile "stop".

I record di accounting TACACS+ sono simili all'output seguente (vengono da Cisco Secure NT, da cui il formato delimitato da virgole):

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
```

```
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RAGGIO

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

L'aspetto del debug è lo stesso indipendentemente dal fatto che l'accounting sia attivato o disattivato. Tuttavia, al momento della "Creazione", viene inviato un record contabile di "inizio". Al momento del "Teardown", viene inviata una registrazione contabile "stop".

I record di accounting RADIUS hanno questo aspetto (provengono da Cisco Secure UNIX; quelle in Cisco Secure NT possono essere invece delimitate da virgole):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

Uso del comando Except

Nella nostra rete, se decidiamo che una particolare origine e/o destinazione non ha bisogno di autenticazione, autorizzazione o contabilità, possiamo fare qualcosa come questo output:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Se si sta "escludendo" una casella dall'autenticazione e si dispone dell'autorizzazione attivata, è inoltre necessario escludere la casella dall'autorizzazione.

Numero massimo sessioni e visualizzazione utenti connessi

Alcuni server TACACS+ e RADIUS dispongono delle funzionalità "max-session" o "view login users" (visualizza utenti connessi). La possibilità di eseguire il numero massimo di sessioni o di controllare gli utenti connessi dipende dai record di accounting. Quando viene generato un record "start" di accounting ma non un record "stop", il server TACACS+ o RADIUS presume che la persona sia ancora connessa (ha una sessione tramite PIX).

Questa procedura è indicata per le connessioni Telnet e FTP a causa della natura delle

connessioni. Questa operazione non è appropriata per HTTP a causa della natura della connessione. In questo output di esempio viene utilizzata una configurazione di rete diversa, ma i concetti sono gli stessi.

L'utente esegue una connessione Telnet attraverso il PIX, autenticandosi lungo il percorso:

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
    to 9.9.9.25 /23
(pix) 109011: Authen Session Start: user 'cse', Sid 3
(pix) 109005: Authentication succeeded for user 'cse'
    from 171.68.118.100/12 00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23
    gaddr 9.9.9.10/12 00 laddr 171.68.118.100/1200 (cse)
(server start account) Sun Nov 8 16:31:10 1998
    rtp-pinecone.rtp.cisco.com cse
 PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
    local_ip=171.68.118.100 cmd=telnet
```

Poiché il server ha rilevato un record "start" ma non un record "stop" (in questo momento), il server indica che l'utente "Telnet" ha eseguito l'accesso. Se l'utente tenta un'altra connessione che richiede l'autenticazione (ad esempio da un altro PC) e max-session è impostato su "1" sul server per questo utente (supponendo che il server supporti max-session), la connessione viene rifiutata dal server.

L'utente continua la propria attività in modalità Telnet o FTP sull'host di destinazione, quindi esce (trascorre 10 minuti in tale posizione):

```
(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
```

Indipendentemente dal fatto che il valore di auth sia 0 (autenticazione ogni volta) o maggiore (autenticazione una sola volta e non durante il periodo di autenticazione), viene tagliato un record di accounting per ogni sito a cui si accede.

Il protocollo HTTP funziona in modo diverso a causa della natura del protocollo. Questo output mostra un esempio di HTTP:

L'utente sfoglia da 171.68.118.100 a 9.9.9.25 attraverso il 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
```

L'utente legge la pagina Web scaricata.

Il record iniziale è stato inviato alle 16:35:34 e il record finale è stato inviato alle 16:35:35. Il download ha richiesto un secondo, ovvero tra il record iniziale e il record finale è stato interrotto meno di un secondo. L'utente è ancora connesso al sito Web e la connessione è ancora aperta durante la lettura della pagina Web? No. Il numero massimo di sessioni o la visualizzazione degli utenti connessi funzioneranno qui? No, perché il tempo di connessione (il tempo che intercorre tra "Built" e "Teardown") in HTTP è troppo breve. I record "start" e "stop" sono al secondo. Non ci sarà un record "start" senza un record "stop", dal momento che le registrazioni avvengono praticamente nello stesso istante. Verranno comunque inviati al server i record "start" e "stop" per ogni transazione, indipendentemente dal fatto che l'autenticazione sia impostata su 0 o su un valore superiore. Tuttavia, max-session e visualizza gli utenti connessi non funzionano a causa della natura delle connessioni HTTP.

