Configurazioni di esempio PIX, TACACS+ e RADIUS: 4.4.x

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.

èsupportata l'autorizzazione TACACS+; L'autorizzazione RADIUS non è valida. Le modifiche di autenticazione, autorizzazione e accounting (AAA) di PIX 4.4.1 rispetto alla versione precedente includono: Gruppi di server AAA e failover, autenticazione per l'abilitazione e l'accesso alla console seriale e accettazione e rifiuto dei messaggi di richiesta.

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.
- Autenticazione valida senza autorizzazione.
- Autorizzazione non valida senza autenticazione.

Si supponga di avere 100 utenti e che si desideri che solo 6 di questi utenti siano in grado di eseguire operazioni FTP, Telnet o HTTP all'esterno della rete. Si consiglia al PIX di autenticare il traffico in uscita e fornire a tutti e 6 gli utenti gli ID sul server di sicurezza TACACS+/RADIUS. Con l'autenticazione semplice, questi 6 utenti possono essere autenticati con nome utente e password, quindi uscire. Gli altri 94 utenti non sono usciti. Il PIX richiede all'utente un nome utente/password, quindi passa il nome utente e la password al server di sicurezza TACACS+/RADIUS e, a seconda della risposta, apre o nega la connessione. Questi 6 utenti possono utilizzare FTP, Telnet o HTTP.

Ma supponiamo che uno di questi tre utenti, "Terry", non sia affidabile. Si desidera consentire a Terry di eseguire FTP, ma non HTTP o Telnet verso l'esterno. Ciò significa dover aggiungere l'autorizzazione, ossia autorizzare ciò che gli utenti possono fare oltre ad autenticare chi sono. Quando si aggiunge l'autorizzazione al PIX, il PIX invia 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 stato configurato correttamente, Terry può utilizzare "FTP 1.2.3.4" ma non può utilizzare HTTP o Telnet.

Caratteristiche visualizzate dall'utente con Autenticazione/Autorizzazione attivata

Quando si cerca di 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 - Nel browser viene visualizzata una finestra 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 CiscoSecure UNIX TACACS

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 CiscoSecure UNIX RADIUS

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

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

Cisco Secure NT 2.x RADIUS

Attenersi alla seguente procedura.

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 il comando **Add/Edit** new 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 e/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 della 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** per ogni comando che si desidera consentire (ad esempio, Telnet).
4. Se si desidera consentire Telnet a siti specifici, immettere gli indirizzi IP consentiti 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 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.

Configurazione server RADIUS Livingston

Aggiungere l'indirizzo 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
```

Configurazione server Freeware TACACS+

```
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 {
```

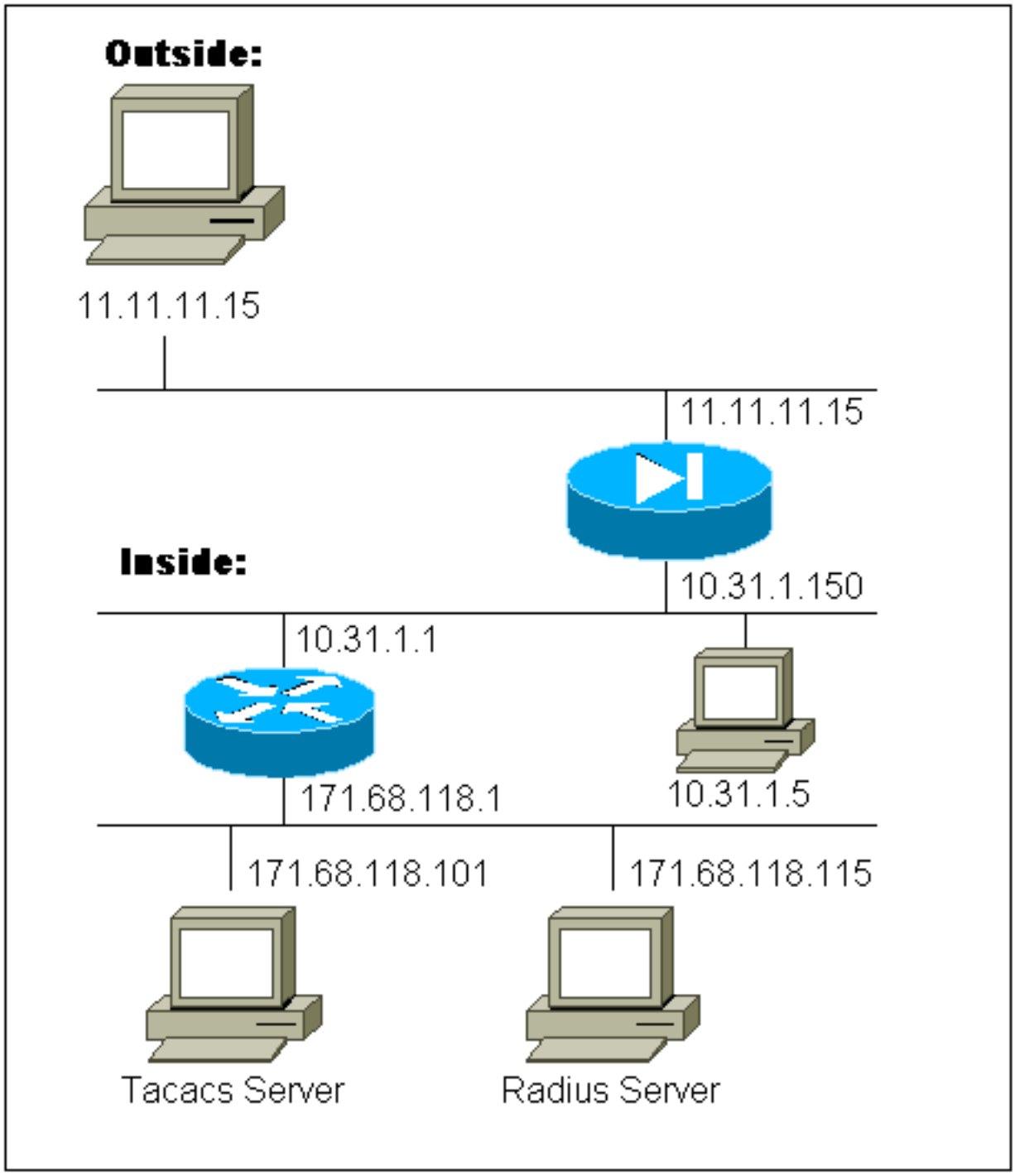
```
permit .*
}
}

user = can_only_do_ftp {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}
```

Passaggi di debug

- Verificare che le configurazioni PIX funzionino correttamente prima di aggiungere autenticazione, autorizzazione e accounting (AAA).Se non è possibile trasmettere il traffico prima di richiedere l'autenticazione e l'autorizzazione, non sarà possibile farlo in seguito.
- Abilitare la registrazione in PIX:Il 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
 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
```

Esempi di debug di autenticazione 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 11.11.15 e viene autenticato tramite TACACS+ (il traffico in uscita usa l'elenco di server "In uscita" che include il server TACACS 171.68.118.101).

In entrata

L'utente esterno alla versione 11.11.11.15 avvia il traffico verso l'interno della versione 10.31.1.5 (11.11.12) e viene autenticato tramite RADIUS (il traffico in entrata utilizza l'elenco dei server "In entrata" che include il server RADIUS 171.68.118.115).

Debug PIX - Buona autenticazione - TACACS+

L'esempio seguente mostra il debug PIX con una buona autenticazione:

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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

Nell'esempio seguente viene mostrato il debug PIX con autenticazione non valida (nome utente o password). L'utente vede quattro set di nome utente/password. Viene visualizzato il seguente messaggio: "Errore: numero massimo di tentativi superato".

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX debug - Can Ping, ma nessuna risposta - TACACS+

Nell'esempio seguente viene illustrato il debug PIX per un server che non sta parlando al PIX. Il nome utente viene visualizzato una volta e PIX non richiede mai una password (in Telnet).

