ASA 8.2: Flusso di pacchetti attraverso un firewall ASA

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Cisco ASA Packet Process Algorithm](#)
[Spiegazione di NAT](#)
[Comandi show](#)
[Messaggi syslog](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive il flusso di pacchetti attraverso un firewall di Cisco Adaptive Security Appliance (ASA). Indica la procedura Cisco ASA per elaborare i pacchetti interni. Descrive inoltre le diverse possibilità in cui il pacchetto potrebbe essere scartato e le diverse situazioni in cui il pacchetto avanza.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle appliance ASA Cisco serie 5500.

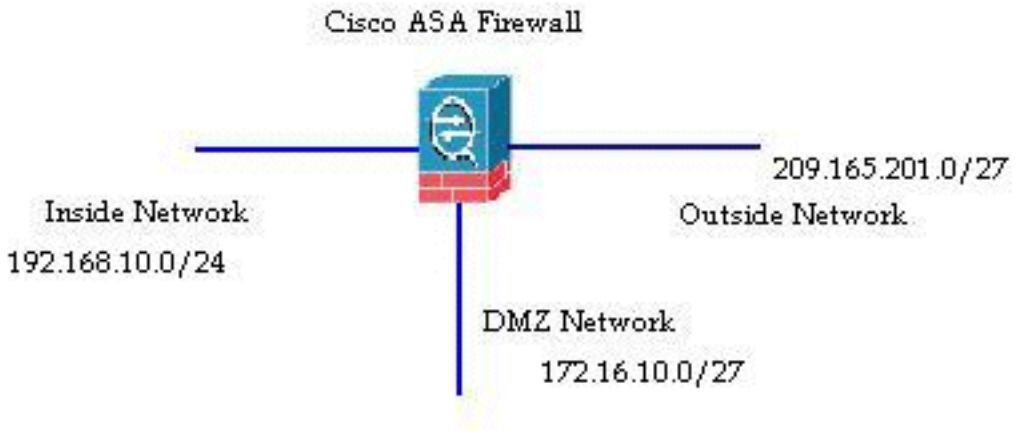
Componenti usati

Per la stesura del documento, sono state usate appliance Cisco ASA serie 5500 ASA con software versione 8.2.

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.

Premesse

L'interfaccia che riceve il pacchetto è chiamata interfaccia **in entrata** e l'interfaccia attraverso cui il pacchetto esce è chiamata interfaccia **in uscita**. Quando si fa riferimento al flusso di pacchetto attraverso un dispositivo, l'operazione è facilmente semplificata se si guarda al flusso in termini di queste due interfacce. Di seguito è riportato uno scenario di esempio:



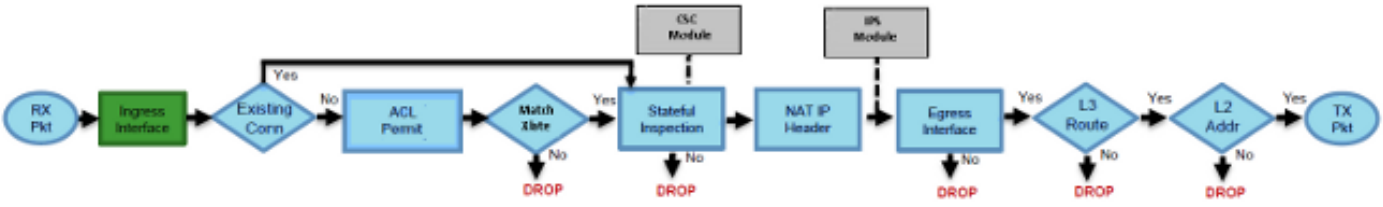
Quando un utente interno (192.168.10.5) tenta di accedere a un server Web nella rete delle zone demilitarizzate (DMZ) (172.16.10.5), il flusso del pacchetto ha il seguente aspetto:

- Source address - 192.168.10.5
- Porta di origine - 22966
- Indirizzo di destinazione - 172.16.10.5
- Porta di destinazione - 8080
- Interfaccia in ingresso - Interna
- Interfaccia in uscita - DMZ
- Protocollo utilizzato - TCP (Transmission Control Protocol)

Dopo aver determinato i dettagli del flusso di pacchetto come descritto qui, è facile isolare il problema a questa voce di connessione specifica.

Cisco ASA Packet Process Algorithm

Di seguito è riportato un diagramma del modo in cui Cisco ASA elabora il pacchetto che riceve:



Di seguito sono riportati in dettaglio i singoli passaggi:

1. Il pacchetto viene raggiunto dall'interfaccia in entrata.
2. Quando il pacchetto raggiunge il buffer interno dell'interfaccia, il contatore di input

dell'interfaccia viene incrementato di un'unità.

3. Cisco ASA esamina innanzitutto i dettagli della tabella delle connessioni interne per verificare se si tratta di una connessione corrente. Se il flusso del pacchetto corrisponde a una connessione corrente, il controllo Access Control List (ACL) viene ignorato e il pacchetto viene spostato in avanti.Se il flusso del pacchetto non corrisponde a una connessione corrente, lo stato TCP viene verificato. Se si tratta di un pacchetto SYN o UDP (User Datagram Protocol), il contatore di connessione viene incrementato di un'unità e il pacchetto viene inviato per un controllo ACL. Se non è un pacchetto SYN, il pacchetto viene scartato e l'evento registrato.
4. Il pacchetto viene elaborato come da ACL di interfaccia. Viene verificato in ordine sequenziale tra le voci dell'elenco e, se corrisponde a una delle voci dell'elenco, si sposta in avanti. In caso contrario, il pacchetto viene scartato e le informazioni vengono registrate. Il numero di accessi all'ACL viene incrementato di un'unità quando il pacchetto corrisponde alla voce ACL.
5. Il pacchetto viene verificato per le regole di conversione. Se un pacchetto passa attraverso questo controllo, viene creata una voce di connessione per questo flusso e il pacchetto si sposta in avanti. In caso contrario, il pacchetto viene scartato e le informazioni vengono registrate.
6. Il pacchetto è sottoposto a un controllo. Questa ispezione verifica se il flusso di pacchetto specifico è conforme al protocollo. Cisco ASA dispone di un motore di ispezione integrato che controlla ciascuna connessione secondo la serie predefinita di funzionalità a livello di applicazione. Se ha superato l'ispezione, viene spostato in avanti. In caso contrario, il pacchetto viene scartato e le informazioni vengono registrate.Se è coinvolto un modulo CSC (Content Security), verranno implementati ulteriori controlli di sicurezza.
7. Le informazioni dell'intestazione IP vengono tradotte in base alla regola NAT/PAT (Network Address Translation/Port Address Translation) e i checksum vengono aggiornati di conseguenza. Il pacchetto viene inoltrato al modulo Advanced Inspection and Prevention Security Services Module (AIP-SSM) per i controlli di sicurezza correlati a IPS quando è coinvolto il modulo AIP.
8. Il pacchetto viene inoltrato all'interfaccia in uscita in base alle regole di conversione. Se nella regola di conversione non viene specificata alcuna interfaccia in uscita, l'interfaccia di destinazione viene decisa in base alla ricerca globale della route.
9. Sull'interfaccia di uscita viene eseguita la ricerca della route di interfaccia. L'interfaccia di uscita è determinata dalla regola di conversione che ha la priorità.
10. Dopo aver trovato un percorso di layer 3 e aver identificato l'hop successivo, viene eseguita la risoluzione di layer 2. La riscrittura di layer 2 dell'intestazione MAC si verifica in questa fase.
11. Il pacchetto viene trasmesso su filo e i contatori di interfaccia si incrementano sull'interfaccia in uscita.

Spiegazione di NAT

Fare riferimento a questi documenti per ulteriori dettagli sull'ordine del funzionamento NAT:

- Software Cisco ASA versione 8.2 e precedenti
- Software Cisco ASA versione 8.3 e successive

Comandi show

Di seguito sono elencati alcuni comandi utili per tenere traccia dei dettagli del flusso di pacchetto nelle diverse fasi del processo:

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

Messaggi syslog

I messaggi Syslog forniscono informazioni utili sull'elaborazione dei pacchetti. Di seguito sono riportati alcuni messaggi syslog di esempio da utilizzare come riferimento:

- Messaggio syslog in assenza di voce di connessione:
  `%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Messaggio syslog quando il pacchetto viene rifiutato da un ACL:
  `%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Messaggio syslog quando non viene trovata alcuna regola di conversione:
  `%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Messaggio syslog quando un pacchetto viene rifiutato da Ispezione sicurezza:
  `%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Messaggio syslog in assenza di informazioni sulla route:
  `%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port`

Per un elenco completo di tutti i messaggi syslog generati da Cisco ASA e una breve spiegazione, consultare i messaggi syslog della serie Cisco ASA.

Informazioni correlate

- Pagina di supporto per Cisco ASA
- Cisco ASA serie 5500 Command Reference, 8.2
- Guida alla configurazione di Cisco ASA serie 5500, 8.3
- Documentazione e supporto tecnico – Cisco Systems