Autenticazione e abilitazione sul PIX stesso

Nella discussione precedente è stata descritta l'autenticazione del traffico Telnet (e HTTP, FTP) *attraverso* il PIX. Ci assicuriamo che Telnet *to* the PIX funzioni *senza* autenticazione su:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Quando gli utenti si collegano in modalità Telnet al PIX, viene richiesta la password Telnet (**ww**). Quindi il PIX richiede anche il nome utente e la password TACACS+ (in questo caso, poiché si utilizza l'elenco dei server "AuthInbound") o RADIUS. Se il server non funziona, è possibile accedere al PIX immettendo **pix** per il nome utente e quindi la password di abilitazione (**abilita password *o altro***) per ottenere l'accesso.

Con questo comando:

```
aaa authentication enable console AuthInbound
```

all'utente vengono richiesti un nome utente e una password, da inviare al server TACACS (in questo caso, poiché viene utilizzato l'elenco dei server "AuthInbound", la richiesta viene inviata al server TACACS) o al server RADIUS. Poiché il pacchetto di autenticazione per enable è lo stesso del pacchetto di autenticazione per login, se l'utente può accedere al PIX con TACACS o RADIUS, può farlo tramite TACACS o RADIUS con lo stesso nome utente/password. Al problema è stato assegnato l'ID bug Cisco CSCdm47044 (solo utenti registrati).

Autenticazione sulla console seriale

Il comando **aaa authentication serial console AuthInbound** richiede la verifica dell'autenticazione per accedere alla console seriale del PIX.

Quando l'utente esegue i comandi di configurazione dalla console, i messaggi syslog vengono tagliati (presupponendo che il PIX sia configurato per inviare syslog a livello di debug a un host syslog). Questo è un esempio di quello che viene visualizzato sul server syslog:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

Modifica la richiesta visualizzata agli utenti

Se si dispone del comando **auth-prompt PIX_PIX_PIX**, gli utenti che attraversano il PIX vedranno la seguente sequenza:

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

All'arrivo alla casella di destinazione finale, viene visualizzato il prompt "Username:" (Nome utente:) e "Password:" (Password:). Questa richiesta ha effetto solo sugli utenti che *passano attraverso* il PIX, non *verso* il PIX.

Nota: non esistono record contabili tagliati per l'accesso al PIX.

Personalizza il messaggio visualizzato dagli utenti in caso di esito positivo o negativo

Se si dispone dei comandi:

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

gli utenti visualizzano questa sequenza in caso di accesso non riuscito/riuscito tramite PIX:

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

Timeout di inattività e assoluti per utente

I timeout di inattività e di autenticazione assoluta possono essere inviati dal server TACACS+ per ciascun utente. Se tutti gli utenti della rete devono avere lo stesso "timeout auth", non

implementare questa soluzione. Tuttavia, se sono necessarie diverse autenticazioni per utente, continuare a leggere.

nell'esempio, viene usato il comando **timeout auth 3:00:00**. Una volta autenticata, la persona non deve ripetere l'autenticazione per tre ore. Tuttavia, se si configura un utente con questo profilo e si dispone dell'*autorizzazione* TACACS AAA su nel PIX, i timeout di inattività e assoluti nel profilo utente sostituiscono l'autenticazione di timeout nel PIX per tale utente. Ciò non significa che la sessione Telnet tramite PIX venga disconnessa dopo il timeout di inattività/assoluto. Controlla semplicemente se viene eseguita la riautenticazione.

