Configurazione di PIX 5.1.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 meno comuni. è supportata l'autorizzazione TACACS+; L'autorizzazione RADIUS non è valida. Le modifiche di autenticazione, autorizzazione e accounting (AAA) PIX 5.1 rispetto alla versione precedente includono l'autenticazione estesa (xauth), ovvero l'autenticazione dei tunnel IPSec dal client Cisco Secure VPN 1.1.

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.

Premesse

Autenticazione e autorizzazione

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

Si supponga di avere un centinaio di utenti interni e che si desideri che solo sei 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 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 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 sei utenti potevano utilizzare FTP, Telnet o HTTP.

Ma supponiamo che *uno* di questi sei utenti, "Festo", non sia da fidarsi. Si desidera consentire a Festus 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. Questa condizione è valida solo con TACACS+. Quando aggiungiamo l'*autorizzazione* al PIX, il PIX invia prima il nome utente e la password di Festus al server di sicurezza, quindi invia una richiesta di autorizzazione per comunicare al server di sicurezza il "*comando*" che Festus sta cercando di fare. Con il server configurato correttamente, Festus potrebbe essere autorizzato a "ftp 1.2.3.4", ma sarebbe negata la possibilità di HTTP o Telnet ovunque.

Caratteristiche visualizzate dall'utente con Autenticazione/Autorizzazione attivata

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

- **Telnet**: viene visualizzato un prompt con il nome utente e 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** per il nome utente e **local_password@remote_password** per la password. Il PIX invia il nome_utente e la password_locale al server di sicurezza locale e, se l'autenticazione (e l'autorizzazione) hanno esito positivo sul PIX/server, il nome_utente_remoto e la password_remota vengono passati al server FTP di destinazione oltre.
- **HTTP** - Nel browser viene visualizzata una finestra che richiede un nome utente e una 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 stia per scadere una connessione HTTP, ma non lo sta facendo, è probabile che la riautenticazione sia in corso effettivamente 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 mostrato 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.
- **Tunnel**: quando si tenta di eseguire il tunnel del traffico IPSec nella rete con il client VPN e xauth attivato, viene visualizzata una casella grigia per "Autenticazione utente per nuova connessione" per nome utente/password.**Nota:** questa autenticazione è supportata a partire da Cisco Secure VPN Client 1.1. Se il menu **Guida > Informazioni** non visualizza la versione 2.1.x o successive, non funziona.

Configurazioni del server di sicurezza utilizzate per tutti gli scenari

Configurazione server TACACS Cisco Secure UNIX

In questa sezione vengono presentate le informazioni necessarie per configurare il server di sicurezza.

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 la GUI per aggiungere l'indirizzo 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 ACS per Windows 2.x RADIUS

Utilizzare questa procedura per configurare Cisco Secure ACS per Windows 2.x RADIUS.

1. Ottenere una password nella sezione User Setup GUI.
2. Dalla sezione GUI di Group Setup, impostare l'attributo 6 (Service-Type) su **Login** o **Administrative**.
3. Aggiungere l'indirizzo IP PIX nell'interfaccia utente della sezione 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 è consentita la connessione in modalità Telnet a siti specifici, immettere gli indirizzi IP nella sezione degli argomenti nel formato "allow #.#.#.#". In caso contrario, per consentire il collegamento in modalità Telnet, 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, nella parte inferiore della configurazione del gruppo fare clic su **Deny unmatched IOS commands**.
3. Selezionare **Aggiungi/Modifica nuovo comando** per ogni comando che si desidera consentire (ad esempio, **Telnet**).
4. Per consentire la connessione Telnet a siti specifici, immettere l'indirizzo IP nella sezione degli argomenti nel formato "allow #.#.#.#". Per consentire la connessione Telnet a qualsiasi sito, 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. Accertarsi che l'indirizzo IP PIX sia stato aggiunto nella sezione NAS Configuration GUI.