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

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

L'esempio seguente mostra il debug PIX per un server su cui non è possibile eseguire il ping. Il nome utente viene visualizzato una volta. PIX non richiede mai una password (in Telnet). Viene visualizzato il seguente messaggio: "Timeout to TACACS+ server" e "Error: "Numero massimo di tentativi superato" (la configurazione in questo esempio riflette un server fittizio).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

Debug PIX - Buona autenticazione - RADIUS

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

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

Nell'esempio seguente viene mostrato il debug PIX con autenticazione non valida (nome utente o password). L'utente vede una richiesta di Nome utente e Password. In caso di errore, viene visualizzato quattro volte il messaggio "Password errata". L'utente viene quindi disconnesso. Al problema è stato assegnato l'ID bug #CSCdm46934.

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

Debug PIX - Deamon inattivo, non comunica con PIX - RADIUS

Nell'esempio seguente viene illustrato il debug PIX con un server di cui è possibile eseguire il ping, ma il daemon non è attivo. Il server non comunica con PIX. L'utente visualizza il nome utente, seguito dalla password. Vengono visualizzati i seguenti messaggi: "Server RADIUS non

riuscito" e "Errore: Numero massimo di tentativi superato".

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

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

L'esempio seguente mostra il debug PIX per un server su cui non è possibile eseguire il ping o in cui la chiave o il client non corrispondono. L'utente visualizza Nome utente e Password. Vengono visualizzati i seguenti messaggi: "Timeout sul server RADIUS" e "Errore: "Numero massimo di tentativi superato" (il server nella configurazione è solo a scopo esemplificativo).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

Aggiunta dell'autorizzazione

Poiché l'autorizzazione non è valida senza autenticazione, sarà necessaria l'autorizzazione per lo stesso intervallo di origine e di destinazione:

```
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
```

In uscita

L'autorizzazione per "traffico in ingresso" non viene aggiunta perché il traffico in ingresso è autenticato con RADIUS e l'autorizzazione RADIUS non è valida

Esempi di debug di autenticazione e autorizzazione da PIX

Debug dei PIX con una buona autenticazione e una corretta autorizzazione - TACACS+

Nell'esempio seguente viene mostrato il debug PIX con una buona autenticazione e un'autorizzazione riuscita:

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

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

Nell'esempio seguente viene illustrato il 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 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Aggiunta di accounting

TACACS+

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

Il debug ha lo stesso aspetto indipendentemente dal fatto che l'accounting sia attivato o disattivato. Tuttavia, al momento della "Costruzione", sarà inviato un record contabile di "inizio". Al momento del "Teardown", verrà inviato un documento contabile di "stop".

I record di accounting TACACS+ hanno il seguente aspetto (sono di Cisco Secure UNIX; quelle in CiscoSecure NT possono essere invece delimitate da virgole):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RAGGIO

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

Il debug ha lo stesso aspetto 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 di "stop":

I record di accounting RADIUS hanno il seguente aspetto: (questi sono forniti da Cisco Secure UNIX; quelle in CiscoSecure NT possono essere invece delimitate da virgole):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

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 segue:

```
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 si "escludono" gli indirizzi IP dall'autenticazione e si dispone dell'autorizzazione attivata, è necessario escluderli anche 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 (ossia, che abbia 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. Nell'esempio seguente viene utilizzata una configurazione di rete diversa ma i

concetti sono identici.

L'utente si connette via 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 verrà rifiutata dal server.

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

```
(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.

Tuttavia, il protocollo HTTP funziona in modo diverso a causa della natura del protocollo. Di seguito è riportato 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 pubblicato alle 16:35:34 e il record finale è stato pubblicato alle 16:35:35. Questo download ha richiesto un secondo (ovvero meno di un secondo tra il record iniziale e quello finale). 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 funzioneranno a causa della natura delle connessioni HTTP.

Autenticazione e abilitazione sul PIX stesso

La discussione precedente riguardava l'autenticazione del traffico Telnet (e HTTP, FTP) attraverso il PIX. Nell'esempio seguente, viene verificato che Telnet to the pix funzioni senza autenticazione su:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Quindi, si aggiunge il comando per autenticare gli utenti Telnetting al PIX:

```
aaa authentication telnet console Outgoing
```

Quando gli utenti si collegano in modalità Telnet al PIX, viene richiesta la password Telnet ("ww"). In questo caso, il PIX richiede anche il nome utente e la password TACACS+ (poiché viene utilizzato l'elenco dei server "in uscita") o RADIUS.

```
aaa authentication enable console Outgoing
```

Con questo comando viene richiesto all'utente di immettere un nome utente e una password da inviare al server TACACS o RADIUS. In questo caso, poiché si utilizza l'elenco dei server "In uscita", la richiesta viene inviata al server TACACS. Poiché il pacchetto di autenticazione per enable è lo stesso del pacchetto di autenticazione per l'accesso, l'utente può usare TACACS o RADIUS con lo stesso nome utente/password, a condizione che possa accedere al PIX con TACACS o RADIUS. Al problema è stato assegnato l'ID bug #CSCdm47044.

Nel caso in cui il server non sia attivo, l'utente può accedere alla modalità di abilitazione PIX immettendo "PIX" come nome utente e la normale password di abilitazione da PIX ("enable password any"). Se l'opzione "enable password what" non è presente nella configurazione PIX, l'utente deve immettere "PIX" come nome utente e premere il tasto Invio. Se la password di abilitazione è impostata ma non è nota, sarà necessario un disco di recupero password per reimpostare.

Autenticazione sulla console seriale

Il comando **aaa authentication serial console** 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 (se il PIX è configurato per inviare syslog a livello di debug a un host syslog). Di seguito è riportato un esempio dal server syslog:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

Modifica del prompt degli utenti Vedere

Se si dispone del comando:

```
auth-prompt THIS_IS_PIX_5
```

gli utenti che passano attraverso il PIX vedono la sequenza:

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

e all'arrivo alla casella di destinazione finale, viene visualizzata la casella di richiesta "Nome utente:" e "Password:".

Questo prompt ha effetto solo sugli utenti che passano attraverso il PIX e non al PIX.

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

Personalizzazione del messaggio visualizzato dagli utenti in caso di esito positivo o negativo

Se disponiamo dei comandi:

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

In caso di accesso non riuscito/riuscito tramite PIX, gli utenti vedranno quanto segue:

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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. Ma se avete bisogno di diverse autenticazioni per utente, continuate a leggere.

Nell'esempio relativo al PIX, viene utilizzato il comando **timeout auth 3:00:00**. Ciò significa che una volta autenticata, la persona non dovrà ripetere l'autenticazione per 3 ore. Tuttavia, se si configura un utente con il seguente profilo e si dispone dell'autorizzazione TACACS AAA su PIX, i timeout di inattività e assoluti nel profilo utente sostituiscono l'autorizzazione 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.

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

Dopo l'autenticazione, usare il comando **show auth** sul file 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 dovrà ripetere l'autenticazione quando ritorna 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.