Questo profilo proviene dal freeware TACACS+:

```
user = timeout {
default service = permit
login = cleartext "timeout"
service = exec {
timeout = 2
idletime = 1
}
}
```

Dopo l'autenticazione, eseguire un comando **show auth** sul 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
```

Quando l'utente rimane inattivo per un minuto, il debug sul PIX visualizza:

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

L'utente deve eseguire nuovamente l'autenticazione quando torna allo stesso host di destinazione o a un host diverso.

HTTP virtuale

Se l'autenticazione è richiesta su siti esterni al PIX, così come sul PIX stesso, può essere osservato un comportamento insolito del browser, dal momento che i browser memorizzano il nome utente e la password.

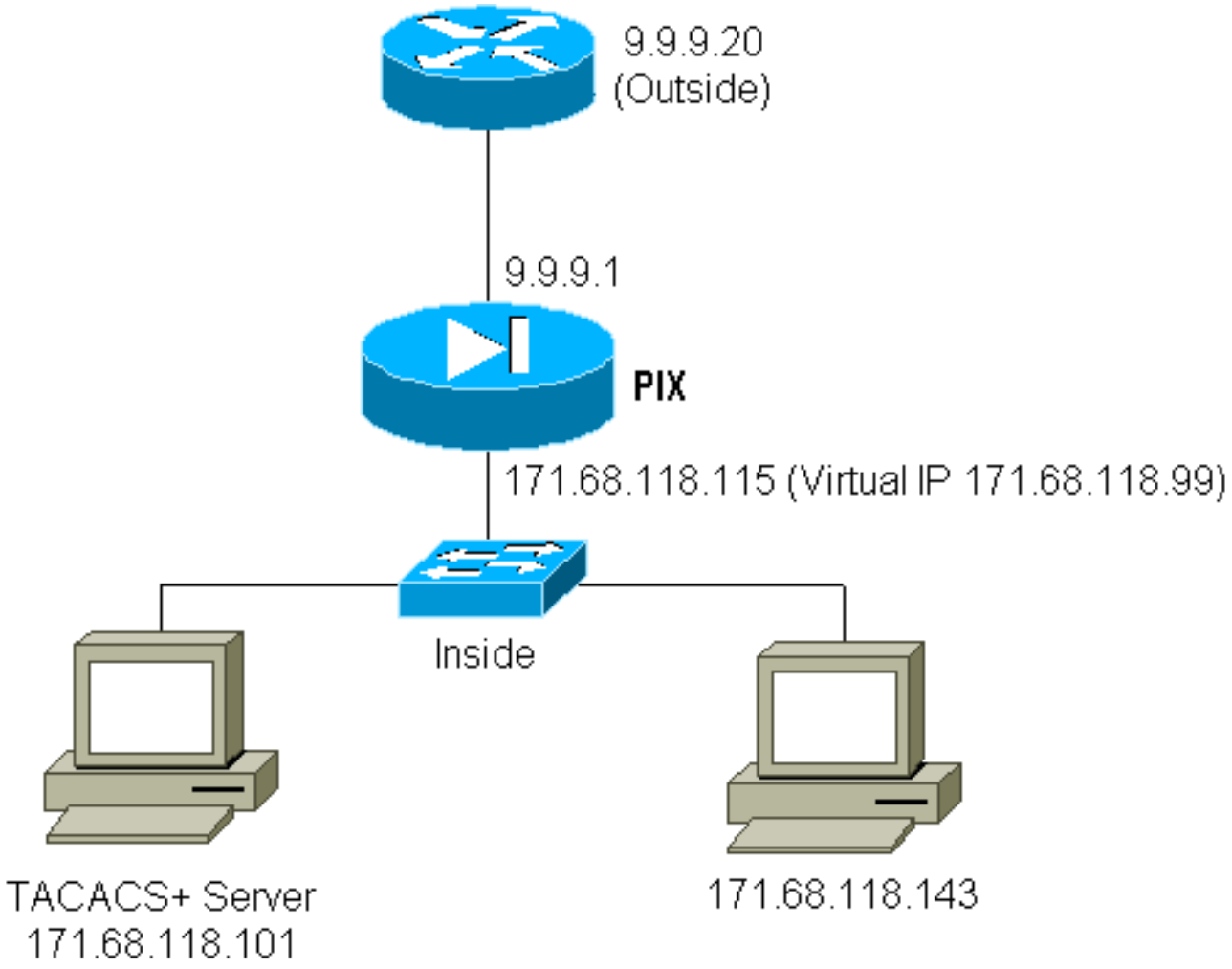
Per evitare ciò, è possibile implementare il protocollo HTTP virtuale aggiungendo un indirizzo RFC 1918 (un indirizzo non instradabile su Internet, ma valido e univoco per la rete PIX interna) alla configurazione PIX utilizzando questo comando:

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

Quando l'utente tenta di uscire dal PIX, è necessaria l'autenticazione. Se il parametro warn è presente, l'utente riceve un messaggio di reindirizzamento. L'autenticazione è valida per la durata

