Configurazioni di esempio PIX, TACACS+ e RADIUS: 4.2.x

Sommario

Introduzione

L'autenticazione RADIUS e TACACS+ può essere eseguita per le connessioni FTP, Telnet e HTTP. è supportata l'autorizzazione TACACS+; L'autorizzazione RADIUS non è valida.

La sintassi per l'autenticazione è stata leggermente modificata in PIX software 4.2.2. Nel presente

documento viene utilizzata la sintassi per le versioni software 4.2.2.

Prerequisiti

Requisiti

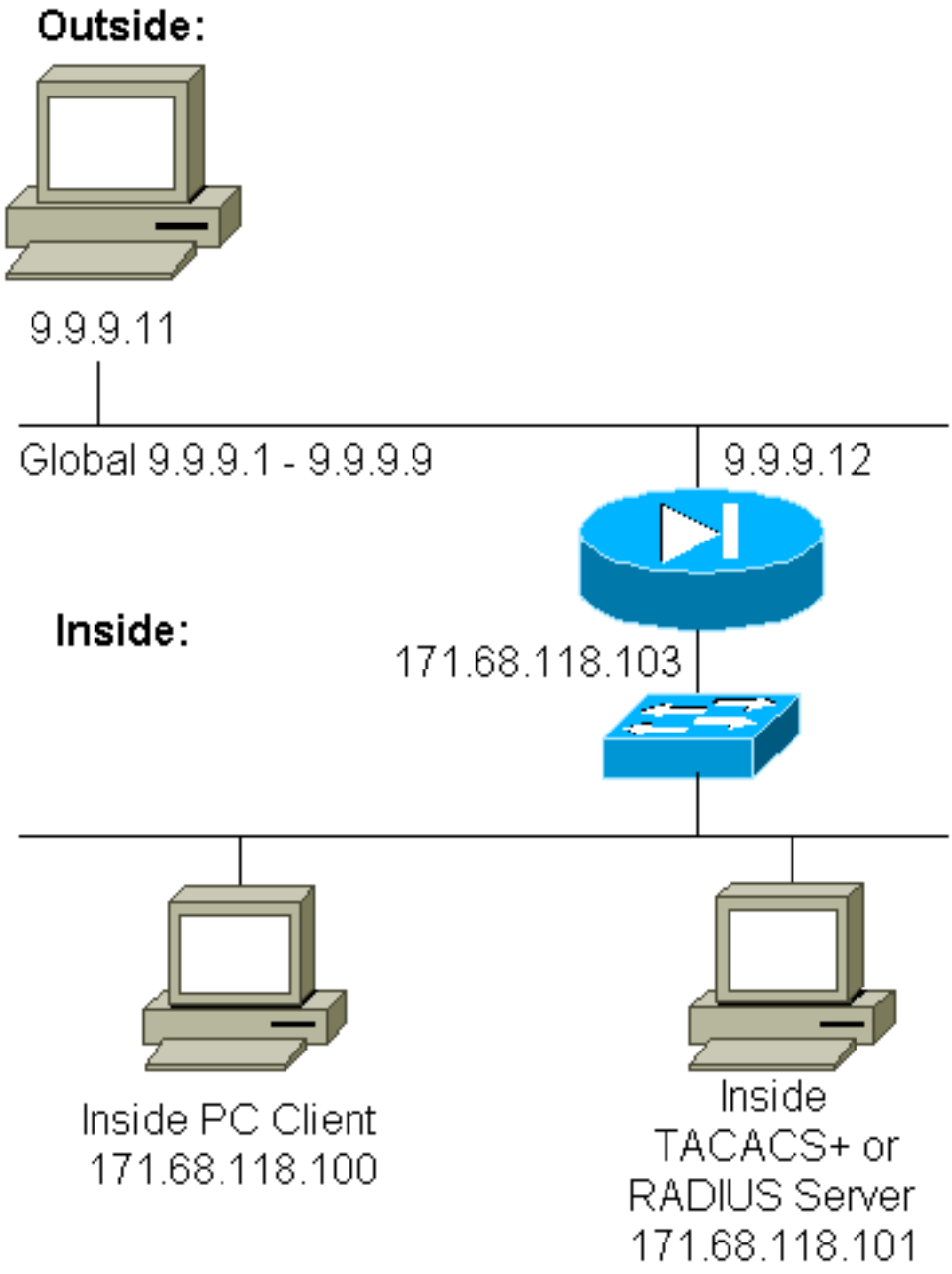
Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione PIX

```
pix2# write terminal
Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
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  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
!--- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout
10
!
!--- The focus of concern is with hosts on the inside
network !--- accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11
   255.255.255.255 tacacs+|radius
!
!--- It is possible to be less granular and authenticate
```

```
!--- all outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

Convenzioni

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

Autenticazione e autorizzazione

- L'autenticazione è *l'*utente.
- L'autorizzazione è *ciò che* l'utente può fare.
- L'autenticazione *è* valida senza autorizzazione.
- Autorizzazione *non* 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 possono 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. Inoltre, a seconda della risposta, apre o nega la connessione. Questi sei utenti potevano utilizzare FTP, Telnet o HTTP.

Si supponga tuttavia che uno di questi tre utenti, "Terry", non sia da considerare attendibile. 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 l'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 che indica 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** - 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 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 "sparare" il nome utente e la password memorizzati nella cache al PIX. e inoltra il messaggio al server di autenticazione. Questo fenomeno viene mostrato nei syslog PIX e/o nei debug del server. Se le connessioni Telnet e FTP sembrano funzionare normalmente, ma le connessioni HTTP no, questo è il motivo.

Configurazioni server utilizzate per tutti gli scenari

Negli esempi di configurazione del server TACACS+, se è attiva solo l'autenticazione, funzionano tutti gli utenti "all", "telnetonly", "httponly" e "ftponly". Negli esempi di configurazione del server RADIUS, l'utente "all" funziona.

Quando si aggiunge l'autorizzazione al PIX, oltre a inviare il nome utente e la password al server di autenticazione TACACS+, il PIX invia i comandi (Telnet, HTTP o FTP) al server TACACS+. Il server TACACS+ controlla quindi se l'utente è autorizzato per il comando.

In un esempio successivo, l'utente all'indirizzo 171.68.118.100 usa il comando **telnet 9.9.9.11**. Quando lo riceve al PIX, il PIX passa il nome utente, la password e il comando al server TACACS+ per elaborarlo.

Pertanto, con l'autorizzazione attivata oltre all'autenticazione, l'utente "telnet only" può eseguire operazioni Telnet tramite il PIX. Tuttavia, gli utenti "httponly" e "ftponly" non possono eseguire operazioni Telnet tramite il PIX.

Anche in questo caso, l'autorizzazione non è supportata con RADIUS a causa della natura della specifica del protocollo.

Configurazione server Cisco Secure UNIX TACACS+

Cisco Secure 2.x

- Le stanze utente sono visualizzate qui.
- Aggiungere l'indirizzo IP PIX o il nome di dominio completo e la chiave a CSU.cfg.

```
user = all {
password = clear "all"
default service = permit
}
```

```
user = telnetonly {
password = clear "telnetonly"
service = shell {
cmd = telnet {
permit .*
}
}
}

user = ftponly {
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 grafica utente (GUI) avanzata per aggiungere l'IP e la chiave PIX all'elenco dei server di accesso alla rete (NAS). La stanza dell'utente appare come mostrato di seguito:

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

Cisco Secure NT 2.x RADIUS

Nella sezione Configurazioni di esempio della documentazione in linea e Web di Cisco Secure 2.1 è descritta la configurazione. L'attributo 6 (Service-Type) sarà Login o Administrative.

Aggiungere l'indirizzo IP del PIX nella sezione di configurazione NAS utilizzando la GUI.

EasyACS TACACS+

La documentazione di EasyACS fornisce informazioni sulla 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** 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. 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 da 1 a 5 per ogni comando consentito (ad esempio, Telnet, HTTP e/o FTP).
7. Aggiungere l'indirizzo IP del PIX nella sezione di configurazione NAS utilizzando la GUI.

Cisco Secure NT 2.x TACACS+

La documentazione di Cisco Secure 2.x fornisce informazioni sulla 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 la casella di controllo **comando** nella parte inferiore e immettere il comando che si desidera consentire, ad esempio Telnet.
4. Se si desidera consentire Telnet a siti specifici, immettere l'indirizzo IP nella sezione degli argomenti (ad esempio, "allow 1.2.3.4"). Per consentire Telnet a tutti i siti, fare clic su **Consenti argomenti non in elenco**.
5. Fare clic su **Invia**.
6. Eseguire i passaggi da 1 a 5 per ogni comando consentito (ad esempio, Telnet, FTP e/o HTTP).
7. Aggiungere l'indirizzo IP del PIX nella sezione di configurazione NAS utilizzando la GUI.

Configurazione server RADIUS Livingston

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

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

Configurazione server RADIUS di tipo Merit

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

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

Configurazione server Freeware TACACS+

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

user = telnetonly {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}
```

```
user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = ftponly {
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 superare il traffico prima di istituire l'AAA, non sarà possibile farlo successivamente.
- 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.

Esempi di debug di autenticazione da PIX

Debug PIX - Buona autenticazione - RADIUS

Questo è un esempio di debug PIX con una buona autenticazione:

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

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

Questo è un esempio di debug PIX con autenticazione (nome utente o password) errata. L'utente vede quattro set di nome utente/password. Viene visualizzato il messaggio di errore: numero massimo di tentativi superato".

Nota: se si tratta di un tentativo FTP, è consentito un solo tentativo. Per HTTP sono consentiti tentativi infiniti.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

Debug PIX - Server inattivo - RADIUS

Questo è un esempio di debug PIX con il server inattivo. Il nome utente viene visualizzato una volta. Il server si blocca e chiede una password (tre volte).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

Debug PIX - Buona autenticazione - TACACS+

Questo è un esempio di debug PIX con una buona autenticazione:

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

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

Questo è un esempio di debug PIX con autenticazione (nome utente o password) errata. L'utente vede quattro set di nome utente/password. Viene visualizzato il messaggio di errore: numero massimo di tentativi superato".

Nota: se si tratta di un tentativo FTP, è consentito un solo tentativo. Per HTTP sono consentiti tentativi infiniti.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

Debug PIX - Server inattivo - TACACS+

Questo è un esempio di debug PIX con il server inattivo. Il nome utente viene visualizzato una volta. Immediatamente viene visualizzato il messaggio di errore "Error: Numero massimo di tentativi superato".

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

Aggiunta dell'autorizzazione

Poiché l'autorizzazione non è valida senza autenticazione, è necessaria per la stessa origine e destinazione:

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius
```

Oppure, se tutti e tre i servizi in uscita sono stati originariamente autenticati:

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
```

Esempi di debug di autenticazione e autorizzazione da PIX

Debug PIX - Buona autenticazione e autorizzazione - TACACS+

Questo è un esempio di debug PIX con una buona autenticazione e autorizzazione:

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

Debug PIX - Buona autenticazione, ma errore di autorizzazione - TACACS+

Questo è un esempio di debug PIX con una buona autenticazione ma un errore nell'autorizzazione:

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

Debug PIX - Autenticazione non valida, Autorizzazione non tentata - TACACS+

Questo è un esempio di debug PIX con autenticazione e autorizzazione, ma il tentativo di autorizzazione non è riuscito a causa di un errore di autenticazione (nome utente o password). L'utente vede quattro set di nome utente/password. Viene visualizzato il messaggio di errore: numero massimo di tentativi superato." viene visualizzato un messaggio

Nota: se si tratta di un tentativo FTP, è consentito un solo tentativo. Per HTTP sono consentiti tentativi infiniti.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
```

```
   to 9.9.9.11/23
```

Debug PIX - Autenticazione/Autorizzazione, Server inattivo - TACACS+

Questo è un esempio di debug PIX con autenticazione e autorizzazione. Il server non è attivo. Il nome utente viene visualizzato una volta. Immediatamente viene visualizzato il messaggio di errore "Error: Numero massimo di tentativi superato." viene visualizzato.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

Aggiungi accounting

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+
```

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". Inoltre, al momento del "Teardown", viene inviata una registrazione contabile "stop":

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

I record di accounting TACACS+ hanno questo aspetto (provengono da Cisco Secure UNIX; i record in Cisco Secure Windows possono essere delimitati da virgole):

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
```

```
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

I campi si scompongono come mostrato di seguito:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RAGGIO

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

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". Inoltre, al momento del "Teardown", viene inviata una registrazione contabile "stop":

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

I record di accounting RADIUS hanno questo aspetto (provengono da Cisco Secure UNIX; quelle in Cisco Secure Windows sono delimitate da virgole):

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

I campi si scompongono come mostrato di seguito:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

Numero massimo di sessioni e visualizzazione degli 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 ha una sessione tramite PIX). Questa procedura è indicata per le connessioni Telnet e FTP a causa della natura delle connessioni. Ad esempio:

L'utente esegue una connessione Telnet da 171.68.118.100 a 9.9.9.25 attraverso il PIX, autenticando durante 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" è connesso. Se l'utente tenta un'altra connessione che richiede l'autenticazione (ad esempio da un altro PC) e max-sessions è impostato su "1" sul server per questo utente, la connessione viene rifiutata dal server.

L'utente avvia il business 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
```

Indica se uauth è uguale a 0, ovvero esegue l'autenticazione ogni volta) o più volte (esegue l'autenticazione 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 tuttavia in modo diverso a causa della natura del protocollo. Questo è un esempio:

L'utente naviga 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 una pagina Web scaricata.

Prendete nota dell'ora. Questo download ha richiesto un secondo (tra il record iniziale e quello finale c'è stato meno di un secondo). L'utente è ancora connesso al sito Web e la connessione è ancora aperta? No.

Max-session o visualizzare gli utenti connessi funzioneranno qui? No, perché il tempo di connessione in HTTP è troppo breve. L'intervallo di tempo tra "Built" e "Teardown" (registrazione di "start" e "stop") è inferiore al secondo. Non ci sarà un record "start" senza un record "stop", dal momento che le registrazioni avvengono praticamente nello stesso istante. Per ogni transazione, sia che l'autenticazione sia impostata su 0 o su un valore superiore, verrà inviato al server un record di tipo "start" e "stop". Tuttavia, il numero massimo di sessioni e la visualizzazione degli utenti connessi non funzioneranno a causa della natura delle connessioni HTTP.

Uso del comando Except

Nella nostra rete, se decidiamo che un utente in uscita (171.68.118.100) non ha bisogno di essere autenticato, possiamo farlo:

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
   255.255.255.255 tacacs+
```

Autenticazione sul PIX

La discussione precedente riguarda l'autenticazione del traffico Telnet (e HTTP, FTP) attraverso il PIX. Nella versione 4.2.2, possono essere autenticate anche le connessioni Telnet al PIX. In questa sezione vengono definiti gli indirizzi IP delle caselle che possono connettersi in modalità Telnet al PIX:

```
telnet 171.68.118.100 255.255.255.255
```

Specificare quindi la password Telnet: **passwd ww**.

Aggiungere il nuovo comando per autenticare gli utenti Telnet su PIX:

```
aaa authentication telnet console tacacs+|radius
```

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.

Modifica del prompt degli utenti Vedere

Se si aggiunge il comando: **auth-prompt YOU_ARE_AT_THE_PIX**, gli utenti che passano attraverso il PIX vedranno la sequenza:

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter the password]
```

All'arrivo alla destinazione finale, vengono visualizzati i prompt "Username:" (Nome utente:) e "Password:" (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.

Informazioni correlate

- Supporto dei prodotti software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems