Risoluzione dei problemi di connessione tramite PIX e ASA

Sommario

Introduzione

In questo documento vengono forniti suggerimenti e suggerimenti per la risoluzione dei problemi quando si usano Cisco ASA serie 5500 Adaptive Security Appliance (ASA) e Cisco PIX serie 500 Security Appliance. Nella maggior parte dei casi, quando le applicazioni o le origini di rete si interrompono o non sono disponibili, i firewall (PIX o ASA) tendono ad essere una destinazione

primaria e sono ritenuti la causa delle interruzioni. Con alcuni test sull'appliance ASA o sui PIX, l'amministratore può determinare se l'appliance ASA/i PIX causa il problema o meno.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA: Stabilire e risolvere i problemi di connettività tramite Cisco Security Appliance per ulteriori informazioni sulla risoluzione dei problemi relativi all'interfaccia sulle appliance di sicurezza Cisco.

Nota: questo documento si focalizza sull'appliance ASA e sui PIX. Una volta completata la risoluzione dei problemi sull'appliance ASA o sul PIX, potrebbe essere necessaria un'ulteriore risoluzione dei problemi con altri dispositivi (router, switch, server e così via).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco ASA 5510 con OS 7.2.1 e 8.3.

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.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- ASA e PIX OS 7.0, 7.1, 8.3 e versioni successive
- Firewall Services Module (FWSM) 2.2, 2.3 e 3.1

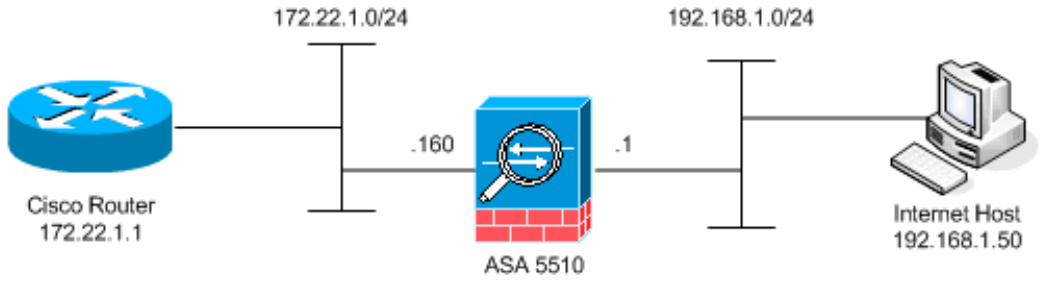
Nota: la sintassi e i comandi specifici possono variare a seconda della versione del software.

Convenzioni

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

Premesse

L'esempio presuppone che l'ASA o il PIX sia in produzione. La configurazione ASA/PIX può essere relativamente semplice (solo 50 linee di configurazione) o complessa (da centinaia a migliaia di linee di configurazione). Gli utenti (client) o i server possono trovarsi su una rete protetta (interna) o non protetta (DMZ o esterna).



L'ASA inizia con questa configurazione. La configurazione ha lo scopo di fornire al laboratorio un punto di riferimento.

Configurazione iniziale dell'ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
```

```
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


!--- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Problema

Un utente contatta il reparto IT e segnala che l'applicazione X non funziona più. La richiesta di assistenza viene inoltrata all'amministratore ASA/PIX. L'amministratore non ha alcuna conoscenza di questa particolare applicazione. Con l'uso di ASA/PIX, l'amministratore scopre quali porte e protocolli vengono usati dall'applicazione X e quale potrebbe essere la causa del problema.

Soluzione

L'amministratore ASA/PIX deve raccogliere quante più informazioni possibile dall'utente. Le informazioni utili includono:

- Indirizzo IP di origine: in genere corrisponde alla workstation o al computer dell'utente.
- Indirizzo IP di destinazione: l'indirizzo IP del server a cui l'utente o l'applicazione tenta di connettersi.
- Porte e protocolli utilizzati dall'applicazione

Spesso l'amministratore ha la fortuna di ottenere una risposta a una di queste domande. In questo esempio, l'amministratore non è in grado di raccogliere informazioni. L'analisi dei messaggi syslog ASA/PIX è ideale, ma se l'amministratore non sa cosa cercare, è difficile individuare il problema.

Passaggio 1 - Individuazione dell'indirizzo IP dell'utente

Esistono molti modi per individuare l'indirizzo IP dell'utente. In questo documento vengono illustrati l'appliance ASA e i PIX, quindi l'indirizzo IP viene individuato usando le appliance ASA e PIX.

L'utente tenta di comunicare con l'appliance ASA/PIX. Questa comunicazione può essere ICMP, Telnet, SSH o HTTP. Il protocollo scelto deve avere un'attività limitata sull'appliance ASA/PIX. Nell'esempio specifico, l'utente esegue il ping sull'interfaccia interna dell'appliance ASA.

L'amministratore deve configurare una o più opzioni e chiedere all'utente di eseguire il ping sull'interfaccia interna dell'appliance ASA.

- **Syslog**Assicurarsi che la registrazione sia attivata. Il livello di registrazione deve essere impostato su **debug**. La registrazione può essere inviata a vari percorsi. In questo esempio viene utilizzato il buffer di registro ASA. Potrebbe essere necessario un server di registrazione esterno negli ambienti di produzione.
```
ciscoasa(config)#logging enable
ciscoasa(config)#logging buffered debugging
```

  L'utente effettua il ping sull'interfaccia interna dell'ASA (ping 192.168.1.1). Viene visualizzato questo output.
```
ciscoasa#show logging
!--- Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
%ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
!--- The user IP address is 192.168.1.50.
```
- **Funzione di acquisizione ASA**L'amministratore deve creare un elenco degli accessi che definisca il traffico che l'appliance ASA deve acquisire. Dopo aver definito l'elenco degli accessi, il comando **capture** incorpora l'elenco degli accessi e lo applica a un'interfaccia.
```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

  L'utente effettua il ping sull'interfaccia interna dell'ASA (ping 192.168.1.1). Viene visualizzato questo output.
```
ciscoasa#show capture inside_interface
   1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
 !--- The user IP address is 192.168.1.50.
```
  Nota: per scaricare il file di acquisizione in un sistema come Etheral, potete farlo come mostrato in questo output.

```
!--- Open an Internet Explorer and browse with this https link format: https://[
```

  Per ulteriori informazioni, fare riferimento al documento ASA/PIX: Acquisizione di pacchetti con CLI e ASDM - Esempio di configurazione per ulteriori informazioni sull'acquisizione di pacchetti nell'appliance ASA.
- **Debug**Il comando **debug icmp trace** viene usato per acquisire il traffico ICMP dell'utente.
```
ciscoasa#debug icmp trace
```

  L'utente effettua il ping sull'interfaccia interna dell'ASA (ping 192.168.1.1). Questo output viene visualizzato sulla console.

```
ciscoasa#
!--- Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

Per disabilitare **debug icmp trace**, usare uno dei seguenti comandi:**nessuna traccia icmp di debugannulla debug traccia icmpundebug all**, **undebug all** o **undebug all**

Ognuna di queste tre opzioni consente all'amministratore di determinare l'indirizzo IP di origine. In questo esempio, l'indirizzo IP di origine dell'utente è 192.168.1.50. L'amministratore è pronto a ottenere ulteriori informazioni sull'applicazione X e a determinare la causa del problema.

Passaggio 2 - Individuare la causa del problema

Con riferimento alle informazioni elencate nella sezione Passaggio 1 di questo documento, l'amministratore ora conosce l'origine di una sessione X dell'applicazione. L'amministratore è pronto per ottenere ulteriori informazioni sull'applicazione X e per iniziare a individuare i possibili problemi.

L'amministratore ASA/PIX deve preparare l'ASA per almeno uno dei suggerimenti elencati. Quando l'amministratore è pronto, l'utente avvia l'applicazione X e limita tutte le altre attività, in quanto un'attività aggiuntiva dell'utente potrebbe creare confusione o fuorviare l'amministratore ASA/PIX.

- **Monitorare i messaggi syslog.**Cercare l'indirizzo IP di origine dell'utente che si trova nel passo 1. L'utente avvia l'applicazione X. L'amministratore ASA usa il comando **show logging** e visualizza l'output.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-
305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
```

  I log rivelano che l'indirizzo IP di destinazione è 172.22.1.1, il protocollo è TCP, la porta di destinazione è HTTP/80 e che il traffico viene inviato all'interfaccia esterna.
- **Modificare i filtri di acquisizione.**il comando **access-list inside_test** è stato usato in precedenza e viene usato qui.

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the
ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.
ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
!--- Clears the previously logged data. !--- The no capture inside_interface removes/deletes
the capture.
```

  L'utente avvia l'applicazione X. L'amministratore ASA usa quindi il comando **show capture inside_interface** e visualizza l'output.

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

Il traffico acquisito fornisce all'amministratore diverse informazioni importanti:Indirizzo di destinazione—172.22.1.1Numero porta—80/httpProtocollo—TCP (si noti il flag "S" o syn)Inoltre, l'amministratore sa che il traffico di dati per l'applicazione X arriva all'appliance ASA.Se l'output del comando **show capture inside_interface** è stato questo, il traffico dell'applicazione non ha mai raggiunto l'ASA oppure il filtro di acquisizione non è stato impostato per acquisire il traffico:

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

In questo caso, l'amministratore deve prendere in considerazione l'eventualità di verificare anche il computer dell'utente e i router o altri dispositivi di rete presenti nel percorso tra il computer dell'utente e l'appliance ASA.**Nota:** quando il traffico arriva a un'interfaccia, il comando **capture** registra i dati prima che i criteri di sicurezza ASA analizzino il traffico. Ad esempio, un elenco degli accessi nega tutto il traffico in entrata su un'interfaccia. Il comando **capture** registra ancora il traffico. La policy di sicurezza ASA analizza quindi il traffico.

- **Debug**L'amministratore non ha familiarità con l'applicazione X e pertanto non sa quali servizi di debug abilitare per l'analisi dell'applicazione X. A questo punto, il debug potrebbe non essere l'opzione migliore per la risoluzione dei problemi.

Con le informazioni raccolte nel passaggio 2, l'amministratore ASA ottiene diverse informazioni importanti. L'amministratore sa che il traffico arriva all'interfaccia interna dell'ASA, all'indirizzo IP di origine, all'indirizzo IP di destinazione e all'applicazione di servizio usata da X (TCP/80). Dai syslog, l'amministratore sa anche che inizialmente la comunicazione era permessa.

Fase 3 - Conferma e monitoraggio del traffico delle applicazioni

L'amministratore ASA desidera verificare che il traffico X dell'applicazione abbia lasciato l'ASA e controllare l'eventuale traffico di ritorno dall'Application X Server.

- **Monitorare i messaggi syslog.**Filtrare i messaggi syslog per l'indirizzo IP di origine (192.168.1.50) o per l'indirizzo IP di destinazione (172.22.1.1). Dalla riga di comando, filtrare i messaggi syslog equivale a **visualizzare la registrazione | includere 192.168.1.50** o **mostrare logging | include 172.22.1.1**. Nell'esempio, il comando **show logging** viene usato senza filtri. L'output viene eliminato per facilitare la lettura.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

Il messaggio syslog indica che la connessione è stata chiusa a causa del timeout SYN. Questo messaggio avvisa l'amministratore che l'appliance ASA non ha ricevuto alcuna risposta dall'application X server. I motivi di interruzione dei messaggi di syslog possono variare.Il timeout SYN viene registrato a causa di una terminazione forzata della connessione dopo 30 secondi che si verifica dopo il completamento dell'handshake a tre vie. Questo problema si verifica in genere se il server non risponde a una richiesta di connessione e, nella maggior parte dei casi, non è correlato alla configurazione in PIX/ASA.Per risolvere il problema, fare riferimento all'elenco di controllo seguente:Assicurarsi che il comando statico

sia stato immesso correttamente e che non si sovrapponga ad altri comandi statici, ad esempio

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

Il NAT statico in ASA 8.3 e versioni successive può essere configurato come mostrato di seguito:

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

Verificare che esista un elenco degli accessi per consentire l'accesso all'indirizzo IP globale dall'esterno e che sia associato all'interfaccia:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

Per una connessione corretta al server, il gateway predefinito sul server deve puntare all'interfaccia DMZ di PIX/ASA.Per ulteriori informazioni sui messaggi syslog, consultare il documento sui messaggi di sistema ASA.

- **Crea un nuovo filtro di acquisizione.**In base al traffico acquisito in precedenza e ai messaggi syslog, l'amministratore sa che l'applicazione X deve lasciare l'ASA attraverso l'interfaccia esterna.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
!--- When you leave the source as 'any', it allows !--- the administrator to monitor any
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
!--- When you reverse the source and destination information, !--- it allows return traffic
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
interface outside
```

L'utente deve avviare una nuova sessione con l'applicazione X. Dopo aver avviato una nuova sessione X dell'applicazione, l'amministratore ASA deve usare il comando **show capture outside_interface** sull'appliance ASA.

```
ciscoasa(config)#show capture outside_interface
3 packets captured
   1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
   2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
   3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

L'acquisizione mostra il traffico in uscita dall'interfaccia esterna, ma non mostra il traffico di risposta dal server 172.22.1.1. Questa acquisizione mostra i dati quando escono dall'appliance ASA.

- **Usare l'opzione packet-tracer.**Nelle sezioni precedenti, l'amministratore ASA ha ricevuto informazioni sufficienti per usare l'opzione **packet-tracer** nell'appliance ASA.**Nota:** l'ASA supporta il comando **packet-tracer** a partire dalla versione 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any
number can be used. !--- More common source ports typically range !--- between 1025 and
65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC
Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule
Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW
Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type:
ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0
255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-
```

group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
** match ip inside 192.168.1.0 255.255.255.0 outside any**
**   dynamic translation to pool 1 (172.22.1.254)**
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13

```
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the
next host !--- that should receive the data packet. Result: input-interface: inside input-
status: up input-line-status: up output-interface: outside output-status: up output-line-
status: up Action: allow
```

L'output più importante del comando **packet-tracer** è l'ultima riga, ossia `Action: consentire`.

Le tre opzioni del passo 3 mostrano ciascuna all'amministratore che l'ASA non è responsabile dei problemi X dell'applicazione. Il traffico X dell'applicazione lascia l'ASA e l'ASA non riceve una risposta dall'Application X Server.

Cos'è il prossimo?

Esistono molti componenti che consentono all'applicazione X di funzionare correttamente per gli utenti. I componenti includono il computer dell'utente, il client X dell'applicazione, il routing, i criteri di accesso e il server X dell'applicazione. Nell'esempio precedente, è stato dimostrato che l'ASA riceve e inoltra il traffico X dell'applicazione. Gli amministratori di server e applicazioni X dovrebbero essere coinvolti. Gli amministratori devono verificare che i servizi dell'applicazione siano in esecuzione, esaminare eventuali registri sul server e verificare che il traffico dell'utente sia ricevuto dal server e dall'applicazione X.

Problema: Messaggio di errore Terminazione connessione TCP-Proxy

Viene visualizzato questo messaggio di errore:

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

Soluzione

Spiegazione: Questo messaggio viene visualizzato quando viene superato il limite del buffer di riassemblaggio durante l'assemblaggio dei segmenti TCP.

- *source_address/source_port*: indirizzo IP di origine e porta di origine del pacchetto che avvia la connessione.
- *dest_address/dest_port*: indirizzo IP di destinazione e porta di destinazione del pacchetto che avvia la connessione.
- *interface_inside*: nome dell'interfaccia a cui arriva il pacchetto che ha avviato la connessione.
- *interface_outside* - Nome dell'interfaccia su cui si trova il pacchetto che ha avviato la connessione.
- *limit* - Limite configurato per le connessioni embrionali per la classe di traffico.

Per risolvere il problema, disattivare l'ispezione RTSP nell'accessorio di sicurezza come illustrato.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsl15229 (solo utenti registrati).

Problema: "%ASA-6-10003: Il routing non è riuscito a individuare l'hop successivo per il protocollo dall'interfaccia src" Messaggio di errore

ASA interrompe il traffico con l'`errore:%ASA-6-10003: Il routing non è in grado di individuare l'hop successivo per il protocollo dal messaggio di` errore `interfaccia:src IP/src porta all'interfaccia:dest IP/dest porta.`

Soluzione

Questo errore si verifica quando l'ASA cerca di trovare l'hop successivo su una tabella di routing dell'interfaccia. In genere, questo messaggio viene ricevuto quando l'ASA ha una conversione (xlate) creata su un'interfaccia e un percorso che punta a un'interfaccia diversa. Verificare la presenza di una configurazione errata nelle istruzioni NAT. La risoluzione della configurazione errata può risolvere l'errore.

Problema: Connessione bloccata dall'ASA con " %ASA-5-305013: Corrispondenza delle regole NAT asimmetriche per i flussi forward e reverse" Messaggio di errore

La connessione è bloccata dall'ASA e viene visualizzato questo messaggio di errore:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
```

```
 failure.
```

Soluzione

Quando si esegue il NAT, l'ASA tenta anche di invertire il pacchetto e controlla se ha esito positivo sulle traduzioni. Se non colpisce nessuna o una traduzione NAT diversa, allora c'è una mancata corrispondenza. Questo messaggio di errore viene visualizzato in genere quando vi sono diverse regole NAT configurate per il traffico in entrata e in uscita con la stessa origine e destinazione. Controllare la dichiarazione NAT per il traffico in questione.

Problema: Errore di ricezione - %ASA-5-321001: Raggiunto limite di 10000 risorse 'conns' per il sistema

Soluzione

Questo errore indica che le connessioni per un server situato su un'appliance ASA hanno raggiunto il limite massimo. Ciò potrebbe indicare un attacco DoS a un server della rete. Usare MPF sull'appliance ASA e ridurre il limite delle connessioni embrionali. Inoltre, abilitare Dead Connection Detection (DCD). Fare riferimento a questo frammento di configurazione:

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

Problema: Errore di ricezione %PIX-1-106021: Nega controllo inverso percorso TCP/UDP da src_addr a dest_addr nell'interfaccia int_name

Soluzione

Questo messaggio di registro viene ricevuto quando è abilitata la verifica inversa del percorso. Per risolvere il problema e disattivare il controllo inverso del percorso, usare questo comando:

```
no ip verify reverse-path interface
```

Problema: Interruzione della connettività Internet a causa del rilevamento di minacce

Sull'appliance ASA viene visualizzato questo messaggio di errore:

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

Soluzione

Questo messaggio viene generato dal rilevamento delle minacce a causa della configurazione predefinita, quando viene rilevato un comportamento anomalo del traffico. Il messaggio riguarda Miralix Licen 3000, una porta TCP/UDP. Individuare il dispositivo che utilizza la porta 3000. Controllare le statistiche grafiche ASDM per rilevare le minacce e verificare i primi attacchi per verificare se mostra la porta 3000 e l'indirizzo IP di origine. Se il dispositivo è legittimo, è possibile aumentare la velocità di rilevamento delle minacce sull'appliance ASA per risolvere il messaggio di errore.

Informazioni correlate

- Guida di riferimento ai comandi di Cisco ASA
- Guida di riferimento ai comandi di Cisco PIX
- Messaggi di errore e di sistema Cisco ASA
- Messaggi di errore e di sistema Cisco PIX
- Cisco ASA serie 5500 Adaptive Security Appliance Support
- Cisco PIX serie 500 Security Appliance Support
- Documentazione e supporto tecnico – Cisco Systems