dell'autenticazione. Come indicato nella documentazione, non impostare la durata del comando **timeout auth** su 0 secondi con HTTP virtuale. Ciò impedisce le connessioni HTTP al server Web reale.

Diagramma HTTP virtuale in uscita



Configurazione PIX HTTP virtuale in uscita

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Telnet virtuale

Èpossibile configurare il PIX per autenticare tutto il traffico in entrata e in uscita, ma non è una buona idea farlo. Ciò è dovuto al fatto che alcuni protocolli, come "mail", non sono facilmente autenticati. Quando un server e un client di posta cercano di comunicare attraverso il PIX quando tutto il traffico attraverso il PIX viene autenticato, il syslog PIX per i protocolli non autenticabili

mostra messaggi come:

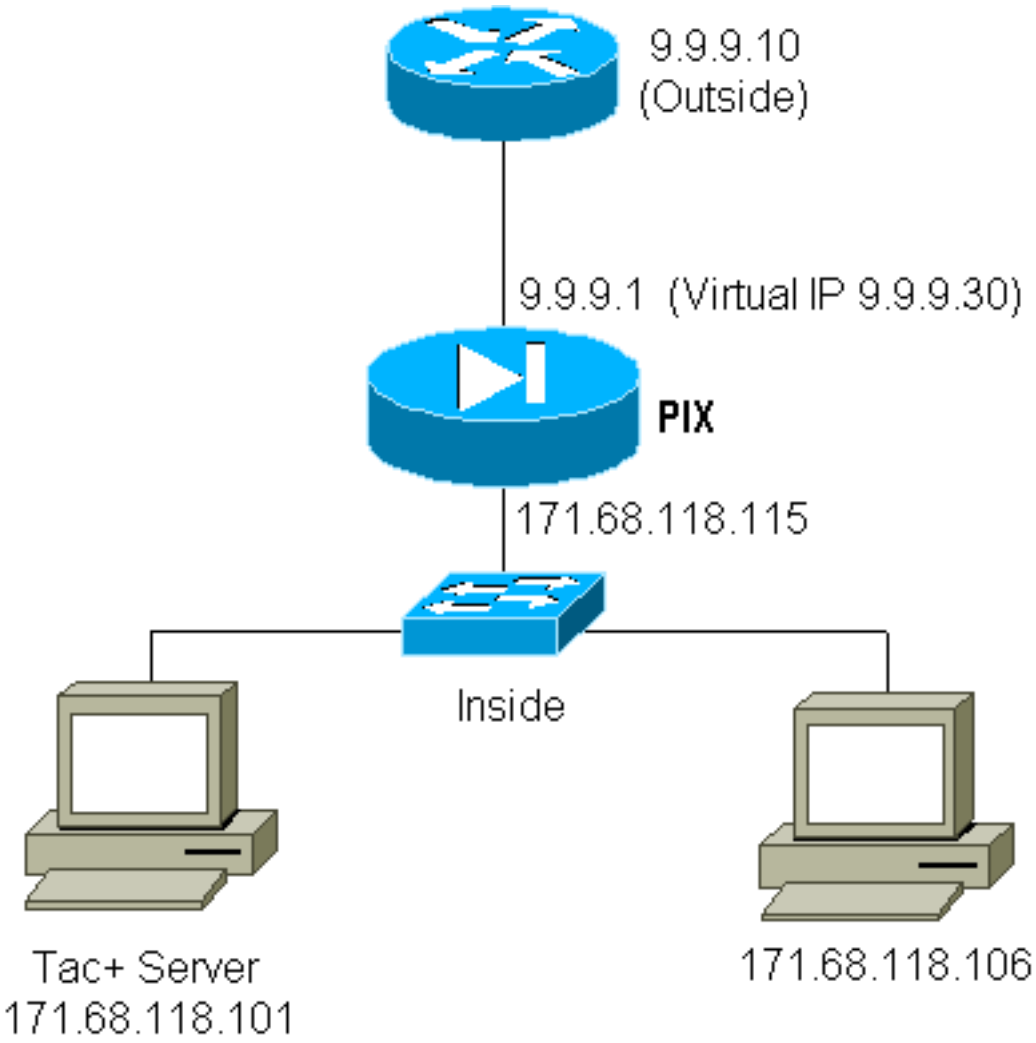
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

Poiché la posta elettronica e alcuni altri servizi non sono sufficientemente interattivi da consentire l'autenticazione, una soluzione consiste nell'utilizzare il comando **except** per l'autenticazione/autorizzazione (autenticare tutti gli elementi tranne origine/destinazione del server/client di posta).

Se è necessario autenticare un servizio insolito, è possibile utilizzare il comando **telnet virtuale**. Questo comando consente l'autenticazione dell'IP Telnet virtuale. Dopo questa autenticazione, il traffico per il servizio insolito può passare al server reale.

Nell'esempio, il traffico della porta TCP 49 deve passare dall'host esterno 9.9.9.10 all'host interno 171.68.118.106. Poiché questo traffico non è autenticabile, è stato configurato un Telnet virtuale. Per Telnet virtuale in ingresso, deve essere presente un oggetto static associato. In questo caso, sia la versione 9.9.20 che la versione 171.68.118.20 sono indirizzi virtuali.

Diagramma in entrata Telnet virtuale



Configurazione PIX Virtual Telnet in entrata

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

Configurazione utente server TACACS+ Telnet virtuale in entrata

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

Debug Virtual Telnet PIX in entrata

L'utente alla 9.9.9.10 deve prima eseguire l'autenticazione tramite Telnet all'indirizzo 9.9.9.20 sul PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

Una volta completata l'autenticazione, il comando **show auth** mostra che l'utente ha "l'ora sul misuratore":

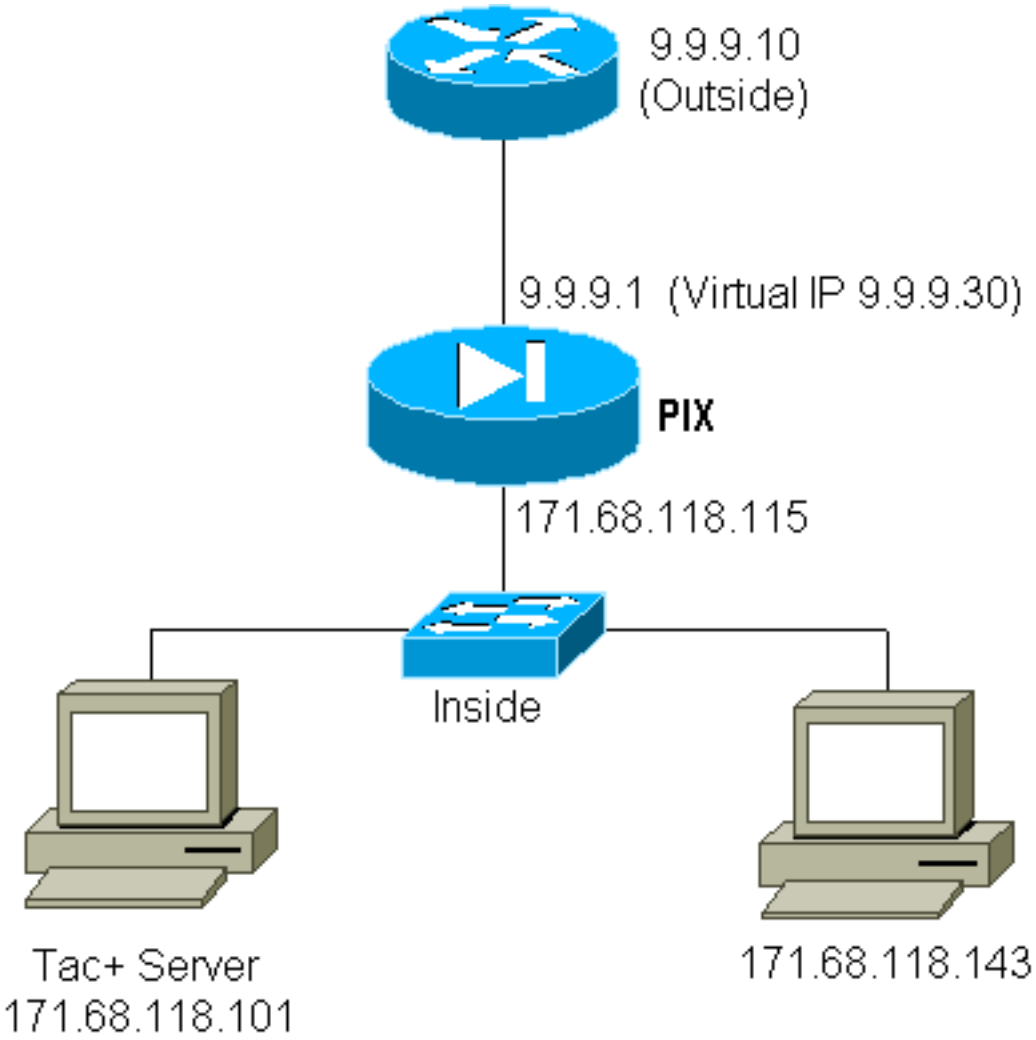
```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

In questo caso, il dispositivo alla versione 9.9.9.10 desidera inviare il traffico TCP/49 al dispositivo alla versione 171.68.118.106:

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Virtual Telnet in uscita

Poiché il traffico in uscita è consentito per impostazione predefinita, non è richiesto alcun traffico statico per l'utilizzo di Telnet virtuale in uscita. Nell'esempio, l'utente interno alla porta 171.68.118.143 Telnet viene impostato sulla porta virtuale 9.9.9.30 e autenticato. La connessione Telnet viene interrotta immediatamente. Una volta autenticato, il traffico TCP viene autorizzato da 171.68.118.143 verso il server a 9.9.9.10:



Configurazione PIX Virtual Telnet in uscita

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

Debug Virtual Telnet PIX in uscita

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
```

```
109011: Authen Session Start: user 'timeout_143', Sid 25
109005: Authentication succeeded for user 'timeout_143' from
   171.68.118.143/1536 to 9. 9.9.30/23
302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
   9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
   9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
   9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
   bytes 625 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
   9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
   bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

Disconnessione Telnet Virtuale

Quando l'utente si connette in modalità Telnet all'indirizzo IP Telnet virtuale, il comando **show auth** visualizza l'autenticazione.

Se si desidera impedire il passaggio del traffico al termine della sessione (quando il tempo rimanente nell'autenticazione è sufficiente), è necessario che l'utente esegua nuovamente la connessione Telnet all'indirizzo IP Telnet virtuale. La sessione viene disattivata.

Port Authorization

Èpossibile richiedere l'autorizzazione per un intervallo di porte. In questo esempio, l'autenticazione era ancora necessaria per tutte le connessioni in uscita, ma per le porte TCP 23-49 era richiesta solo l'autorizzazione.

Configurazione PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

Quando la connessione Telnet è stata effettuata tra le 17.68.118.143 e le 9.9.9.10, l'autenticazione e l'autorizzazione si sono verificate perché la porta Telnet 23 è compresa nell'intervallo 23-49.

Quando si esegue una sessione HTTP da 171.68.118.143 a 9.9.9.10, è comunque necessario eseguire l'autenticazione, ma il PIX non chiede al server TACACS+ di autorizzare il protocollo HTTP perché 80 non è compreso nell'intervallo 23-49.

Configurazione server Freeware TACACS+

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
```

```
        }
        }
```

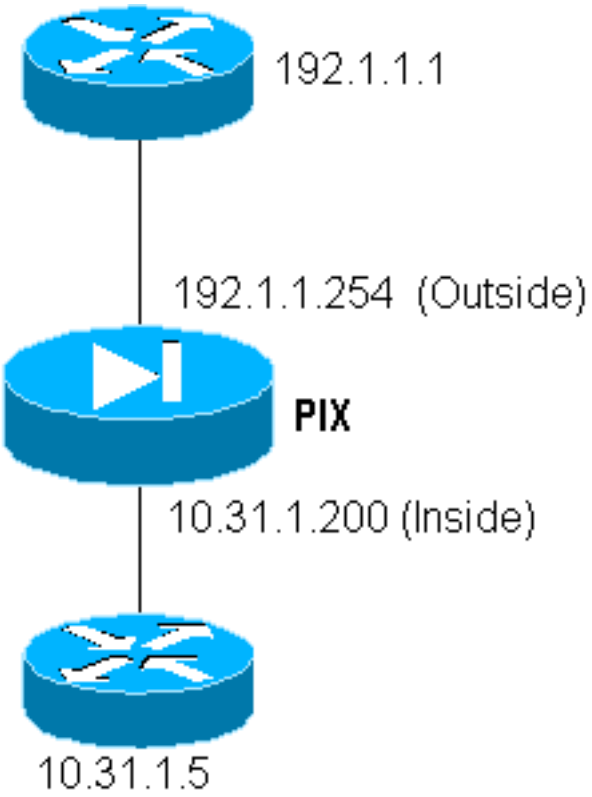
Il PIX invia "`cmd=tcp/23-49`" e "`cmd-arg=9.9.9.10`" al server TACACS+.

Debug del PIX

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109007: Authorization permitted for user 'telnetrange'
    from 171.68.118.143/1051 to 9.9 .9.10/23
 302001: Built TCP connection 0 for faddr 9.9.9.10/23
    gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
 109001: Auth start for user '???' from 171.68.118.143/1105
    to 9.9.9.10/80
 109001: Auth start for user '???' from 171.68.118.143/1110
    to 9.9.9.10/80
 109011: Authen Session Start: user 'telnetrange', Sid 1
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1110 to 9. 9.9.10/80
 302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
  laddr 171.68.1 18.143/1110 (telnetrange)
 302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
  laddr 171.68.1 18.143/1111 (telnetrange)
 302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
  laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
  laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

AAA Accounting per il traffico diverso da HTTP, FTP e Telnet

Il software PIX versione 5.0 modifica la funzionalità di contabilità del traffico. Una volta completata l'autenticazione, è possibile tagliare i record di accounting per il traffico diverso da HTTP, FTP e Telnet.



Per copiare un file dal router esterno (192.1.1.1) al router interno (10.31.1.5) tramite il protocollo TFTP, aggiungere la funzionalità Virtual Telnet per aprire un foro per il processo TFTP:

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Quindi, Telnet dal router esterno a 192.1.1.1 all'IP virtuale 192.1.1.30 e autenticazione all'indirizzo virtuale che consente a UDP di attraversare il PIX. Nell'esempio, il processo di **copia tftp flash** è stato avviato dall'esterno all'interno:

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Per ogni **copia tftp flash** sul PIX (ce ne sono state tre durante questa copia IOS), viene tagliato un record di accounting e inviato al server di autenticazione. Di seguito è riportato un esempio di record TACACS su Cisco Secure Windows):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

Informazioni correlate

- Informazioni di riferimento sui comandi PIX
- Pagina di supporto dei prodotti PIX