Configurazione server RADIUS Livingston

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

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

Configurazione server RADIUS di tipo Merit

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

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

Configurazione server Freeware TACACS+

```
key = "cisco"
user = adminuser {
login = cleartext "all"
```

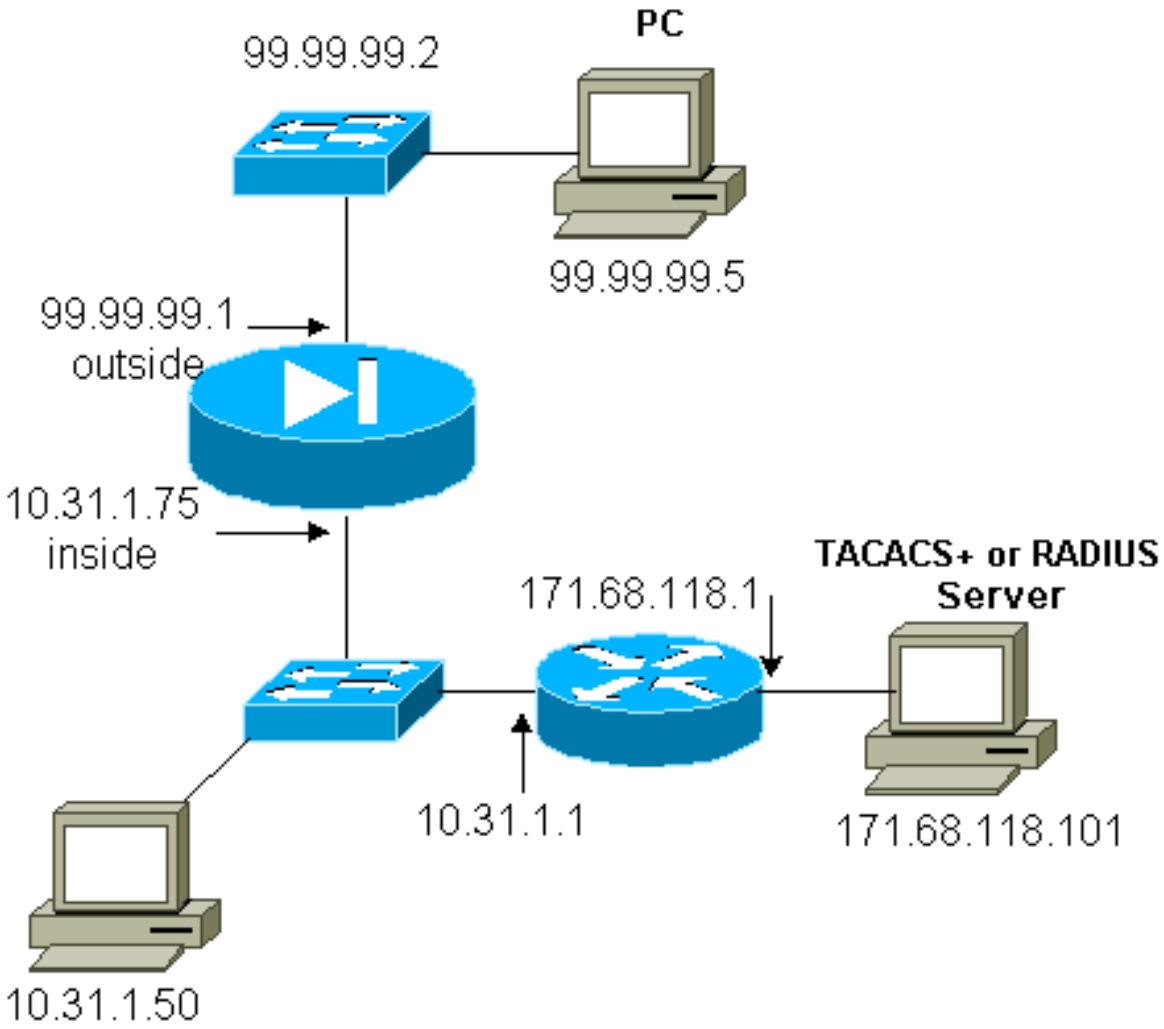
```
default service = permit
}

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

Nota: alcuni comandi **show** sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- Verificare che la configurazione PIX funzioni prima di aggiungere il server AAA. Se non è possibile passare il traffico prima di istituire l'autenticazione e l'autorizzazione, non sarà possibile farlo in seguito.
- Abilitare la registrazione in PIX.Il debug della console di registrazione non deve essere utilizzato in un sistema con carico elevato.Èpossibile utilizzare la registrazione del debug memorizzato nel buffer, quindi eseguire il comando **show logging**.La registrazione può anche essere inviata a un server syslog ed esaminata in tale server.
- Attiva il debug sui server TACACS+ o RADIUS (tutti i server dispongono di questa opzione).

Esempio di rete



Configurazione 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]
```

Esempi di debug di autenticazione da PIX

In questa sezione vengono illustrati esempi di debug di autenticazione per vari scenari.

