ASA/PIX 7.x e versioni successive: Riduzione degli attacchi alla rete

Sommario

Introduzione

In questo documento viene descritto come mitigare i vari attacchi alla rete, ad esempio la negazione dei servizi (DoS), utilizzando Cisco Security Appliance (ASA/PIX).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata una appliance Cisco Adaptive Security Appliance (ASA) serie 5500 con software versione 7.0 e successive.

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

Questo documento può essere usato anche con Cisco serie 500 PIX con software versione 7.0 e successive.

Convenzioni

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

Protezione dagli attacchi SYN

Come mitigare gli attacchi TCP (Transmission Control Protocol) di sincronizzazione/avvio (SYN) sull'appliance ASA/PIX?

Attacco SYN TCP

L'attacco SYN di TCP è un tipo di attacco DoS in cui un mittente trasmette un volume di connessioni che non possono essere completate. In questo modo le code di connessione si riempiono, negando in tal modo il servizio agli utenti TCP legittimi.

Quando si avvia una normale connessione TCP, un host di destinazione riceve un pacchetto SYN da un host di origine e restituisce una conferma di sincronizzazione (SYN ACK). L'host di destinazione deve quindi ascoltare un ACK del SYN ACK prima di stabilire la connessione. Questo processo è noto come handshake TCP a tre vie.

In attesa che il ACK venga inviato al SYN ACK, una coda di connessione di dimensioni finite sull'host di destinazione tiene traccia delle connessioni in attesa di completamento. In genere questa coda si svuota rapidamente perché si prevede che l'ACK arrivi alcuni millisecondi dopo l'ACK SYN.

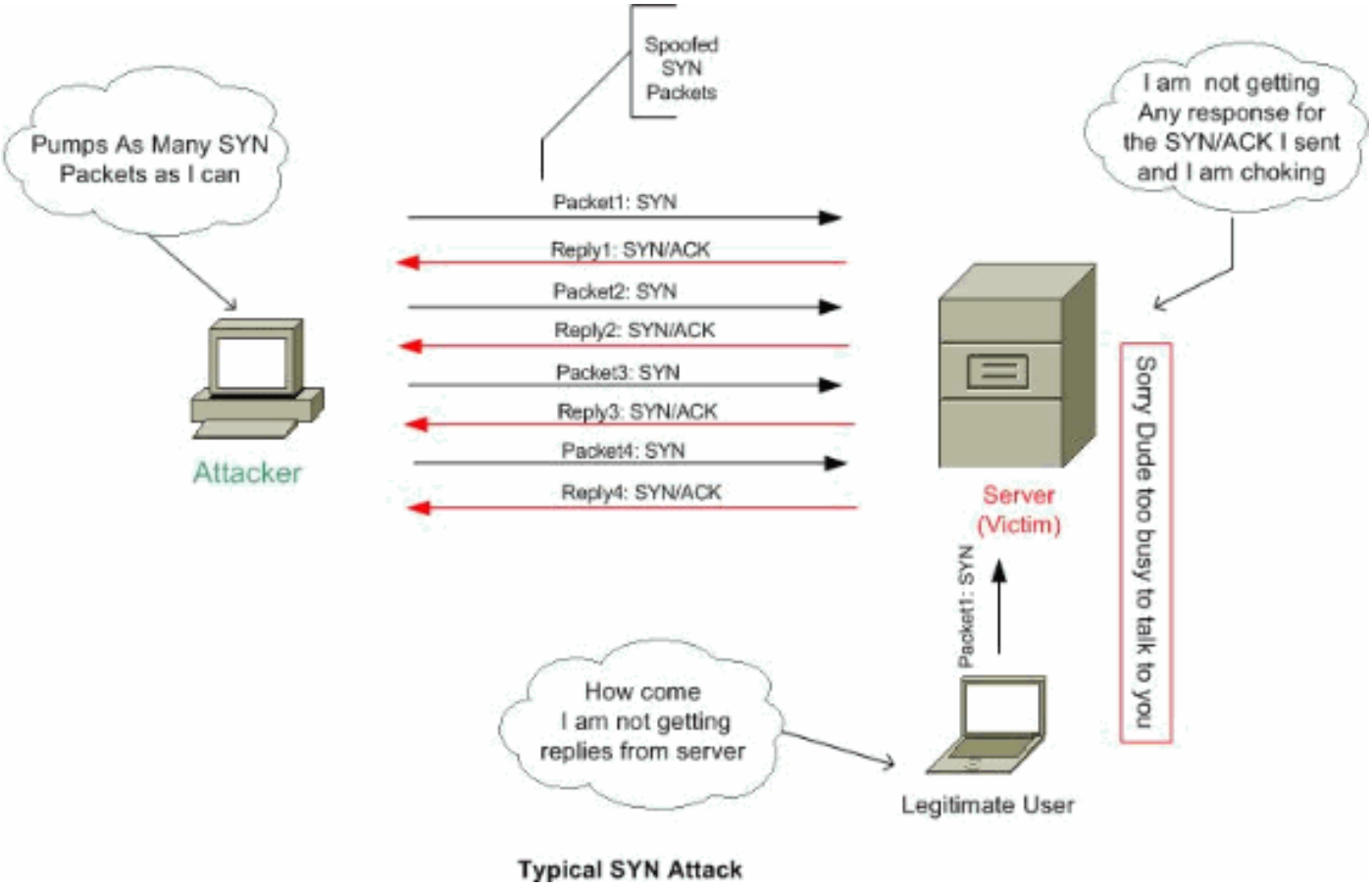
L'attacco TCP SYN sfrutta questo progetto facendo in modo che un host di origine di attacco generi pacchetti TCP SYN con indirizzi di origine casuali verso un host vittima. L'host di destinazione della vittima invia un SYN ACK all'indirizzo di origine casuale e aggiunge una voce alla coda di connessione. Poiché l'ACK SYN è destinato a un host errato o inesistente, l'ultima parte dell'handshake a tre vie non viene mai completata e la voce rimane nella coda di connessione fino alla scadenza di un timer, in genere per circa un minuto. Generando rapidamente pacchetti TCP SYN falsi da indirizzi IP casuali, è possibile riempire la coda di connessione e negare i servizi TCP (come e-mail, trasferimento file o WWW) agli utenti legittimi.

Non c'è un modo semplice per rintracciare l'autore dell'attacco perché l'indirizzo IP della fonte è falsificato.

Le manifestazioni esterne del problema includono l'impossibilità di ricevere posta elettronica, di accettare connessioni ai servizi WWW o FTP o a un numero elevato di connessioni TCP sull'host nello stato SYN_RCVD.

Per ulteriori informazioni sugli attacchi SYN di TCP, fare riferimento a Difese dagli attacchi

flooding SYN di TCP.



Typical SYN Attack

Riduzione

In questa sezione viene descritto come mitigare gli attacchi SYN impostando il numero massimo di connessioni TCP e UDP (User Datagram Protocol), il numero massimo di connessioni embrionali, i timeout di connessione e come disabilitare la randomizzazione della sequenza TCP.

Se viene raggiunto il limite di connessioni embrionali, l'appliance di sicurezza risponde a ogni pacchetto SYN inviato al server con SYN+ACK e non passa il pacchetto SYN al server interno. Se il dispositivo esterno risponde con un pacchetto ACK, l'appliance di sicurezza sa che la richiesta è valida (e non fa parte di un potenziale attacco SYN). L'accessorio di protezione stabilisce quindi una connessione con il server e unisce le connessioni. Se l'appliance di sicurezza non ottiene un ACK dal server, interrompe aggressivamente la connessione embrionale.

Ogni connessione TCP ha due ISN (Initial Sequence Number): uno generato dal client e uno generato dal server. L'appliance di sicurezza usa l'ISN di TCP SYN in modo casuale, passando in entrambe le direzioni di entrata e di uscita.

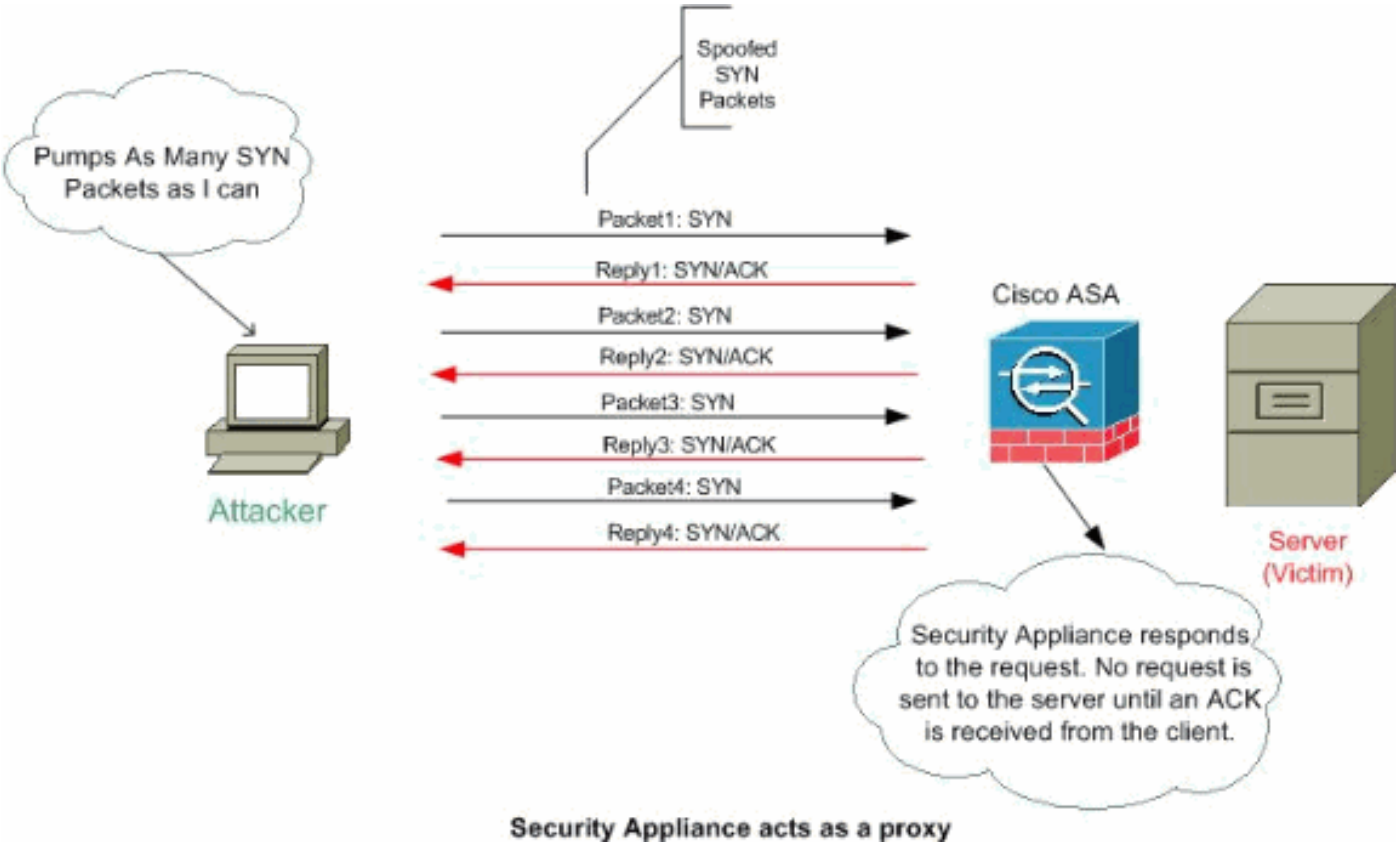
La casualità dell'ISDN dell'host protetto impedisce all'autore di un attacco di prevedere l'ISDN successivo per una nuova connessione e potenzialmente di dirottare la nuova sessione.

Se necessario, è possibile disabilitare la randomizzazione dei numeri di sequenza iniziali TCP. Ad esempio:

- Se anche un altro firewall in linea sta randomizzando i numeri di sequenza iniziali, non è necessario che entrambi i firewall eseguano questa azione, anche se questa azione non influisce sul traffico.

- Se si utilizza il multi-hop BGP (eBGP) esterno tramite l'appliance di sicurezza e i peer eBGP utilizzano l'MD5, la casualità interrompe il checksum MD5.
- Èpossibile utilizzare un dispositivo WAAS (Wide Area Application Services) che richiede che l'accessorio di sicurezza non utilizzi numeri di sequenza casuali delle connessioni.

Nota: è anche possibile configurare il numero massimo di connessioni, il numero massimo di connessioni embrionali e la randomizzazione della sequenza TCP nella configurazione NAT. Se si configurano queste impostazioni per lo stesso traffico utilizzando entrambi i metodi, l'accessorio di protezione utilizzerà il limite inferiore. Per l'assegnazione casuale della sequenza TCP, se viene disattivata utilizzando uno dei due metodi, l'appliance di sicurezza disattiva l'assegnazione casuale della sequenza TCP.



Security Appliance acts as a proxy

Completare questa procedura per impostare i limiti della connessione:

1. Per identificare il traffico, aggiungere una mappa delle classi utilizzando il comando **class-map** in base a Utilizzo di Modular Policy Framework.
2. Per aggiungere o modificare una **mappa dei criteri** che imposta le azioni da eseguire con il traffico della mappa delle classi, immettere questo comando:
   ```
   hostname(config)#policy-map name
   ```
3. Per identificare la mappa di classe (dal passaggio 1) a cui si desidera assegnare un'azione, immettere questo comando:
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. Per impostare il numero massimo di connessioni (sia TCP che UDP), il numero massimo di connessioni embrionali, per-client-embronic-max, per-client-max o se disabilitare la randomizzazione della sequenza TCP, immettere questo comando:
   ```
   hostname(config-pmap-c)#set connection {[conn-max number]
   [embryonic-conn-max number] [per-client-embryonic-max number]
   [per-client-max number][random-sequence-number {enable |
   ```

```
disable}}
```

Dove number è un numero intero compreso tra 0 e 65535. Il valore predefinito è 0, che indica nessun limite per le connessioni.Èpossibile immettere questo comando su una sola riga (in qualsiasi ordine) oppure immettere ogni attributo come comando separato. Il comando viene combinato su una riga nella configurazione corrente.

5. Per impostare il timeout per le connessioni, le connessioni embrionali (semichiuse) e le connessioni semichiuse, immettere questo comando:

```
hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
[half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
```

Dove hh[:mm[:ss] **embrionale** è un'ora compresa tra 0:0:5 e 1192:59:59. Il valore predefinito è 0:0:30. È inoltre possibile impostare questo valore su 0, che indica che la connessione non si interrompe mai.I valori **semichiusi** hh[:mm[:ss] e **tcp** hh[:mm[:ss] sono compresi tra 0:5:0 e 1192:59:59. Il valore predefinito per **semichiuso** è 0:10:0 e il valore predefinito per **tcp** è 1:0:0. È inoltre possibile impostare questi valori su 0, che indica che la connessione non si interrompe mai.Èpossibile immettere questo comando su una sola riga (in qualsiasi ordine) oppure immettere ogni attributo come comando separato. Il comando viene combinato su una riga nella configurazione corrente.**Connessione embrionale (mezza apertura)** - Una connessione embrionale è una richiesta di connessione TCP che non ha completato il handshake necessario tra l'origine e la destinazione.**Connessione semichiusa (Half-closed connection)** - La connessione semichiusa si verifica quando viene chiusa in una sola direzione mediante l'invio di FIN. Tuttavia, la sessione TCP viene ancora gestita dal peer.**Per-client-embronic-max**: il numero massimo di connessioni embrionali simultanee consentite per client, compreso tra 0 e 65535. Il valore predefinito è 0, che consente connessioni illimitate.**Per-client-max**: il numero massimo di connessioni simultanee consentite per client, compreso tra 0 e 65535. Il valore predefinito è 0, che consente connessioni illimitate.

6. Per attivare la mappa dei criteri su una o più interfacce, immettere questo comando:

```
hostname(config)#service-policy policymap_name {global | interface interface_name}
```

Dove **global** applica la mappa dei criteri a tutte le interfacce e **interface** applica il criterio a un'interfaccia. È consentito un solo criterio globale. È possibile sostituire il criterio globale in un'interfaccia applicando un criterio del servizio a tale interfaccia. È possibile applicare una sola mappa dei criteri a ciascuna interfaccia.

Esempio:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Nota: per verificare il numero totale di sessioni half-open per un determinato host, utilizzare questo comando:

```
ASA-5510-8x# show local-host all

Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited

    UDP flow count/limit = 0/unlimited
```

Nota: la linea, `Conteggio embrioni TCP da ospitare`, visualizza il numero di sessioni half-open.

Protezione da attacchi di spoofing IP

Il PIX/ASA può bloccare gli attacchi spoof IP?

Spoofing IP

Per ottenere l'accesso, gli intrusi creano pacchetti con indirizzi IP di origine oggetto di spoofing. In questo modo si sfruttano le applicazioni che utilizzano l'autenticazione basata su indirizzi IP e determinano l'accesso non autorizzato degli utenti e, probabilmente, l'accesso alla directory principale sul sistema di destinazione. Gli esempi sono i servizi rsh e rlogin.

Èpossibile instradare i pacchetti attraverso i firewall del router di filtro se non sono configurati per filtrare i pacchetti in arrivo il cui indirizzo di origine si trova nel dominio locale. È importante notare che l'attacco descritto è possibile anche se nessun pacchetto di risposta può raggiungere l'aggressore.

Esempi di configurazioni potenzialmente vulnerabili sono:

- Firewall proxy in cui le applicazioni proxy utilizzano l'indirizzo IP di origine per l'autenticazione
- Router per reti esterne che supportano più interfacce interne
- Router con due interfacce che supportano la subnet nella rete interna

Riduzione

Il protocollo uRPF (Unicast Reverse Path Forwarding) impedisce lo spoofing IP (un pacchetto utilizza un indirizzo IP di origine errato per oscurare l'origine effettiva) garantendo che tutti i pacchetti abbiano un indirizzo IP di origine corrispondente all'interfaccia di origine corretta in base alla tabella di routing.

Normalmente, l'appliance di sicurezza controlla l'indirizzo di destinazione solo per stabilire a chi inoltrare il pacchetto. Unicast RPF indica all'appliance di sicurezza di controllare anche l'indirizzo

di origine. Per questo motivo viene denominato **inoltro percorso inverso**. Per tutto il traffico che si desidera consentire attraverso l'appliance di sicurezza, la tabella di routing dell'appliance di sicurezza deve includere un percorso di ritorno all'indirizzo di origine. Per ulteriori informazioni, vedere la RFC 2267 .

Nota: il `:- %PIX-1-106021:` Quando è abilitata la `verifica inversa del percorso, è` possibile visualizzare il messaggio di registro `Deny protocol reverse path check da src_addr a dest_addr sull'interfaccia int_name`. Per risolvere il problema, disabilitare il controllo del percorso inverso con il comando **no ip verify reverse path interface (nome interfaccia)**:

`no ip verify reverse-path interface (interface name)`

Per il traffico esterno, ad esempio, l'appliance di sicurezza può utilizzare il percorso predefinito per soddisfare la protezione RPF unicast. Se il traffico entra da un'interfaccia esterna e l'indirizzo di origine non è noto alla tabella di routing, l'appliance di sicurezza utilizza il percorso predefinito per identificare correttamente l'interfaccia esterna come interfaccia di origine.

Se il traffico entra nell'interfaccia esterna da un indirizzo noto alla tabella di routing ma associato all'interfaccia interna, l'appliance di sicurezza scarta il pacchetto. Analogamente, se il traffico entra nell'interfaccia interna da un indirizzo di origine sconosciuto, l'appliance di sicurezza scarta il pacchetto perché il percorso corrispondente (il percorso predefinito) indica l'interfaccia esterna.

La funzionalità RPF unicast è implementata come illustrato di seguito:

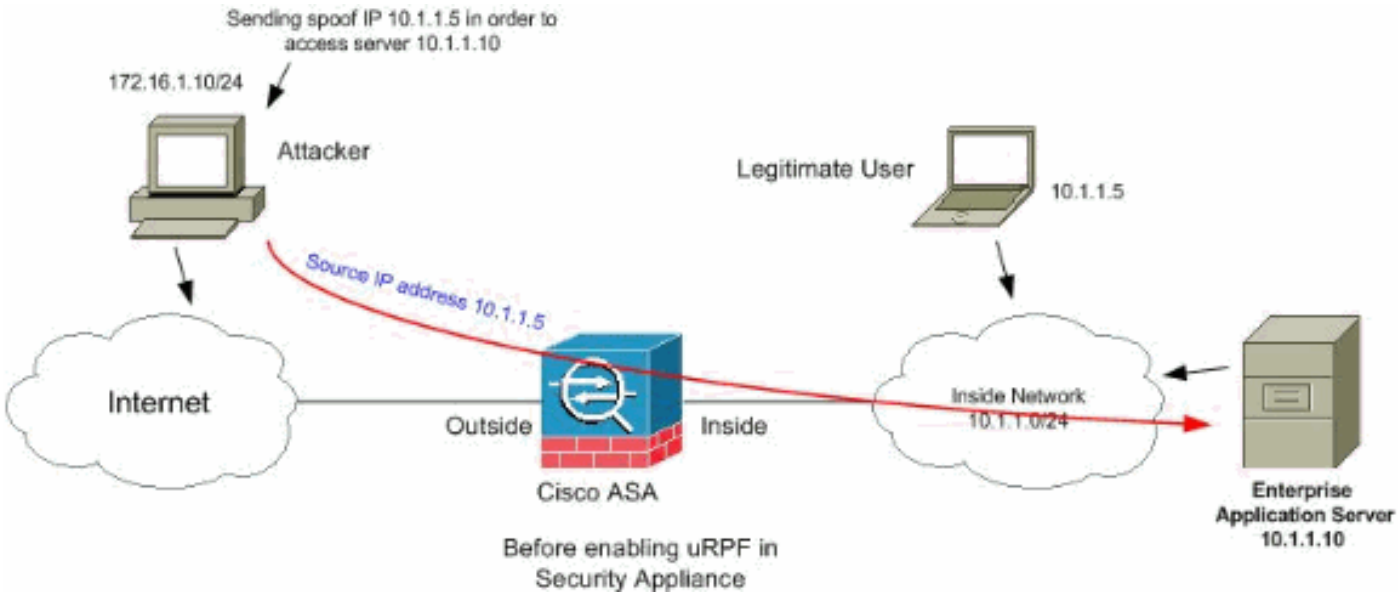
- Poiché i pacchetti ICMP non hanno sessioni, vengono controllati tutti.
- UDP e TCP hanno sessioni, quindi il pacchetto iniziale richiede una ricerca inversa del percorso. I pacchetti successivi che arrivano durante la sessione vengono controllati utilizzando uno stato esistente mantenuto come parte della sessione. I pacchetti non iniziali vengono controllati per assicurarsi che arrivino sulla stessa interfaccia usata dal pacchetto iniziale.

Per abilitare RPF unicast, immettere questo comando:

`hostname(config)#` **`ip verify reverse-path interface`** *`interface_name`*

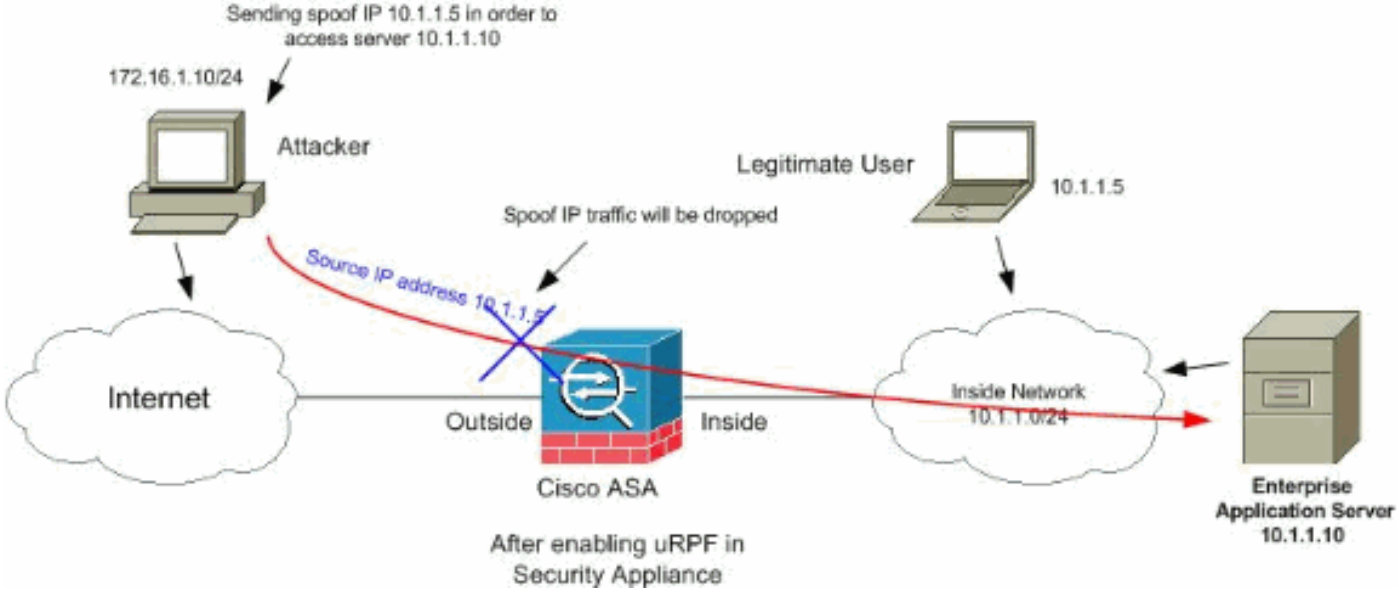
Esempio:

Come mostrato nella figura, l'Attacker PC genera una richiesta al server applicazioni 10.1.1.10 inviando un pacchetto con un indirizzo IP di origine contraffatto 10.1.1.5/24, e il server invia un pacchetto all'indirizzo IP reale 10.1.1.5/24 in risposta alla richiesta. Questo tipo di pacchetto non valido attacca sia il server applicazioni che l'utente legittimo nella rete interna.



RPF unicast può prevenire attacchi basati sullo spoofing degli indirizzi di origine. È necessario configurare l'uRPF nell'interfaccia esterna dell'ASA, come mostrato di seguito:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Identificazione con spoofing mediante messaggi syslog

L'appliance di sicurezza continua a ricevere messaggi di errore syslog come mostrato. Ciò indica potenziali attacchi che utilizzano pacchetti oggetto di spoofing o che potrebbero causare problemi di routing asimmetrico.

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

SpiegazioneQuesto è un messaggio relativo alla connessione. Questo messaggio viene visualizzato quando un tentativo di connessione a un indirizzo interno viene negato dai criteri di sicurezza definiti per il tipo di traffico specificato. I possibili valori *tcp_flags* corrispondono ai flag nell'intestazione TCP presenti quando la connessione è stata negata. Ad esempio, è

arrivato un pacchetto TCP per il quale non esiste alcuno stato di connessione nell'appliance di sicurezza e il pacchetto è stato scartato. I flag *tcp_flags* in questo pacchetto sono FIN e ACK.Di seguito sono riportati i *flag_tcp*:ACK - Numero di conferma ricevuto.FIN: i dati sono stati inviati.PSH - Il ricevitore ha passato i dati all'applicazione.RST - La connessione è stata reimpostata.SYN - I numeri di sequenza sono stati sincronizzati per avviare una connessione.URG - Il puntatore urgente è stato dichiarato valido.Il fallimento della conversione statica su PIX/ASA è dovuto a diversi motivi. Tuttavia, in genere il motivo è che l'interfaccia della zona demilitarizzata (DMZ) è configurata con lo stesso livello di sicurezza (0) dell'interfaccia esterna.Per risolvere il problema, assegnare un livello di sicurezza diverso a tutte le interfacceper ulteriori informazioni, fare riferimento a Configurazione dei parametri dell'interfaccia.Questo messaggio di errore viene visualizzato anche se una periferica esterna invia un pacchetto IDENT al client interno, che viene scartato dal firewall PIX. Per ulteriori informazioni, fare riferimento a Problemi di prestazioni PIX causati dal protocollo IDENT

2.
```
%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port
to inside_address/inside_port due to DNS {Response|Query}
```

SpiegazioneQuesto è un messaggio relativo alla connessione. Questo messaggio viene visualizzato se la connessione specificata non riesce a causa di un comando **deny in uscita**. La variabile protocol può essere ICMP, TCP o UDP.**Azione consigliata:** Utilizzare il comando **show outbound** per controllare gli elenchi in uscita.

3.
```
%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst
interface_name: IP_address (type dec, code dec)
```
SpiegazioneL'appliance di sicurezza ha negato l'accesso ai pacchetti ICMP in entrata. Per impostazione predefinita, a tutti i pacchetti ICMP viene negato l'accesso a meno che non sia esplicitamente autorizzato.

4.
```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```
SpiegazioneQuesto messaggio viene generato quando un pacchetto arriva all'interfaccia dell'appliance di sicurezza con indirizzo IP di destinazione 0.0.0.0 e indirizzo MAC di destinazione dell'interfaccia dell'appliance di sicurezza. Inoltre, questo messaggio viene generato quando l'accessorio di protezione rifiuta un pacchetto con indirizzo di origine non valido che può includere uno dei seguenti indirizzi o altri indirizzi non validi:Rete di loopback (127.0.0.0)Broadcast (limitato, diretto da rete, diretto da subnet e diretto da tutte le subnet)L'host di destinazione (land.c)Per migliorare ulteriormente il rilevamento dei pacchetti spoof, usare il comando **icmp** per configurare l'appliance di sicurezza in modo che ignori i pacchetti il cui indirizzo di origine appartiene alla rete interna. Il comando **access-list** è obsoleto e non è più garantito che funzioni correttamente.**Azione consigliata:** Determinare se un utente esterno sta tentando di compromettere la rete protetta. Verificare la presenza di client non configurati correttamente.

5.
```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```
SpiegazioneL'accessorio di sicurezza ha ricevuto un pacchetto con indirizzo IP di origine uguale alla destinazione IP e porta di destinazione uguale alla porta di origine. Questo messaggio indica un pacchetto oggetto di spoofing progettato per attaccare i sistemi. Questo

attacco è noto come attacco terrestre.**Azione consigliata:** Se il messaggio persiste, è possibile che sia in corso un attacco. Il pacchetto non fornisce informazioni sufficienti per determinare l'origine dell'attacco.

6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
SpiegazioneAttacco in corso. Qualcuno sta tentando di eseguire lo spoofing di un indirizzo IP su una connessione in ingresso. RPF unicast, noto anche come ricerca inversa del percorso, ha rilevato un pacchetto per il quale non è disponibile un indirizzo di origine rappresentato da un percorso e che presuppone che faccia parte di un attacco all'appliance di sicurezza.Questo messaggio viene visualizzato quando si attiva RPF unicast con il comando **ip verify reverse-path**. Questa funzione funziona sui pacchetti in ingresso a un'interfaccia. Se è configurato all'esterno, l'appliance di sicurezza controlla i pacchetti provenienti dall'esterno.L'accessorio di protezione cerca un percorso in base all'indirizzo di origine. Se non viene trovata una voce e non è definita una route, viene visualizzato questo messaggio di registro del sistema e la connessione viene interrotta.In caso di percorso, l'accessorio di sicurezza controlla a quale interfaccia corrisponde. Se il pacchetto è arrivato su un'altra interfaccia, si tratta di uno spoof o di un ambiente di routing asimmetrico che ha più percorsi per raggiungere una destinazione. L'appliance di sicurezza non supporta il routing asimmetrico.Se l'appliance di sicurezza è configurata su un'interfaccia interna, controlla le istruzioni di comando di **routing** statiche o RIP. Se l'indirizzo di origine non viene trovato, un utente interno sta effettuando lo spoofing del proprio indirizzo.**Azione consigliata:** Anche se è in corso un attacco, se questa funzione è abilitata, non è richiesta alcuna azione da parte dell'utente. L'appliance di sicurezza respinge l'attacco.**Nota:** il comando **show asp drop** mostra i pacchetti o le connessioni scartate dal percorso di sicurezza accelerato (asp), che potrebbe aiutare a risolvere un problema. Indica inoltre quando è stata cancellata l'ultima volta i contatori di rilascio asp. Usare il comando **show asp drop rpf-violated** in cui il contatore viene incrementato quando **ip verify-reverse-path** è configurato su un'interfaccia e l'appliance di sicurezza riceve un pacchetto il cui percorso di ricerca dell'IP di origine non ha restituito la stessa interfaccia su cui il pacchetto è stato ricevuto.
```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```
Nota: Raccomandazione: Tracciare l'origine del traffico in base all'IP di origine stampato nel messaggio di sistema successivo e individuare la causa dell'invio di traffico oggetto di spoofing.**Nota: Messaggi registro di sistema:** 106021

7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
SpiegazioneUn pacchetto corrispondente a una connessione arriva su un'interfaccia diversa da quella da cui è iniziata la connessione.Se ad esempio un utente avvia una connessione sull'interfaccia interna, ma l'accessorio di protezione rileva che la stessa connessione arriva su un'interfaccia perimetrale, l'accessorio di protezione dispone di più percorsi verso una destinazione. Questo processo è noto come routing asimmetrico e non è supportato dall'appliance di sicurezza.L'autore di un attacco potrebbe inoltre tentare di aggiungere pacchetti da una connessione all'altra per accedere all'appliance di sicurezza. In entrambi i casi, l'accessorio di protezione visualizza questo messaggio e interrompe la connessione.**Azione raccomandazione:** Questo messaggio viene visualizzato quando il comando **ip verify reverse-path** non è configurato. Verificare che il routing non sia asimmetrico.

8.
```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```
SpiegazionePacchetto IP negato dall'ACL. Questo messaggio viene visualizzato anche se l'opzione **log** non è abilitata per un ACL.**Azione raccomandazione:** Se i messaggi provenienti dallo stesso indirizzo di origine persistono, è possibile che vengano visualizzati messaggi che indicano un tentativo di stampa o di scansione della porta. Contattare gli amministratori dell'host remoto.
9.
```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```
10.
```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```
SpiegazioneQuesto messaggio del registro eventi di sistema indica che se si stabilisce una nuova connessione tramite il dispositivo firewall, verrà superato almeno uno dei limiti di connessione massimi configurati. Il messaggio del registro di sistema si applica sia ai limiti di connessione configurati utilizzando un comando statico sia a quelli configurati utilizzando Cisco Modular Policy Framework. La nuova connessione non sarà consentita attraverso il dispositivo firewall finché una delle connessioni esistenti non verrà disattivata, portando il numero di connessioni correnti al di sotto del numero massimo configurato.*cnt* - Numero di connessioni corrente*limit* - Limite di connessione configurato*dir* - Direzione del traffico in entrata o in uscita*sip*: indirizzo IP di origine*sport* - Porta di origine*dip*: indirizzo IP di destinazione*dport*: porta di destinazione*if_name* - Nome dell'interfaccia su cui viene ricevuta l'unità di traffico, principale o secondaria.**Azione raccomandazione:** Poiché i limiti delle connessioni sono configurati per una valida ragione, questo messaggio del registro eventi di sistema potrebbe indicare un possibile attacco DoS, nel qual caso l'origine del traffico potrebbe essere un indirizzo IP oggetto di spoofing. Se l'indirizzo IP di origine non è totalmente casuale, potrebbe essere utile identificarlo e bloccarlo utilizzando un elenco degli accessi. In altri casi, ottenere tracce di sniffer e analizzare l'origine del traffico aiuterebbe a isolare il traffico indesiderato dal traffico legittimo.

Funzione base di rilevamento minacce in ASA 8.x

Cisco Security Appliance ASA/PIX supporta la funzione di rilevamento delle minacce della versione software 8.0 e successive. Utilizzando il rilevamento delle minacce di base, l'appliance di sicurezza controlla la frequenza dei pacchetti ignorati e degli eventi di sicurezza per i seguenti motivi:

- Elenchi di rifiuto per accesso
- Formato di pacchetto non valido (ad esempio intestazione-ip-non valida o lunghezza-hdr-tcp-non valida)
- Limiti di connessione superati (limiti di risorse a livello di sistema e limiti impostati nella configurazione)
- Rilevato attacco DoS (ad esempio un SPI non valido, errore di controllo del firewall con stato)
- Controlli di base del firewall non riusciti (questa opzione indica una velocità combinata che include tutte le perdite di pacchetti correlate al firewall in questo elenco puntato. Non sono

incluse le perdite non correlate al firewall, ad esempio il sovraccarico dell'interfaccia, i pacchetti non riusciti durante l'ispezione delle applicazioni e gli attacchi di scansione rilevati.)
- Rilevati pacchetti ICMP sospetti
- Ispezione dei pacchetti non riuscita
- Overload dell'interfaccia
- Rilevato attacco di scansione (questa opzione controlla gli attacchi di scansione; ad esempio, il primo pacchetto TCP non è un pacchetto SYN oppure la connessione TCP non è riuscita a eseguire l'handshake a 3 vie. Il rilevamento completo delle minacce di scansione (per ulteriori informazioni, fare riferimento a Configurazione del rilevamento delle minacce di scansione) prende queste informazioni sulla frequenza di attacco di scansione e le agisce classificando gli host come attaccanti ed eseguendone automaticamente lo shun, ad esempio).
- Rilevamento di sessioni incompleto, ad esempio un attacco SYN TCP, o nessun attacco di sessione UDP di dati rilevato.

Quando l'appliance di sicurezza rileva una minaccia, invia immediatamente un messaggio di registro del sistema (730100).

Il rilevamento delle minacce di base influisce sulle prestazioni solo in caso di cadute o minacce potenziali. Anche in questo scenario, l'impatto sulle prestazioni è insignificante.

il comando **show threat-detection rate** viene usato per identificare gli attacchi potenziali quando si è collegati all'appliance di sicurezza.

```
ciscoasa#show threat-detection rate
                        Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                0               0       0                16
  1-hour ACL  drop:                0               0       0               112
  1-hour SYN attck:                5               0       2             21438
  10-min  Scanning:                0               0      29               193
  1-hour  Scanning:              106               0      10            384776
  1-hour Bad  pkts:               76               0       2            274690
  10-min  Firewall:                0               0       3                22
  1-hour  Firewall:               76               0       2            274844
  10-min DoS attck:                0               0       0                 6
  1-hour DoS attck:                0               0       0                42
  10-min Interface:                0               0       0               204
  1-hour Interface:               88               0       0            318225
```

Per ulteriori informazioni sulla parte di configurazione, consultare la sezione Configurazione del rilevamento delle minacce di base della guida alla configurazione di ASA 8.0.

Messaggio Syslog 73100

Messaggio di errore:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
```

L'oggetto specificato nel messaggio del registro eventi di sistema ha superato la soglia di frammentazione o la soglia media specificata. L'oggetto può essere un'attività di drop di un host, di una porta TCP/UDP, di un protocollo IP o di vari drop a causa di potenziali attacchi. Indica che il sistema è sotto potenziale attacco.

Nota: questi messaggi di errore con risoluzione sono applicabili solo ad ASA 8.0 e versioni successive.

1. Oggetto: l'origine generale o particolare di un conteggio della velocità di rilascio, che può includere quanto segue:FirewallPkt non validiLimite di velocitàAttacco DoSEliminazione ACLLimite connattacco ICMPScansioneattacco SYNIspezionareInterfaccia
2. rate_ID - La velocità configurata da superare. La maggior parte degli oggetti può essere configurata con un massimo di tre diverse frequenze per intervalli diversi.
3. rate_val - Valore di tasso specifico.
4. total_cnt - Numero totale dalla creazione o cancellazione dell'oggetto.

Nei tre esempi seguenti viene illustrata la modalità di esecuzione delle variabili:

- In caso di interruzione dell'interfaccia a causa di un limite della CPU o del bus:
```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
    second,
max configured rate is 8000; Current average rate is 2030 per second,
max configured rate is 2000; Cumulative total count is 3930654
```
- Per una perdita di scansione dovuta a potenziali attacchi:
```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
    second_
max configured rate is 10; Current average rate is 245 per second_
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```
- Per i pacchetti danneggiati a causa di potenziali attacchi:
```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

Azione consigliata:

Eseguire la procedura seguente in base al tipo di oggetto specificato visualizzato nel messaggio:

1. Se l'oggetto nel messaggio syslog è uno dei seguenti:FirewallPkt non validiLimite di velocitàAttacco DoSEliminazione ACLLimite connattacco ICMPScansioneattacco SYNIspezionareInterfacciaVerificare se la velocità di rilascio è accettabile per l'ambiente in esecuzione.
2. Regolare la soglia di una determinata perdita su un valore appropriato eseguendo il comando **threat-detection rate *xxx*** dove *xxx* è uno dei seguenti:acl-dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropminaccia di scansionesyn-attack
3. Se l'oggetto nel messaggio syslog è una porta TCP o UDP, un protocollo IP o un host drop, verificare se la velocità di drop è accettabile per l'ambiente in esecuzione.
4. Regolare la velocità di soglia di una determinata perdita su un valore appropriato eseguendo il comando **threat-detection rate bad-packet-drop**. Per ulteriori informazioni, consultare la sezione Configurazione della funzione di rilevamento delle minacce di base della guida alla configurazione di ASA 8.0.

Nota: se non si desidera che venga visualizzato il messaggio di avviso relativo al superamento della velocità di rilascio, è possibile disabilitarlo eseguendo il comando **no threat-detection basic-threat**.

Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance - Pagina di supporto
- Cisco serie 500 PIX Support Page
- Difese dagli attacchi flooding TCP SYN
- Bollettino sulla mitigazione applicata da Cisco: Identificazione e mitigazione dello sfruttamento delle vulnerabilità di Denial of Service nel modulo di switching del contenuto
- Bollettino sulla mitigazione applicata da Cisco: Identificazione e mitigazione dello sfruttamento delle molteplici vulnerabilità in Cisco PIX e ASA Appliance e Firewall Services Module
- Spoofing IP
- Documentazione e supporto tecnico – Cisco Systems