Esecuzione dell'autenticazione, dell'autorizzazione e dell'accounting degli utenti tramite PIX versione 5.2 e successive

Sommario

Introduzione

L'autenticazione RADIUS e TACACS+ può essere eseguita per le connessioni FTP, Telnet e HTTP tramite Cisco Secure PIX Firewall. L'autenticazione per altri protocolli meno comuni viene in genere eseguita correttamente. L'autorizzazione TACACS+ è supportata. Autorizzazione RADIUS non supportata. Le modifiche apportate all'autenticazione, all'autorizzazione e all'accounting (AAA) PIX 5.2 rispetto alla versione precedente includono il supporto dell'elenco degli accessi AAA per il controllo degli utenti autenticati e delle risorse a cui accedono. In PIX 5.3 e versioni successive, l'autenticazione, l'autorizzazione e l'accounting (AAA) vengono modificati rispetto alle versioni precedenti del codice in quanto le porte RADIUS sono configurabili.

Nota: PIX 6.x può considerare il traffico pass-through ma non il traffico destinato al PIX.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco Secure PIX Firewall versioni 5.2.0.205 e 5.2.0.207

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: se si esegue il software PIX/ASA versione 7.x e successive, consultare il documento sulla configurazione dei server AAA e del database locale.

Convenzioni

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

Autenticazione, autorizzazione e accounting

Di seguito è riportata una spiegazione di Autenticazione, Autorizzazione e Accounting:

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

Caratteristiche visualizzate dall'utente con Autenticazione/Autorizzazione attivata

Quando l'utente tenta di passare dall'interno all'esterno (o viceversa) con autenticazione/autorizzazione su:

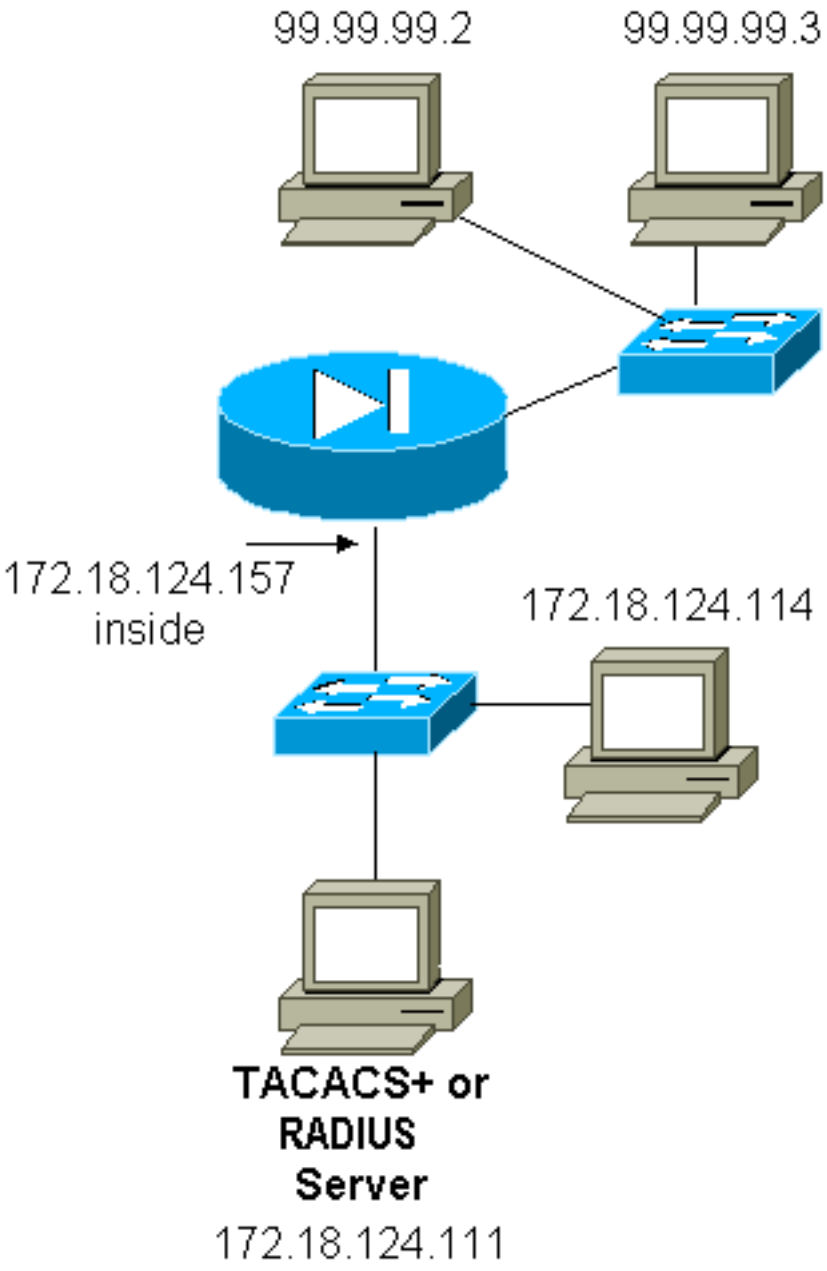
- **Telnet**: viene visualizzato un prompt con il nome utente e una richiesta di password. Se l'autenticazione (e l'autorizzazione) hanno esito positivo sul PIX/server, all'utente vengono richiesti nome utente e password dall'host di destinazione oltre.
- **FTP** - Viene visualizzato il prompt del nome utente. L'utente deve immettere "local_username@remote_username" 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. Se l'autenticazione (e l'autorizzazione) sul PIX/server hanno esito positivo, "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 risulta che il PIX deve interrompere una connessione HTTP ma non lo fa, è probabile che la riautenticazione avvenga effettivamente con il browser che "riprende" il nome utente e la password memorizzati nella cache per il PIX. Il PIX inoltra il messaggio al server di autenticazione. Questo fenomeno viene mostrato nel syslog PIX e/o nel debug del server. Se Telnet e FTP sembrano funzionare "normalmente", ma le connessioni HTTP no, questo è il motivo.

Passaggi di debug

- Verificare che la configurazione PIX funzioni prima di aggiungere l'autenticazione e l'autorizzazione AAA. Se non si riesce a far passare il traffico prima di creare l'autenticazione e l'autorizzazione, non è possibile farlo in seguito.
- Attivare un tipo di accesso al PIX.Eseguire il comando **logging console debug** per attivare il debug della console di registrazione.**Nota:** non utilizzare il debug della console di registrazione in un sistema con carico elevato.Utilizzare il comando **log monitor debug** per registrare una sessione Telnet.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.
- Attivare il debug sui server TACACS+ o RADIUS.

Solo autenticazione

Esempio di rete



Configurazione server - Solo autenticazione

Configurazione server TACACS Cisco Secure UNIX

```
User = cse {
password = clear "cse"
default service = permit
}
```

Configurazione server Cisco Secure UNIX RADIUS

Nota: Aggiungere l'indirizzo IP e la chiave PIX all'elenco dei server di accesso alla rete (NAS) con

l'aiuto della GUI avanzata.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure Windows RADIUS

Per configurare un server Cisco Secure Windows RADIUS, attenersi alla seguente procedura.

1. Ottenere una password nella sezione **Impostazione utente**.
2. Dalla sezione **Configurazione gruppo**, impostare l'attributo 6 (Service-Type) su **Login** o **Administrative**.
3. Aggiungere l'indirizzo IP PIX nella sezione **Configurazione NAS** della GUI.

Cisco Secure Windows TACACS+

L'utente ottiene una password nella sezione **Impostazione utente**.

Configurazione server RADIUS Livingston

Nota: Aggiungere indirizzo IP e chiave PIX al file *client*.

- Bill Password="foo" User-Service-Type = Shell-User

Configurazione server RADIUS di tipo Merit

Nota: Aggiungere indirizzo IP e chiave PIX al file *client*.

- Bill Password="foo" Service-Type = Shell-User

Configurazione server Freeware TACACS+

```
key = "cisco"
user = cse {
login = cleartext "cse"
default service = permit
}
```

Configurazione iniziale PIX - Solo autenticazione

Configurazione iniziale PIX - Solo autenticazione
`PIX Version 5.2(0)205`

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
```

```
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
!
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

Porte RADIUS configurabili (5.3 e versioni successive)

Alcuni server RADIUS utilizzano porte RADIUS diverse da 1645/1646 (generalmente 1812/1813). In PIX 5.3 e versioni successive, le porte di autenticazione e accounting RADIUS possono essere impostate su un valore diverso da quello predefinito 1645/1646 con i seguenti comandi:

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

Esempi di debug dell'autenticazione PIX

Per informazioni su come attivare il debug, vedere Procedura di debug. Questi sono esempi di utenti che in modalità 99.99.99.2 avviano il traffico verso l'interno 172.18.124.114 (99.99.99.99) e viceversa. Il traffico in entrata è autenticato TACACS e il traffico in uscita è autenticato RADIUS.

Autenticazione riuscita - TACACS+ (in entrata)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Autenticazione non riuscita a causa di nome utente/password errati - TACACS+ (in entrata). L'utente vede "Errore: Numero massimo di tentativi superato."

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

Server che non parla a PIX - TACACS+ (in entrata). L'utente vede il nome utente una volta e il PIX non chiede mai una password (questa è in Telnet). L'utente vede "Errore: Numero massimo di tentativi superato."

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Buona autenticazione - RADIUS (in uscita)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

Autenticazione non valida (nome utente o password) - RADIUS (in uscita). L'utente vede la richiesta di Nome utente, quindi Password, ha tre opportunità per inserirli e, se non riesce, vedere "Errore: Numero massimo di tentativi superato."

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

Pingable del server ma daemon inattivo, pingable del server non consentito o key/client non corrispondente. Non è possibile comunicare con PIX - RADIUS (in uscita). L'utente vede Nome

utente, password, "Server RADIUS non riuscito" e infine "Errore: Numero massimo di tentativi superato."

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Autenticazione più autorizzazione

Se si desidera consentire a tutti gli utenti autenticati di eseguire tutte le operazioni (HTTP, FTP e Telnet) tramite PIX, è sufficiente l'autenticazione e l'autorizzazione non è necessaria. Se tuttavia si desidera consentire l'accesso a determinati sottoinsiemi di servizi a determinati utenti o limitare l'accesso a determinati siti, è necessaria l'autorizzazione. L'autorizzazione RADIUS non è valida per il traffico attraverso il PIX. In questo caso, l'autorizzazione TACACS+ è valida.

Se l'autenticazione passa e l'autorizzazione è attiva, il PIX invia al server il comando che l'utente sta eseguendo. Ad esempio, "http 1.2.3.4." Nella versione 5.2 di PIX, l'autorizzazione TACACS+ viene usata in combinazione con gli elenchi degli accessi per controllare dove vanno gli utenti.

Se si desidera implementare l'autorizzazione per HTTP (siti Web visitati), utilizzare un software quale Websense poiché a un singolo sito Web possono essere associati numerosi indirizzi IP.

Configurazione server - Autenticazione più Autorizzazione

Configurazione server TACACS Cisco Secure UNIX

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

  user = can_only_do_ftp {
  password = clear "*******"
  service = shell {
  cmd = ftp {
  permit .*
  }
  }
  }

  user = httponly {
  password = clear "********"
  service = shell {
  cmd = http {
  permit .*
```

```
  }
  }
  }
```

Cisco Secure Windows TACACS+

Completare la procedura seguente per configurare un server Cisco Secure Windows TACACS+.

1. Fare clic su **Deny unmatched IOS commands** in fondo al programma di configurazione del gruppo.
2. Fare clic su **Aggiungi/Modifica nuovo comando (FTP, HTTP, Telnet)**.Ad esempio, se si desidera consentire la connessione Telnet a un sito specifico ("telnet 1.2.3.4"), il comando è **telnet**. L'argomento è *1.2.3.4*. Dopo aver compilato "command=**telnet**", immettere gli indirizzi IP "allow" nel rettangolo dell'argomento (ad esempio, "allow 1.2.3.4"). Se sono consentite tutte le connessioni Telnet, il comando è ancora **telnet**, ma fare clic su **Consenti tutti gli argomenti non elencati**. Fare quindi clic su **Fine modifica**.
3. Eseguire il passaggio 2 per ogni comando consentito, ad esempio Telnet, HTTP e FTP.
4. Aggiungere l'indirizzo IP PIX nella sezione di configurazione NAS con l'aiuto della GUI.

Configurazione server Freeware TACACS+

```
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 .*
   }
   }
```

Configurazione PIX - Aggiunta autorizzazione

Aggiungere comandi per richiedere l'autorizzazione:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

La nuova funzionalità della versione 5.2 consente a questa istruzione, insieme all'elenco degli

accessi 101 definito in precedenza, di sostituire le tre istruzioni precedenti. Il vecchio e il nuovo verbo non devono essere mescolati.

```
aaa authorization match 101 outside AuthInbound
```

Esempi di debug di autenticazione e autorizzazione PIX

Buona autenticazione e autorizzazione riuscite - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

Buona autenticazione ma autorizzazione non riuscita - TACACS+. L'utente vede anche il messaggio "Error: Autorizzazione negata."

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Nuova funzionalità elenco accessi

Nel software PIX versione 5.2 e successive, definire gli elenchi degli accessi sul PIX. Applicarli per singolo utente in base al profilo utente sul server. TACACS+ richiede l'autenticazione e l'autorizzazione. RADIUS richiede solo l'autenticazione. Nell'esempio, vengono modificate l'autenticazione e l'autorizzazione in uscita per TACACS+. È stato configurato un elenco degli accessi sul PIX.

Nota: in PIX versione 6.0.1 e successive, se si utilizza RADIUS, gli elenchi degli accessi vengono implementati immettendo l'elenco nell'attributo standard IETF RADIUS 11 (Filter-Id) [CSCdt50422]. Nell'esempio, l'attributo 11 è impostato su 115 anziché sulla parola "acl=115" specifica del fornitore.

Configurazione PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

Profili server

Nota: la versione 2.1 del freeware TACACS+ non riconosce la parola "acl".

Configurazione server Cisco Secure UNIX TACACS+

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Cisco Secure Windows TACACS+

Per aggiungere l'autorizzazione al PIX per controllare dove l'utente deve andare con gli elenchi degli accessi, selezionare **shell/exec**, selezionare la casella **Access control list** (elenco di controllo degli accessi) e immettere il numero (corrisponde al numero dell'elenco degli accessi sul PIX).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Cisco Secure Windows RADIUS

RADIUS/Cisco è il tipo di dispositivo. L'utente "pixa" ha bisogno di un nome utente, una password, un segno di spunta e "acl=115" nella casella rettangolare Cisco/RADIUS dove dice 009\001 AV-Pair (specifico del fornitore).

Uscita

L'utente in uscita "pixa" con "acl=115" nel profilo esegue l'autenticazione e l'autorizzazione. Il server trasmette l'acl=115 al PIX, e il PIX mostra quanto segue:

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
```

```
access-list 115
absolute   timeout: 0:05:00
inactivity timeout: 0:00:00
```

Quando l'utente "pixa" tenta di passare a 99.99.99.3 (o a un indirizzo IP diverso da 99.99.99.2, perché c'è un rifiuto implicito), vede questo:

```
Error: acl authorization denied
```

Nuovo Elenco Degli Accessi Per Utente Scaricabile Con Versione 6.2

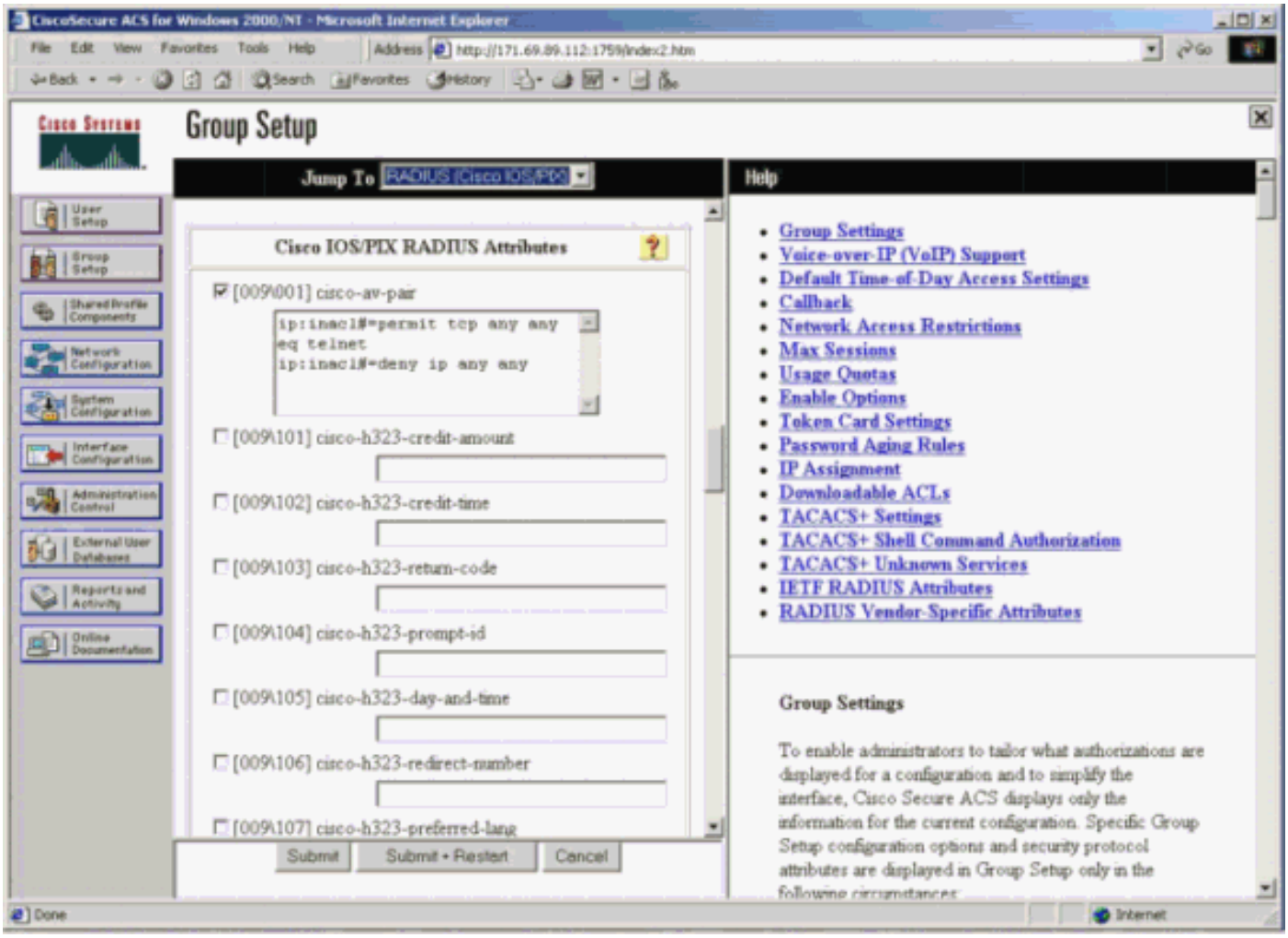
Nel software versione 6.2 e successive del firewall PIX, gli elenchi degli accessi sono definiti su un server di controllo di accesso (ACS) da scaricare sul PIX dopo l'autenticazione. Funziona solo con il protocollo RADIUS. Non è necessario configurare l'elenco degli accessi sul PIX stesso. Un modello di gruppo viene applicato a più utenti.

Nelle versioni precedenti, l'elenco degli accessi viene definito sul PIX. Dopo l'autenticazione, ACS ha inserito il nome dell'elenco degli accessi nel PIX. La nuova versione consente all'ACS di inserire l'elenco degli accessi direttamente nel PIX.

Nota: in caso di failover, la tabella di autenticazione non viene copiata. Gli utenti vengono riautenticati. L'elenco degli accessi viene scaricato nuovamente.

Configurazione ACS

Fare clic su **Group Setup** (Configurazione gruppo) e selezionare il tipo di dispositivo **RADIUS (Cisco IOS/PIX)** per configurare un account utente. Assegnare un nome utente ("case", in questo esempio) e una password per l'utente. Dall'elenco Attributi, selezionare l'opzione per configurare **[009\001]** ***vendor-av*-pair**. Definire l'elenco degli accessi come illustrato nell'esempio seguente:



Debug PIX: Elenco degli accessi scaricati e di autenticazione validi

- Consente solo Telnet e nega altro traffico.

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

Output del comando **show auth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

Output del comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Nega solo Telnet e consente altro traffico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

  Output del comando **show auth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

  Output del comando **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

Nuovo elenco degli accessi scaricabili per utente con ACS 3.0

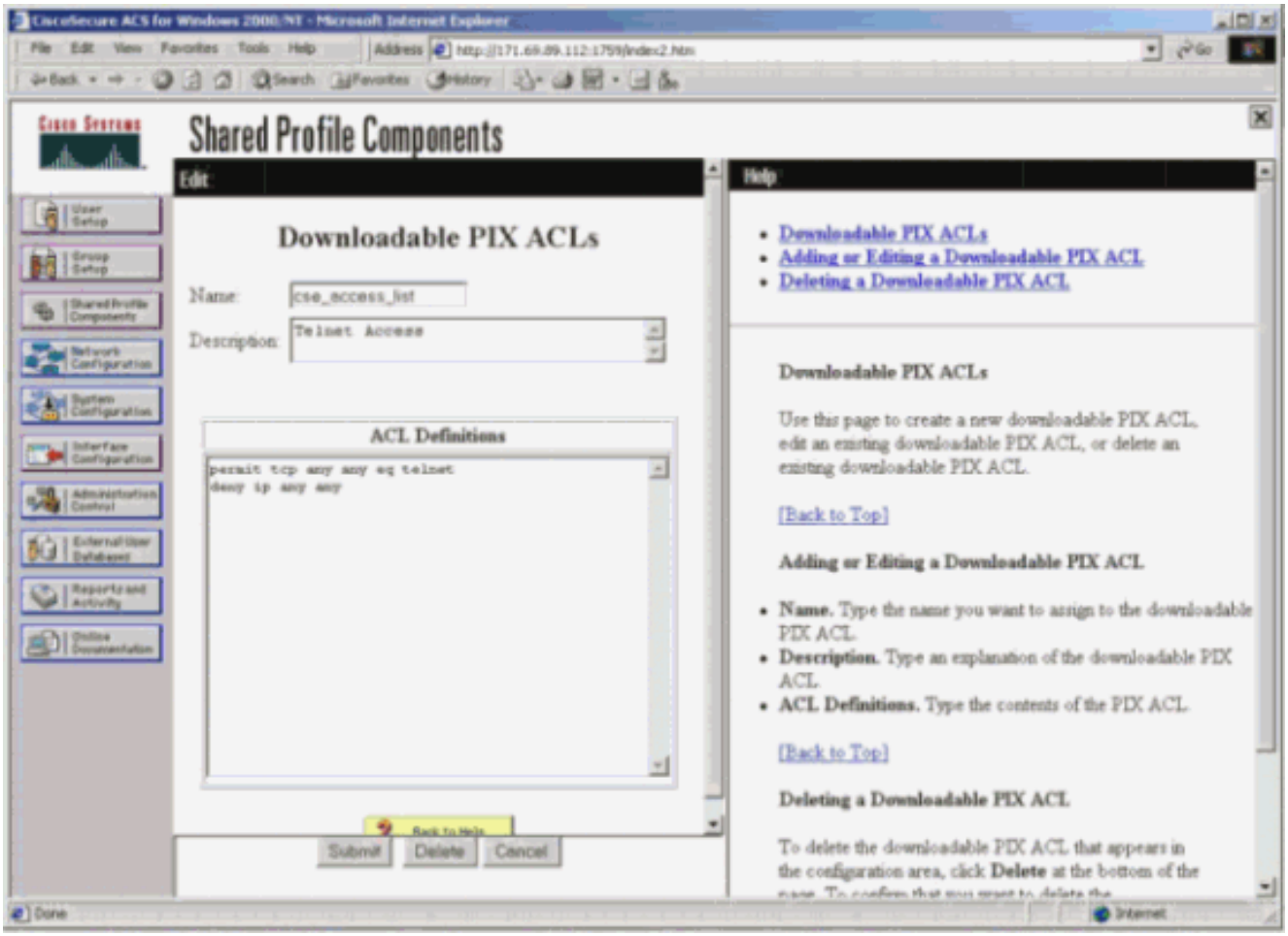
In ACS versione 3.0, il componente del profilo condiviso consente all'utente di creare un modello di elenco degli accessi e di definire il nome del modello per utenti o gruppi specifici. Il nome del modello può essere utilizzato con il numero di utenti o gruppi desiderato. In questo modo, non è più necessario configurare elenchi degli accessi identici per ciascun utente.

Nota: se si verifica il failover, l'autenticazione non viene copiata sul PIX secondario. Nel failover stateful, la sessione viene mantenuta. È tuttavia necessario riautenticare la nuova connessione e scaricare nuovamente l'elenco degli accessi.

Utilizzo dei profili condivisi

Eseguire i seguenti passaggi quando si utilizzano profili condivisi.

1. Fare clic su **Configurazione interfaccia**.
2. Selezionare **ACL scaricabili a livello di utente** e/o **ACL scaricabili a livello di gruppo**.
3. Fare clic su **Componenti profilo condiviso**. Fare clic su **ACL scaricabili a livello utente**.
4. Definire gli ACL scaricabili.
5. Fare clic su **Imposta gruppo**. In ACL scaricabili, assegnare l'elenco degli accessi PIX all'elenco degli accessi creato in precedenza.



Debug PIX: Autenticazione valida ed elenco degli accessi scaricati con profili condivisi

- Consente solo Telnet e nega altro traffico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

Output del comando **show auth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

Output del comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   deny ip any any (hitcnt=0)
```

```
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- Nega solo Telnet e consente altro traffico.

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

Output del comando **show auth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

Output del comando **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

Aggiungi accounting

Configurazione PIX - Aggiungi accounting

TACACS (AuthInbound=tacacs)

Aggiungere questo comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

In alternativa, utilizzare la nuova funzionalità della versione 5.2 per definire gli elementi che devono essere considerati dagli elenchi degli accessi.

```
aaa accounting match 101 outside AuthInbound
```

Nota: l'elenco degli accessi 101 è definito separatamente.

RADIUS (AuthOutbound=radius)

Aggiungere questo comando.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

In alternativa, utilizzare la nuova funzionalità della versione 5.2 per definire gli elementi che devono essere considerati dagli elenchi degli accessi.

```
aaa accounting match 101 outside AuthOutbound
```

Nota: l'elenco degli accessi 101 è definito separatamente.

Nota: i record contabili possono essere generati per le sessioni amministrative sul PIX a partire dal codice PIX 7.0.

Esempi di accounting

- Esempio di contabilità TACACS per Telnet da 99.99.99.2 esterno a 172.18.124.114 interno (99.99.99.99).

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- Esempio di accounting RADIUS per la connessione da 172.18.124.114 interna a 99.99.99.2 esterna (Telnet) e 99.99.99.3 esterna (HTTP).

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23
```

```
    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Start
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Username = cse
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Stop
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Acct-Session-Id = 0x0000000a
            Username = cse
            Acct-Session-Time = 0
            Acct-Input-Octets = 1277
            Acct-Output-Octets = 310
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80
```

Uso del comando exclude

In questa rete, se si decide che una determinata origine o destinazione non richiede autenticazione, autorizzazione o accounting, eseguire questi comandi.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

Nota: I comandi **include** sono già disponibili.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

Oppure, con la nuova feature in 5.2, definite ciò che desiderate escludere.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
```

```
aaa accounting match 101 outside AuthInbound
```

Nota: se si esclude una casella dall'autenticazione e si dispone dell'autorizzazione per, è necessario escludere anche la casella dall'autorizzazione.

Max-session e Visualizza 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 tuttavia appropriata per HTTP. In questo esempio viene utilizzata una configurazione di rete diversa, ma i concetti sono gli stessi.

L'utente esegue una connessione Telnet attraverso il PIX, autenticandosi 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 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 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 di arresto, a questo punto 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 esce (trascorre dieci minuti in tale host).

```
    (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 in cui l'utente scorre 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 non è connesso al sito Web. La connessione non è aperta quando l'utente legge la pagina Web. Max-session o visualizzare gli utenti connessi non funzionano qui. Ciò è dovuto al fatto che 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 esiste una registrazione "start" senza una registrazione "stop", in quanto le registrazioni vengono effettuate praticamente nello stesso istante. È ancora presente un record "start" e "stop" inviato 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 funzionano a causa della natura delle connessioni HTTP.

Interfaccia utente

Modifica del prompt Utenti Vedere

Se si dispone del comando:

```
auth-prompt prompt PIX515B
```

quindi gli utenti che passano attraverso il PIX vedono questo prompt.

```
PIX515B
```

Personalizzare il messaggio visualizzato dagli utenti Vedere

Se si dispone dei comandi:

```
auth-prompt accept "GOOD_AUTHENTICATION"
auth-prompt reject "BAD_AUTHENTICATION"
```

gli utenti visualizzeranno quindi un messaggio relativo allo stato di autenticazione in caso di accesso non riuscito/riuscito.

```
PIX515B
Username: junk
Password:
"BAD_AUTHENTICATION"

PIX515B
Username: cse
Password:
"GOOD_AUTHENTICATION"
```

Timeout di inattività e assoluti per utente

Il comando PIX **timeout auth** controlla la frequenza con cui è richiesta la riautenticazione. Se l'autenticazione/autorizzazione TACACS+ è attiva, il controllo viene effettuato per singolo utente. Questo profilo utente è configurato per controllare il timeout (sul server freeware TACACS+ e i timeout sono espressi in minuti).

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

Dopo l'autenticazione/autorizzazione:

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

Alla fine di due minuti:

Timeout assoluto - la sessione viene interrotta:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

HTTP virtuale in uscita

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

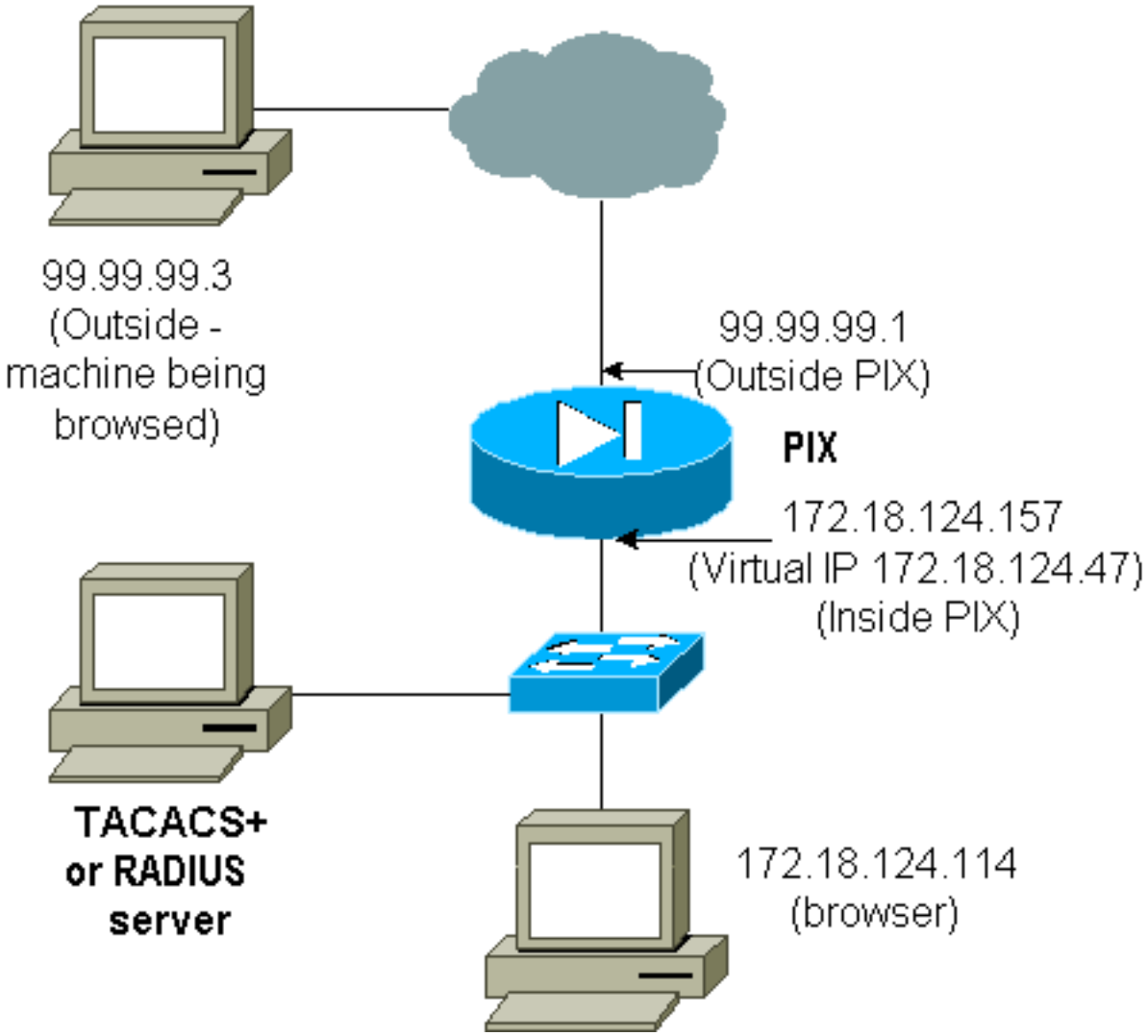
Per evitare questo problema, implementare il protocollo HTTP virtuale aggiungendo un indirizzo

RFC 1918 (un indirizzo non instradabile su Internet, ma valido e univoco per la rete PIX interna) alla configurazione PIX nel formato.

```
virtual http #.#.#.#
```

Quando l'utente tenta di uscire dal PIX, è necessaria l'autenticazione. Se il parametro warn è presente, l'utente riceve un messaggio di reindirizzamento. L'autenticazione è valida per la durata dell'autenticazione. Come indicato nella documentazione, non impostare la durata del comando **timeout auth** su 0 secondi con HTTP virtuale. Ciò impedisce le connessioni HTTP al server Web reale.

Nota: gli indirizzi HTTP e IP Telnet virtuali devono essere inclusi nelle istruzioni di **autenticazione aaa**. In questo esempio, l'impostazione di 0.0.0.0 non include questi indirizzi.



Nella configurazione PIX aggiungere questo comando.

```
virtual http 172.18.124.47
```

L'utente punta il browser su 99.99.99.3. Viene visualizzato questo messaggio.

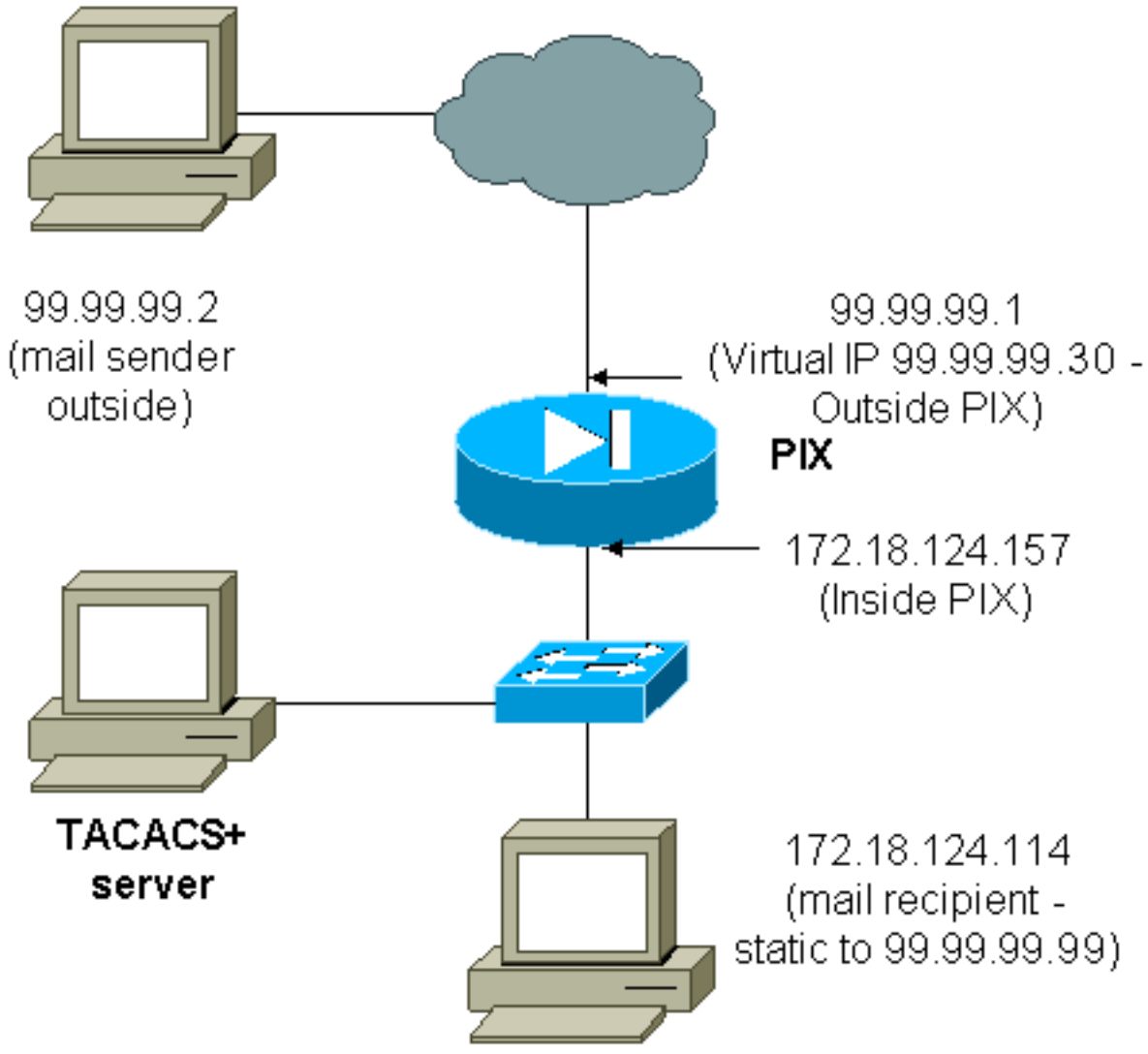
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Dopo l'autenticazione, il traffico viene reindirizzato a 99.99.99.3.

Telnet virtuale

Nota: gli indirizzi HTTP e IP Telnet virtuali devono essere inclusi nelle istruzioni di **autenticazione aaa**. In questo esempio, l'impostazione di 0.0.0.0 non include questi indirizzi.

Virtual Telnet in entrata



Non è consigliabile autenticare la posta in entrata poiché non viene visualizzata una finestra per l'invio della posta in entrata. Usare il comando **exclude**. Ma a scopo illustrativo, questi comandi sono aggiunti.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

```
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

Gli utenti (questo è TACACS+ freeware):

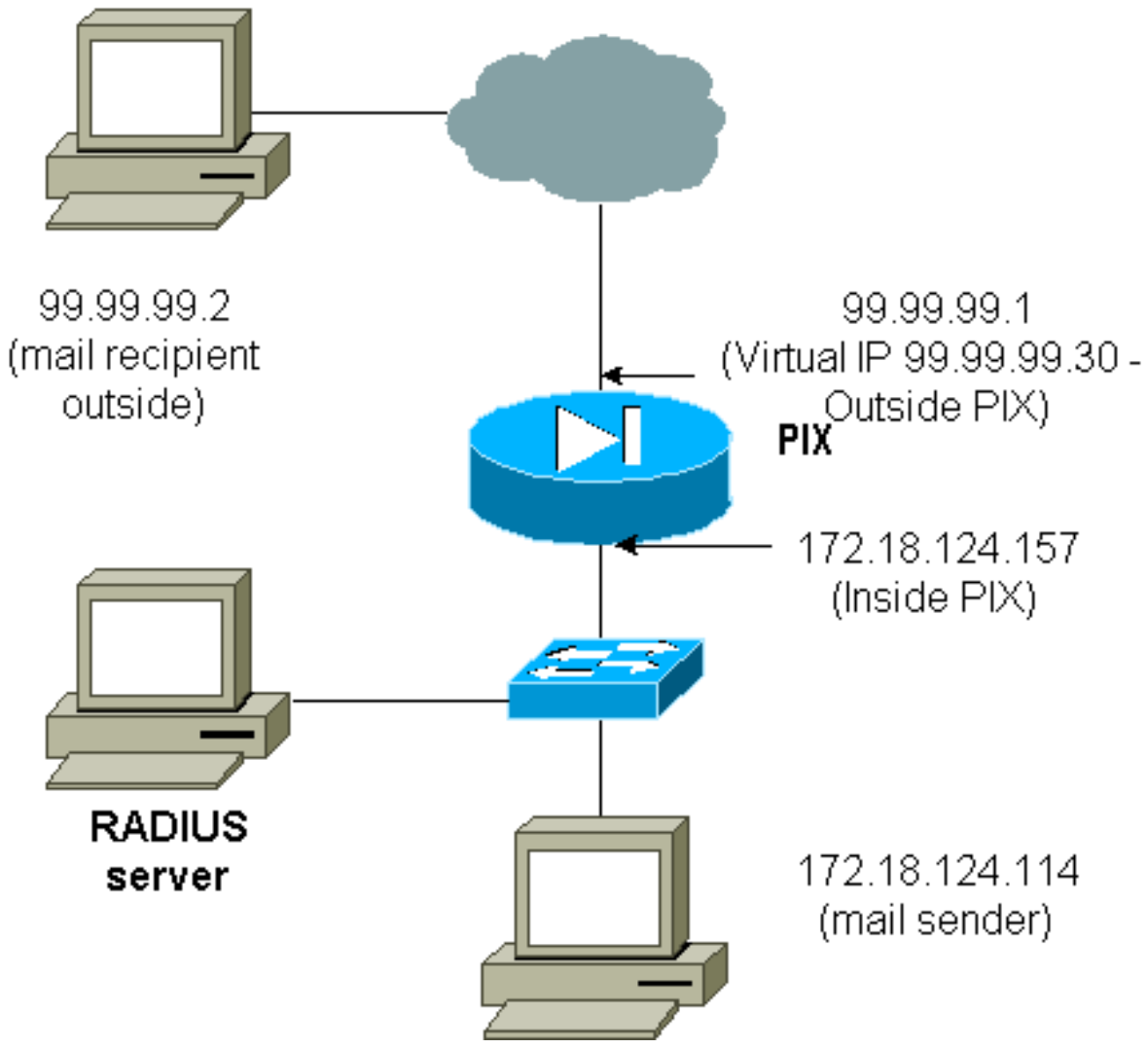
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

Se è attivata solo l'autenticazione, entrambi gli utenti inviano la posta in entrata dopo l'autenticazione su Telnet all'indirizzo IP 99.99.99.30. Se l'autorizzazione è attivata, l'utente "cse" Telnet su 99.99.99.30 e immette il nome utente e la password TACACS+. La connessione Telnet viene interrotta. L'utente "case" invia quindi la posta a 99.99.99.99 (172.18.124.114). Autenticazione riuscita per l'utente "pixuser". Tuttavia, quando il PIX invia la richiesta di autorizzazione per cmd=tcp/25 e cmd-arg=172.18.124.114, la richiesta ha esito negativo, come mostrato in questo output.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
```

```
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

Virtual Telnet in uscita



Non è consigliabile autenticare la posta in entrata poiché non viene visualizzata una finestra per l'invio della posta in entrata. Usare il comando **exclude**. Ma a scopo illustrativo, questi comandi sono aggiunti.

Non è consigliabile autenticare la posta in uscita, poiché non viene visualizzata una finestra per l'invio della posta in uscita. Usare il comando **exclude**. A scopo illustrativo, tuttavia, vengono aggiunti questi comandi.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

Per inviare la posta dall'interno all'esterno, visualizzare un prompt dei comandi sull'host della posta e su Telnet fino a 99.99.99.30. In questo modo si apre la strada alla posta. La posta è inviata da 172.18.124.114 a 99.99.99.2:

```
   305002: Translation built for gaddr 99.99.99.99
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Disconnessione Telnet Virtuale

Quando gli utenti si collegano in modalità Telnet all'indirizzo IP Telnet virtuale, il comando **show auth** visualizza l'ora di apertura del foro. Se si desidera impedire il passaggio del traffico al termine delle sessioni (quando il tempo rimane nell'autenticazione), è necessario che gli utenti eseguano nuovamente la connessione Telnet all'indirizzo IP Telnet virtuale. La sessione viene disattivata. Questo esempio lo illustra.

Prima autenticazione

```
 109001: Auth start for user '???'
```

```
   from 172.18.124.114/32862 to 99.99.99.30/23
109011: Authen Session Start: user 'cse', Sid 15
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/32862 to
   99.99.99.30/23 on interface inside
```

Dopo la prima autenticazione

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

Seconda autenticazione

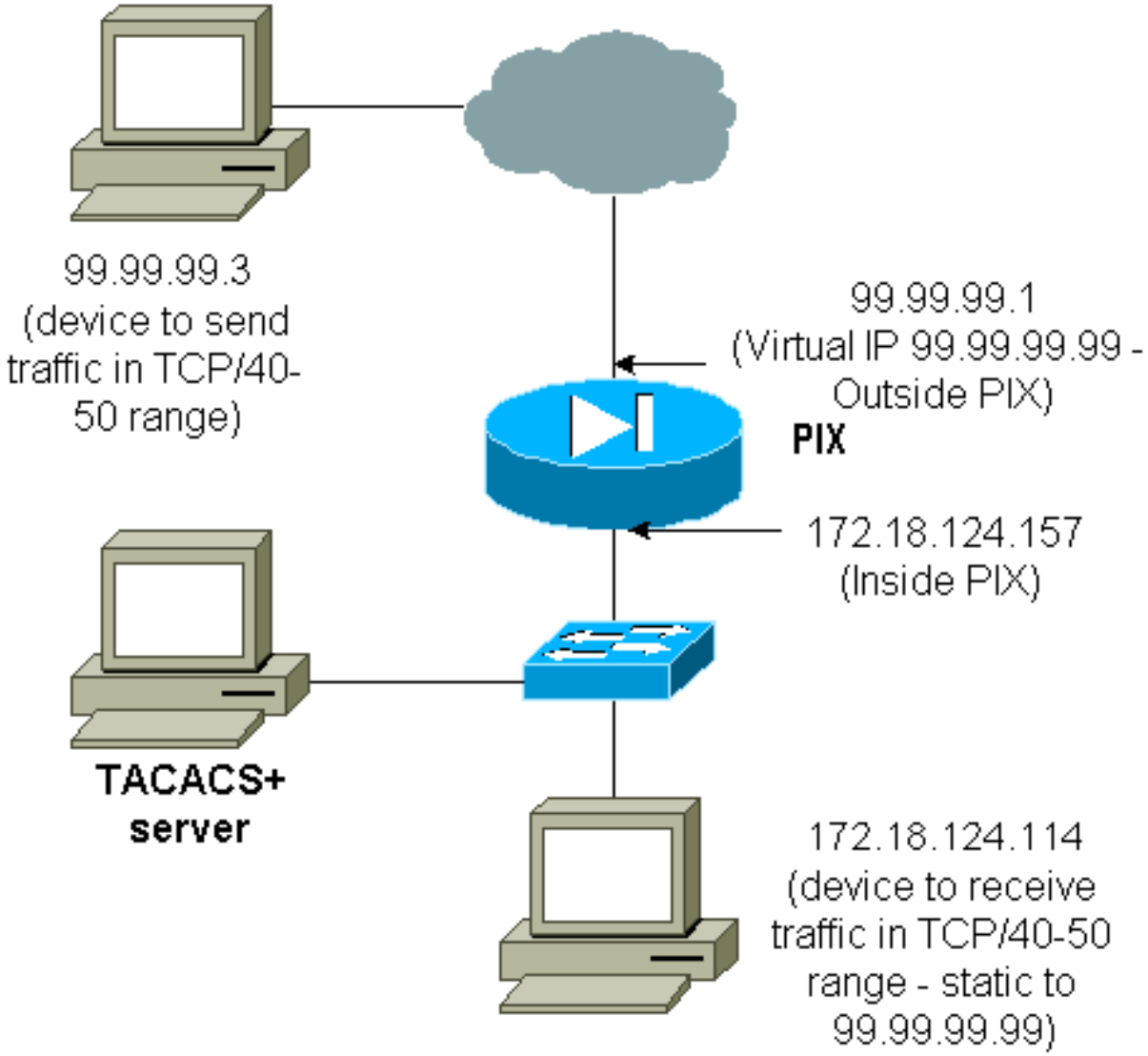
```
   pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

Dopo la seconda autenticazione

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

Port Authorization

Esempio di rete



Autorizzazione consentita per intervalli di porte. Se sul PIX è configurato Virtual Telnet e l'autorizzazione è configurata per un intervallo di porte, l'utente apre il buco con Virtual Telnet. Quindi, se l'autorizzazione per un intervallo di porte è attiva e il traffico in tale intervallo raggiunge il PIX, il PIX invia il comando al server TACACS+ per l'autorizzazione. Nell'esempio viene mostrata l'autorizzazione in entrata su un intervallo di porte.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

Esempio di configurazione del server TACACS+ (freeware):

```
  user = cse {
  login = cleartext "numeric"
  cmd = tcp/40-50 {
  permit 172.18.124.114
  }
  }
```

L'utente deve prima connettersi all'indirizzo IP virtuale 99.99.99.99. Dopo l'autenticazione, quando un utente tenta di eseguire il push del traffico TCP nell'intervallo della porta 40-50 tramite il PIX fino a 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 viene inviato al server TACACS+ con cmd-arg=172.18.124.14 :

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

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

Dopo aver verificato che la modalità Telnet virtuale consenta il traffico TCP/40-50 verso l'host all'interno della rete, aggiungere l'accounting per questo traffico con questi comandi.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.

aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

Esempio di record contabili TACACS+

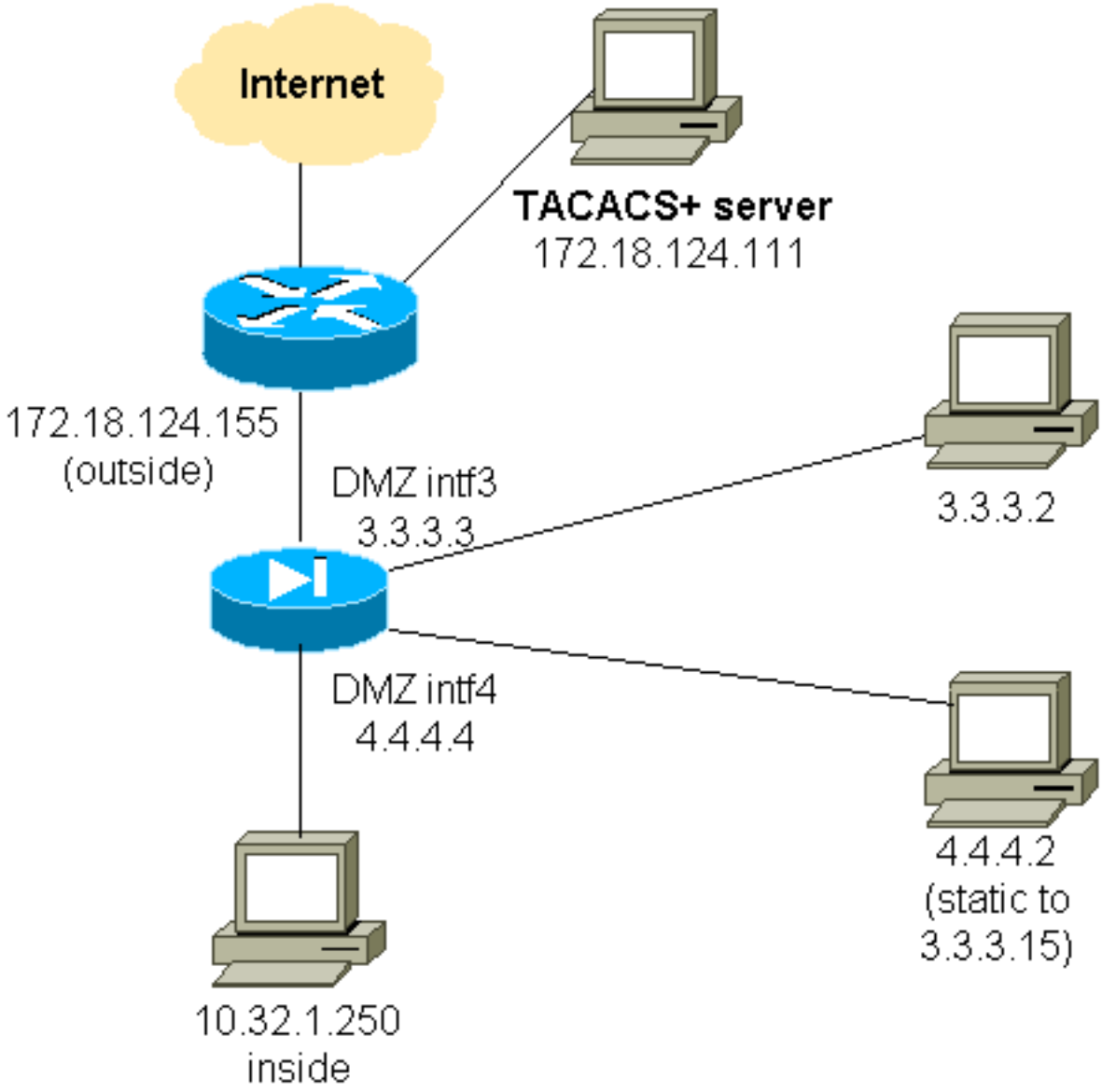
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

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. Per quanto riguarda PIX, la disposizione è la seguente:

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Esempio di rete



Configurazione PIX parziale

Autenticare il traffico Telnet tra pix/intf3 e pix/intf4, come mostrato di seguito.

Configurazione PIX parziale
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) interface ethernet0 auto interface ethernet1 auto (interface ethernet2 auto shutdown)

```
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

Informazioni da raccogliere se si apre una richiesta TAC

Se dopo aver eseguito le procedure di risoluzione dei problemi sopra descritte si desidera continuare a ricevere assistenza e si desidera aprire una richiesta di assistenza in Cisco TAC, includere queste informazioni per la risoluzione dei problemi di PIX Firewall.

- Descrizione del problema e dettagli sulla topologia
- Risoluzione dei problemi prima di aprire la richiesta
- Output del comando **show tech-support**
- Output del comando **show log** dopo l'esecuzione con il comando **logging buffered debugging** o acquisizioni della console che dimostrano il problema (se disponibile)

Allegare i dati raccolti alla richiesta in formato testo normale non compresso (txt). Allegare le informazioni alla richiesta caricandole con l'aiuto dello strumento Case Query Tool (solo utenti registrati). Se non è possibile accedere allo strumento Case Query, inviare le informazioni in un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto.

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Cisco Secure Access Control Server per Windows
- Cisco Secure Access Control Server per UNIX
- TACACS+ (Terminal Access Controller Access Control System)
- RADIUS (Remote Authentication Dial-In User Service)
- Documentazione e supporto tecnico – Cisco Systems