In entrata

L'utente esterno alla porta 99.99.99.2 avvia il traffico verso l'interno della porta 10.31.1.50 (99.99.99.99) e viene autenticato tramite TACACS (ossia, il traffico in entrata usa l'elenco di server "AuthInbound" che include il server TACACS 171.68.118.101).

Debug PIX - Buona autenticazione - TACACS+

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

```
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.)
```

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

Nell'esempio seguente viene mostrato un debug PIX con autenticazione non valida (nome utente o password). Vengono visualizzati tre set di nome utente/password, seguiti dal seguente messaggio: `Errore: numero massimo di tentativi superato.`

```
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
```

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

Nell'esempio seguente viene illustrato un debug PIX in cui è possibile eseguire il ping del server ma non parlare al PIX. Il nome utente viene visualizzato una volta, ma il PIX non richiede mai una password (in modalità Telnet). Viene visualizzato il messaggio di `errore: Numero massimo di tentativi superato.`

```
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
```

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

L'esempio seguente mostra un debug PIX in cui il server non è in grado di eseguire il ping. Il nome

utente viene visualizzato una volta, ma il PIX non richiede mai una password (in modalità Telnet). Vengono visualizzati i seguenti messaggi: `Timeout sul server TACACS+` ed `errore: Numero massimo di tentativi superato` (un server fittizio è stato scambiato nella configurazione).

```
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
```

Debug PIX - Buona autenticazione - RADIUS

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

```
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)
```

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

Nell'esempio seguente viene mostrato un debug PIX con autenticazione non valida (nome utente o password). L'utente vede la richiesta di nome utente e password e ha tre opportunità per immetterli. Se la voce non riesce, viene visualizzato il seguente messaggio: `Errore: numero massimo di tentativi superato`.

```
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
```

Debug PIX - Can Ping Server, Daemon Down - RADIUS

Nell'esempio seguente viene illustrato 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, il messaggio di `errore del server RADIUS` e il messaggio di `errore: Numero massimo di tentativi superato`. x

```
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
```

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

Nell'esempio seguente viene mostrato un debug PIX in cui il server non è in grado di eseguire il ping o in cui il client/la chiave non corrispondono. L'utente visualizza un nome utente, una password, il messaggio di `timeout sul server RADIUS` e il messaggio di `errore: Numero massimo di tentativi superato il` messaggio (un server falso è stato scambiato nella configurazione).

```
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
```

Aggiunta dell'autorizzazione

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

```
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 il traffico 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+

L'esempio seguente mostra un debug PIX con una buona autenticazione e un'autorizzazione riuscita:

```
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)
```

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

Nell'esempio seguente viene mostrato il debug PIX con una buona autenticazione ma un'autorizzazione non riuscita. Viene visualizzato anche il messaggio `Errore: Autorizzazione negata`.

```
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
```

Aggiunta di accounting

TACACS+

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

Output freeware TACACS+:

```
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
```

RAGGIO

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

Output Merit RADIUS:

```
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 del comando Exclude

Se alla rete viene aggiunto un altro host esterno (versione 99.99.99.100) e questo host è attendibile, è possibile escluderlo dall'autenticazione e dall'autorizzazione con i seguenti comandi:

```
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
```

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 l'utente 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 esegue una connessione Telnet attraverso il PIX, autenticandosi durante il percorso:

```
 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 di avvio ma non un record di arresto, 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 esegue la propria attività Telnet o FTP sull'host di destinazione, quindi si chiude (trascorre dieci 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
```

Se il valore di auth è 0, ovvero viene autenticato ogni volta, o più, ovvero viene autenticato una volta e non una seconda volta durante il periodo di autenticazione, verrà 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. 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 viene inviato alle 16:35:34 e il record finale alle 16:35:35. Questo download ha richiesto un secondo, ovvero tra il record iniziale e il record finale è trascorso meno di un secondo. L'utente ha ancora eseguito l'accesso 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. La registrazione di start e stop è al di sotto del secondo.

Non esiste un record iniziale senza un record finale, poiché i record vengono registrati praticamente nello stesso istante. Verranno comunque inviati record di avvio e di arresto al server 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 riguarda l'autenticazione del traffico Telnet (e HTTP, FTP) attraverso il PIX. Verificare che Telnet su PIX funzioni senza autenticazione su:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Quindi aggiungere il comando per autenticare gli utenti Telnetting al PIX:

```
aaa authentication telnet console AuthInbound
```

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

Se il server non è attivo, è possibile accedere al PIX immettendo **pix** per il nome utente e quindi la password enable (**abilita password *o altro***). Con il comando:

```
aaa authentication enable console AuthInbound
```

All'utente vengono richiesti un nome utente e una password da inviare al server TACACS o RADIUS. In questo caso, poiché viene utilizzato l'elenco di server AuthInbound, il PIX richiede il nome utente e la password TACACS+.

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).

Se il server non è attivo, è possibile accedere alla modalità di abilitazione PIX immettendo **pix** per il nome utente e la password di abilitazione normale da PIX (**abilitare password *o altro***). Se si **abilita la password** a *prescindere da quale* sia la configurazione PIX, immettere **pix** come nome utente e premere **Invio**. Se la password di abilitazione è impostata ma non è nota, è necessario creare un disco di recupero password per reimpostare la password.

Modifica del prompt degli utenti Vedere

Se si dispone del comando:

```
auth-prompt PIX_PIX_PIX
```

gli utenti che passano attraverso il PIX vedono 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 destinazione finale, gli utenti vedranno il nome utente: e Password: visualizzato dalla casella di destinazione. Questo prompt ha effetto solo sugli utenti che *attraversano* il PIX e non sul 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 si dispone dei comandi:

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

quindi gli utenti visualizzano la seguente sequenza su un 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

Questa funzione non è al momento disponibile e al problema è stato assegnato l'ID bug Cisco CSCdp93492 (solo utenti registrati).

HTTP virtuale

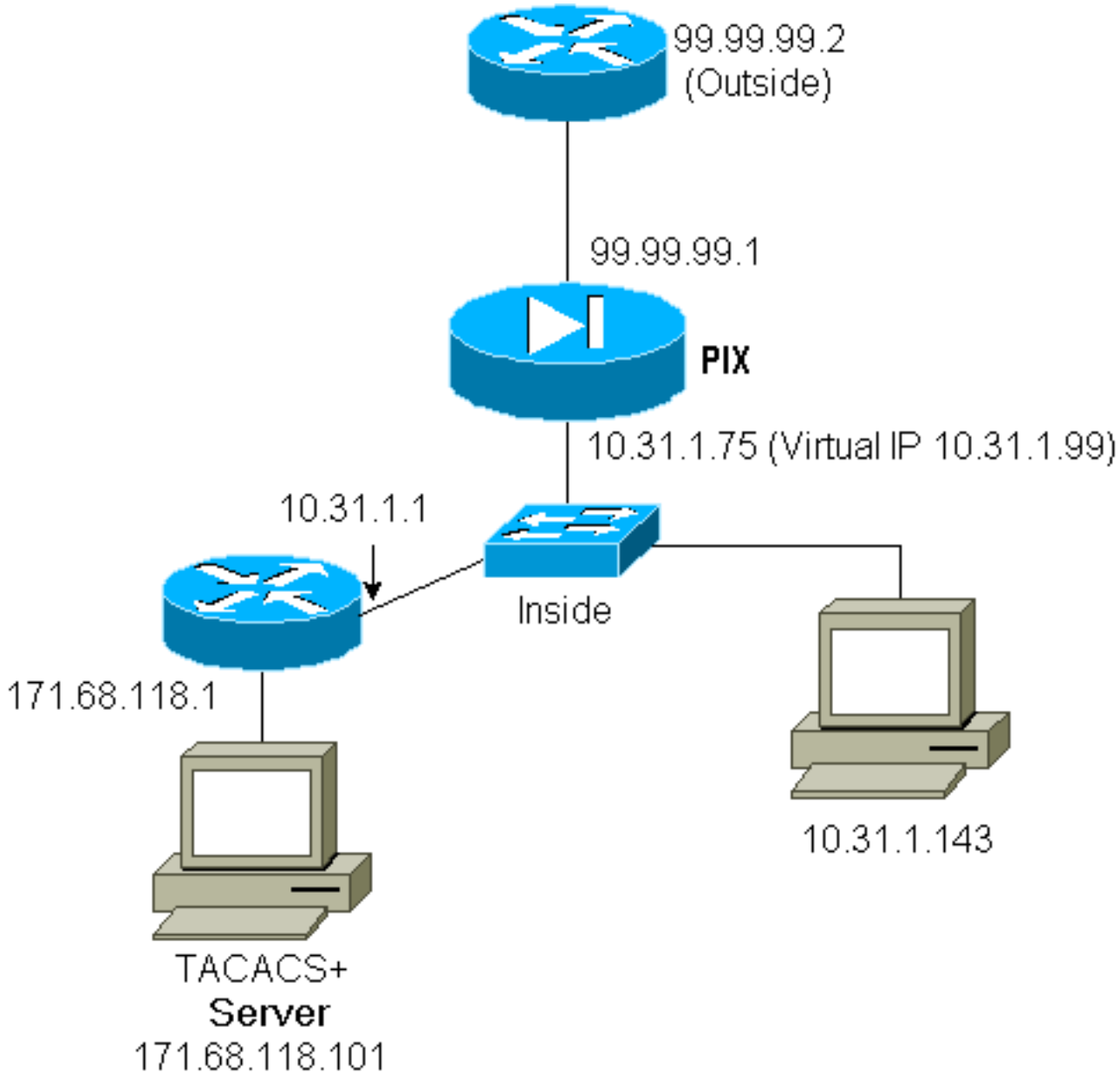
Se l'autenticazione è richiesta su siti esterni al PIX e sul PIX stesso, può essere osservato un comportamento insolito del browser, dal momento che i browser memorizzano il nome utente e la password.

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 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 virtuale

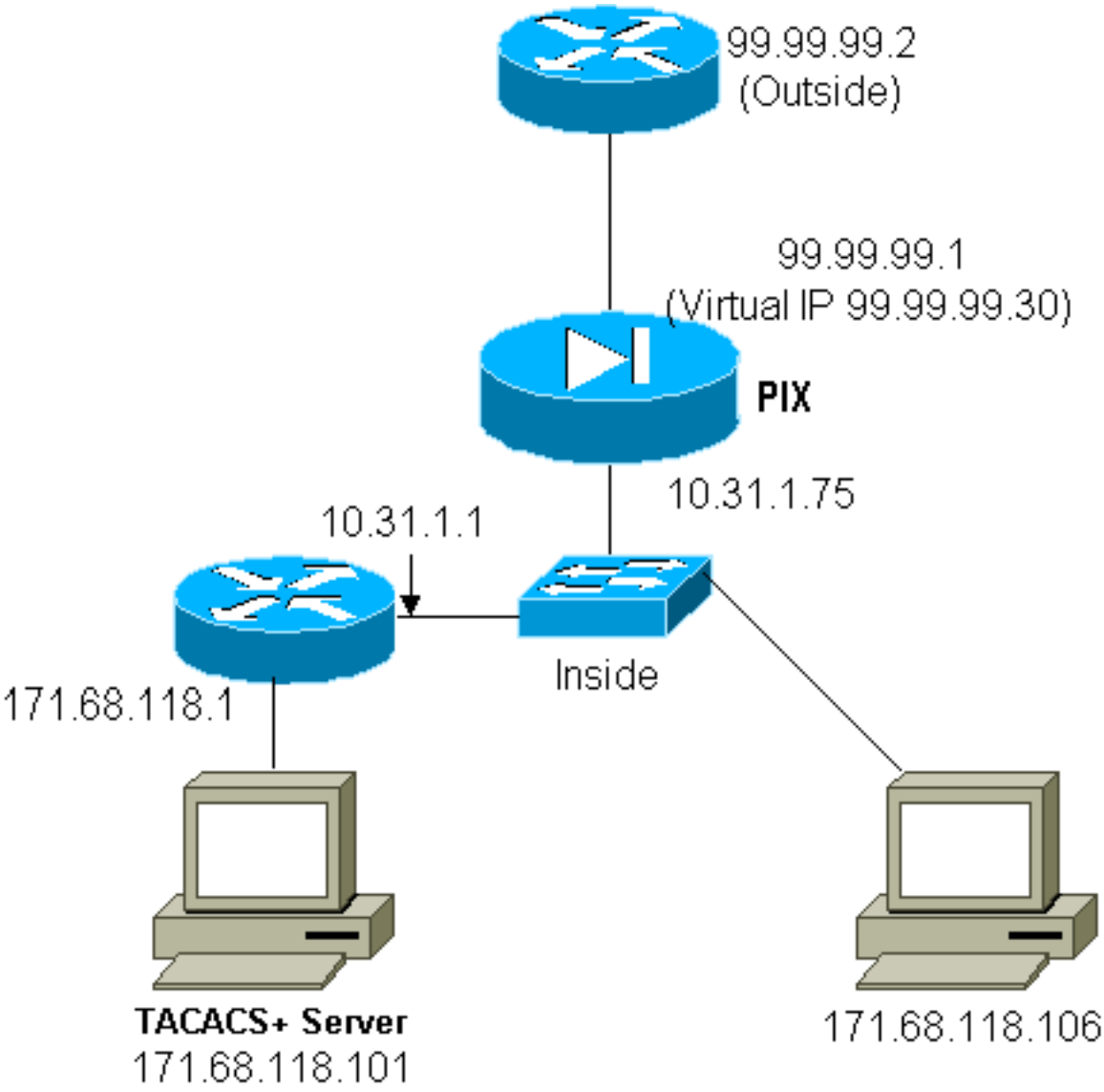
Èpossibile configurare il PIX per autenticare tutti i protocolli in entrata e in uscita, ma non è una buona idea perché alcuni protocolli, come la posta, non sono facilmente autenticati. Quando un server e un client di posta cercano di comunicare attraverso il PIX quando tutto il traffico attraverso il PIX viene autenticato, PIX syslog per i protocolli non autenticabili mostra messaggi come:

```
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)
```

Tuttavia, se è veramente necessario autenticare un servizio insolito, è possibile utilizzare il comando **telnet virtuale**. Questo comando consente l'autenticazione dell'indirizzo 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 99.99.99.2 all'host interno 171.68.118.106. Poiché questo traffico non è autenticabile, configurare una rete Telnet virtuale. Per Telnet virtuale, deve essere presente un oggetto static associato. In questo caso, sia 99.99.99.20 che 171.68.118.20 sono indirizzi virtuali.

Virtual Telnet in entrata



Configurazione PIX Virtual Telnet in entrata

```
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
```

Debug Virtual Telnet PIX in entrata

L'utente che si trova a 99.99.99.2 deve prima autenticarsi tramite Telnet all'indirizzo 99.99.99.20 sul 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
```

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

```
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 il dispositivo alla posizione 99.99.99.2 desidera inviare il traffico TCP/49 al dispositivo alla posizione 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)
```

Èpossibile aggiungere l'autorizzazione:

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

in modo che quando si tenta di effettuare il traffico TCP/49 attraverso il PIX, quest'ultimo invii anche la query di autorizzazione al server:

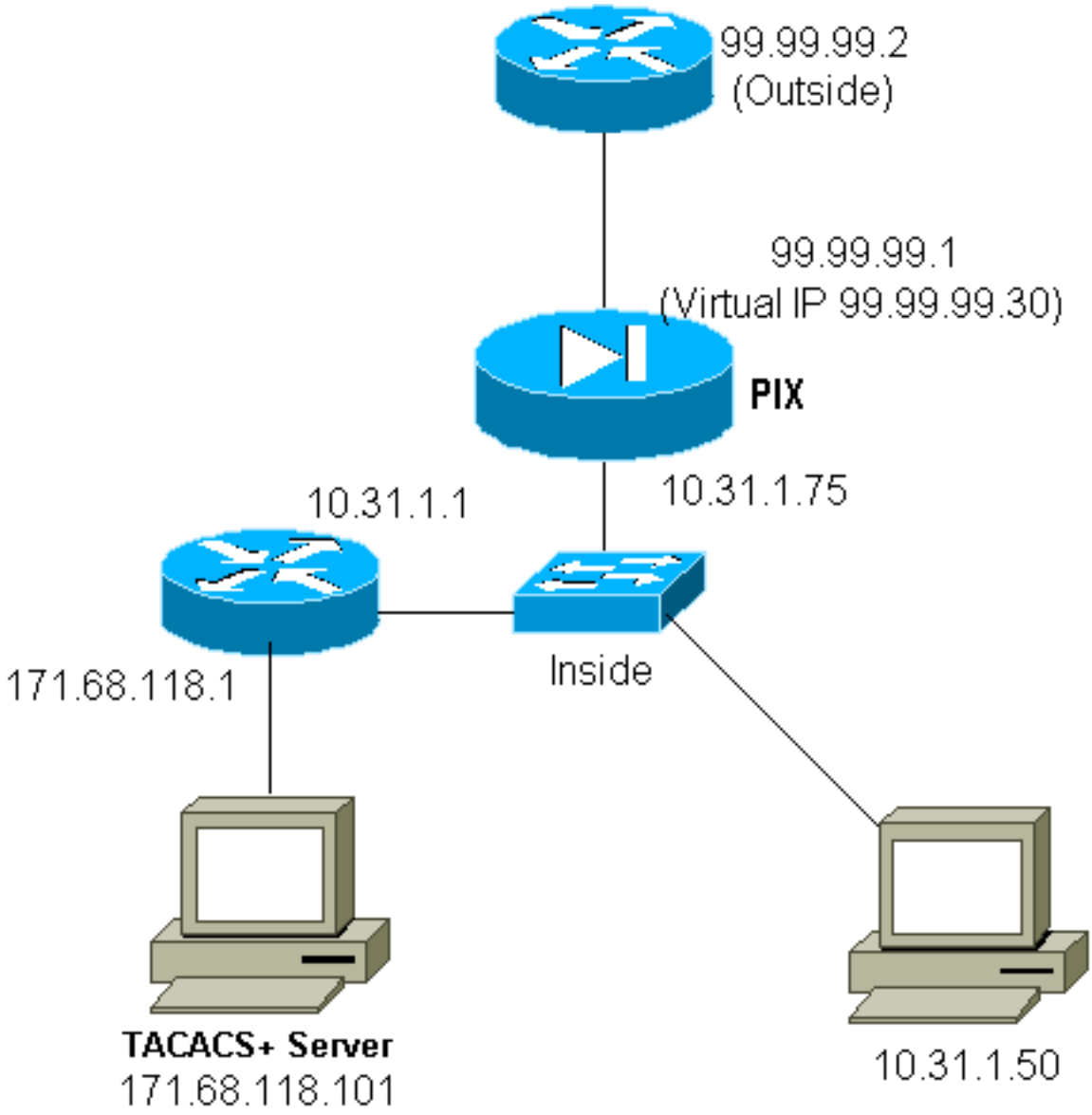
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

Sul server TACACS+, viene visualizzato quanto segue:

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

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 seguente, l'utente interno alla porta 10.31.1.50 Telnet viene impostato sulla porta virtuale 99.99.99.30 e autentica: la connessione Telnet viene interrotta immediatamente. Una volta autenticato, il traffico TCP viene autorizzato dalla versione 10.31.1.50 al server alla versione 99.99.99.2:



Configurazione PIX Virtual Telnet in uscita:

```
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: non esiste alcuna autorizzazione poiché si tratta di RADIUS.

Debug Virtual Telnet PIX in uscita:

```
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)
```

Disconnessione Telnet Virtuale

Quando gli utenti si collegano in modalità Telnet all'indirizzo IP Telnet virtuale, il comando **show auth** restituisce il loro valore di autenticazione. Se si desidera impedire il passaggio del traffico al termine delle sessioni, quando il tempo rimanente nell'autenticazione è sufficiente, è necessario eseguire nuovamente la connessione Telnet all'indirizzo IP Telnet virtuale. La sessione viene disattivata.

Dopo la prima autenticazione:

```
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
```

Dopo la seconda autenticazione (ovvero, il foro viene chiuso):

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

Port Authorization

L'autorizzazione è consentita per gli intervalli di porte (come TCP/30-100). Se sul PIX è configurata la modalità Telnet virtuale e l'autorizzazione per un intervallo di porte, quando il foro viene aperto con la modalità Telnet virtuale, il PIX invia un comando **tcp/30-100** al server TACACS+ per ottenere l'autorizzazione:

```
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
```

Configurazione server Freeware TACACS+:

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

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

Dopo aver verificato il funzionamento di Virtual Telnet per consentire il traffico TCP/49 all'host all'interno della rete, abbiamo deciso che volevamo tenere conto di questo, quindi abbiamo aggiunto:

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

Di conseguenza, viene tagliato un record contabile quando il traffico tcp/49 viene attraversato (questo esempio viene dal 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
```

Autenticazione Estesa (Xauth)

Esempi di configurazione

- Chiusura dei tunnel IPSec su più interfacce Cisco Secure PIX Firewall con Xauth
- IPSec tra Cisco Secure PIX Firewall e un client VPN con autenticazione estesa

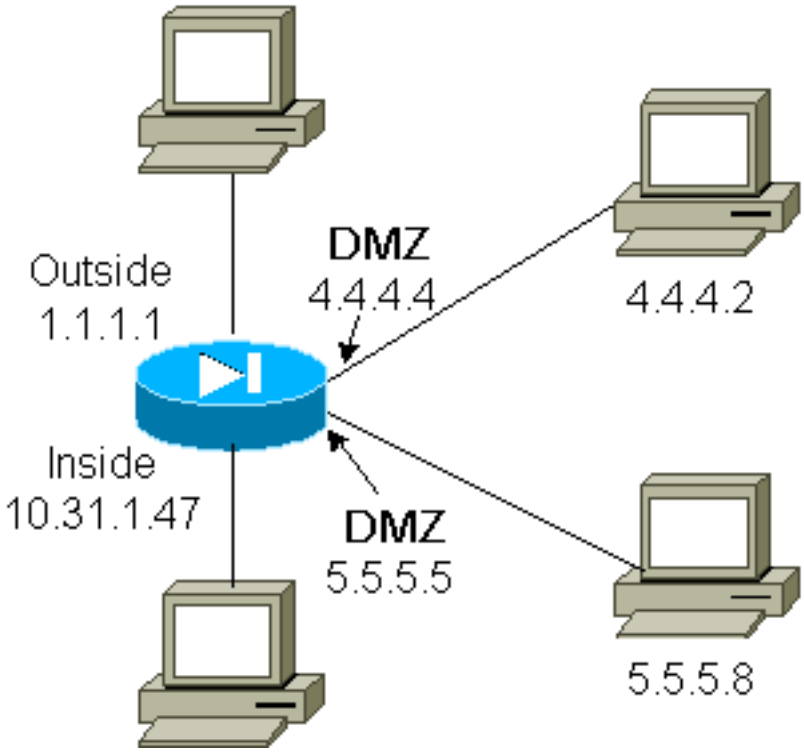
Autenticazione sulla DMZ

Per autenticare gli utenti che passano da un'interfaccia DMZ a un'altra, indicare al PIX di autenticare il traffico per le interfacce denominate. Sulla nostra PIX la disposizione è:

```
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

Esempio di rete



Configurazione PIX

Si desidera autenticare il traffico Telnet tra 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
```

Accounting Xauth

Se il comando **sysopt connection allow-ipsec** e non il comando **sysopt ipsec pl-compatible** sono

configurati in PIX con xauth, l'accounting è valido per le connessioni TCP, ma non per ICMP o UDP.

Informazioni correlate

- Pagina di supporto dei prodotti PIX
- Informazioni di riferimento sui comandi PIX
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Pagina di supporto per Cisco Secure UNIX
- Pagina di supporto di Cisco Secure ACS per Windows
- Supporto tecnico – Cisco Systems