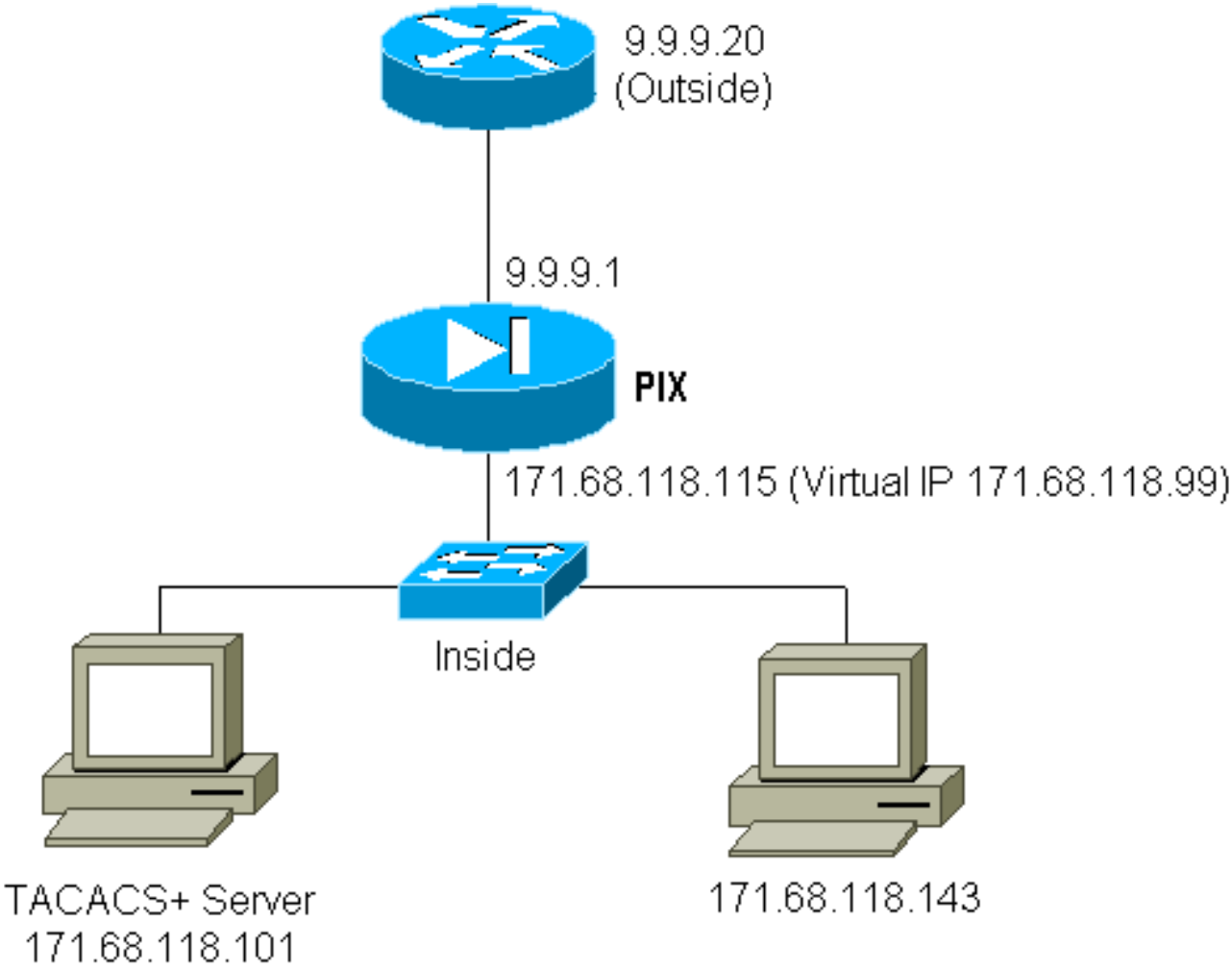
Per evitare ciò, è possibile implementare il protocollo HTTP virtuale aggiungendo un indirizzo RFC 1918 (ovvero un indirizzo non instradabile su Internet, ma valido e univoco per il PIX all'interno della rete) alla configurazione PIX utilizzando il comando seguente:

```
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; in questo modo si evitano le connessioni HTTP al web server reale.

Esempio di 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

Telnet virtuale

Configurare il PIX per autenticare tutto il traffico in entrata e in uscita non è una buona idea perché 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 mostrerà messaggi come:

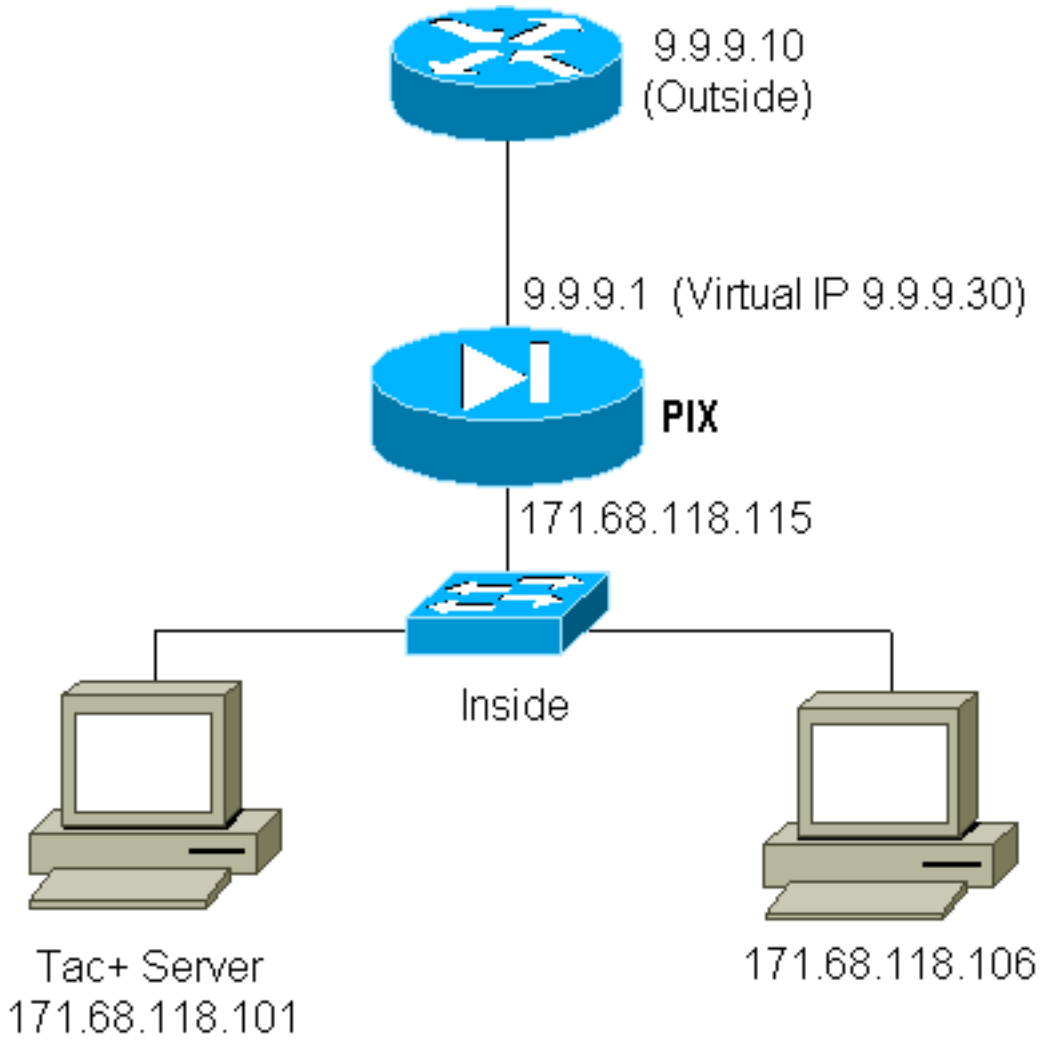
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

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).

Tuttavia, se è necessario autenticare un servizio insolito, è possibile usare il comando **telnet virtuale**. Questo comando consente l'autenticazione dell'IP Telnet virtuale. Dopo questa autenticazione, il traffico per il servizio insolito può andare al server reale che è collegato all'IP virtuale.

Nell'esempio, si desidera consentire il flusso del traffico della porta TCP 49 dall'host esterno 9.9.9.10 all'host interno 171.68.118.106. Poiché questo traffico non è autenticabile, è stata configurata la modalità Telnet virtuale.

Telnet virtuale in ingresso:



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) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
```

```
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

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 ingresso:

L'utente alla 9.9.9.10 deve prima eseguire l'autenticazione tramite telnet all'indirizzo 9.9.9.30 sul PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

Una volta completata l'autenticazione, il comando **show auth** visualizza l'ora sullo strumento:

```
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 il dispositivo alla 9.9.9.10 desidera inviare il traffico TCP/49 al dispositivo alla 171.68.118.106:

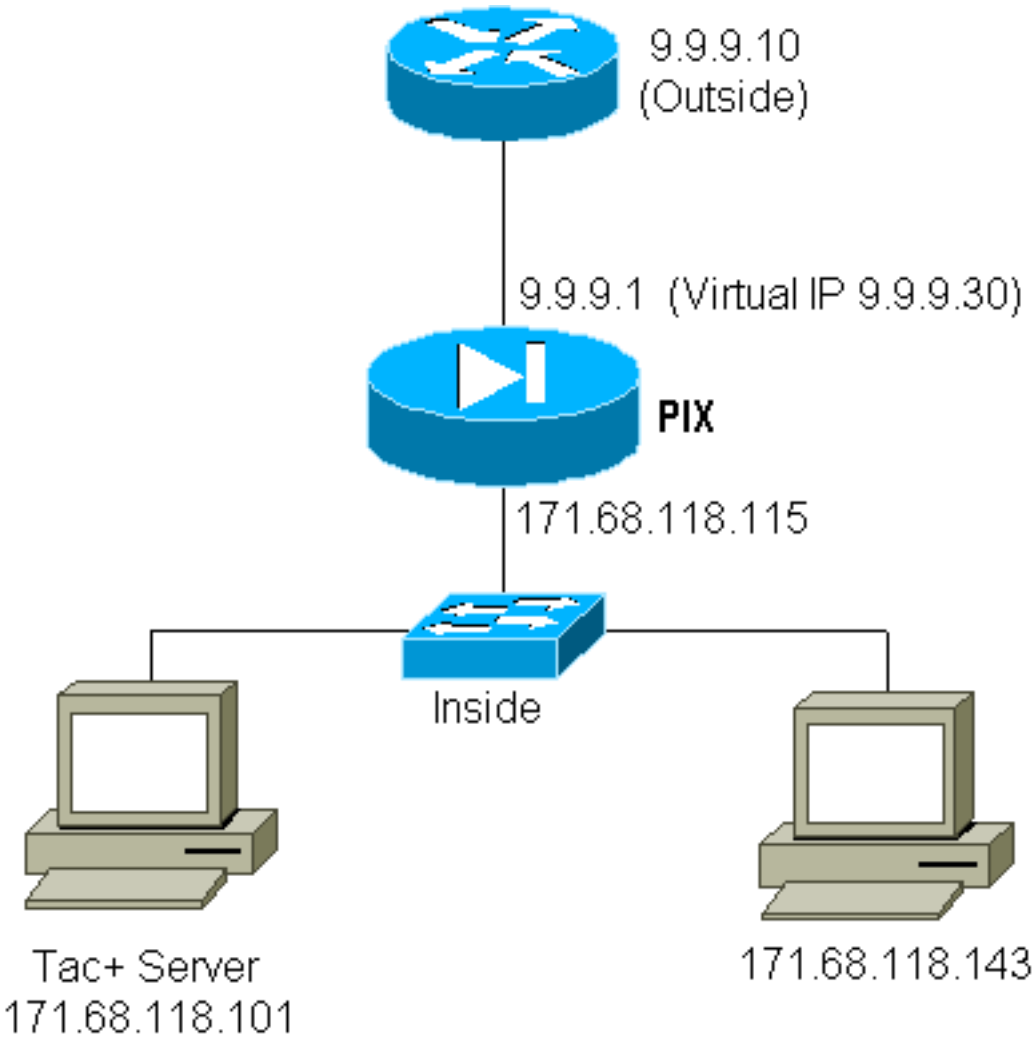
```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 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)
```

Telnet virtuale 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 seguente, l'utente interno alla posizione 171.68.118.143 passerà alla modalità Telnet 9.9.9.30 virtuale e verrà 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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 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 collega in modalità Telnet all'indirizzo IP Telnet virtuale, il comando **show auth** restituisce il valore di autenticazione. Se l'utente desidera impedire il passaggio del traffico al termine della sessione (quando il tempo è rimasto nell'autenticazione), deve connettersi di nuovo all'indirizzo IP Telnet virtuale. La sessione viene disattivata.

Port Authorization

Èpossibile richiedere l'autorizzazione per un intervallo di porte. Nell'esempio seguente, l'autenticazione era ancora richiesta per tutte le porte in uscita, ma l'autorizzazione è richiesta solo per le porte TCP 23-49.

Configurazione 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
```

Quando si usa Telnet da 171.68.118.143 a 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 ancora necessario eseguire l'autenticazione, ma il PIX non chiede al server TACACS+ di autorizzare il protocollo HTTP perché il protocollo 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
        }
        }
```

Notare che il PIX sta inviando "cmd=tcp/23-49" e "cmd-arg=9.9.9.10" al server TACACS+.

Debug sul 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)
```

Informazioni correlate

- Supporto dei prodotti software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall