Uso della guida per proteggere il firewall ASA

Sommario

Introduzione

Questo documento descrive le informazioni per proteggere i dispositivi Cisco ASA e aumentare la sicurezza complessiva della rete.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Active Security Appliance (ASA) 9.16(1) e versioni 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.

Premesse

Questo documento è strutturato in 4 sezioni.

1. Protezione avanzata del piano di gestione: si applica a tutte le funzionalità di gestione e al traffico di sistema correlate all'appliance ASA, ad esempio SNMP, SSH e così via.

2. Proteggere config: comandi tramite i quali è possibile interrompere il popolamento delle password e così via per la configurazione in esecuzione e così via.
3. Log and Monitoring (Registrazione e monitoraggio): questa opzione viene applicata a tutte le impostazioni relative all'accesso all'ASA.
4. Traffico attraverso: questo problema si verifica quando il traffico attraversa l'appliance ASA.

La descrizione delle funzionalità di sicurezza in questo documento spesso fornisce informazioni sufficienti per configurare la funzionalità. Tuttavia, in caso contrario, la feature viene spiegata in modo che sia possibile valutare se è necessaria una maggiore attenzione alla feature stessa. Ove possibile e opportuno, questo documento contiene raccomandazioni che, se implementate, contribuiscono a proteggere una rete.

Prodotti correlati

Questa configurazione può essere utilizzata anche con il software Cisco ASA versione 9.1x.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Operazioni sicure

La sicurezza delle operazioni di rete è un argomento fondamentale. Anche se la maggior parte di questo documento è dedicata alla configurazione sicura di un dispositivo Cisco ASA, le sole configurazioni non proteggono completamente una rete. Le procedure operative in uso sulla rete contribuiscono alla sicurezza tanto quanto la configurazione dei dispositivi sottostanti.

Questi argomenti contengono suggerimenti operativi che è consigliabile implementare. Questi argomenti evidenziano aree critiche specifiche delle operazioni di rete e non sono completi.

Monitoraggio dei consigli e delle risposte sulla sicurezza Cisco

Il Cisco Product Security Incident Response Team (PSIRT) crea e gestisce pubblicazioni, comunemente note come consigli PSIRT, per problemi relativi alla sicurezza dei prodotti Cisco. Il metodo utilizzato per la comunicazione di problemi meno gravi è Cisco Security Response. Gli avvisi e le risposte sulla sicurezza sono disponibili sul sito PSIRT.

Ulteriori informazioni su questi veicoli di comunicazione sono disponibili in Cisco Security Vulnerability Policy.

Per mantenere una rete sicura, è necessario conoscere le avvertenze e le risposte sulla sicurezza Cisco rilasciate. È necessario essere a conoscenza di una vulnerabilità prima di poter valutare la minaccia che può rappresentare per una rete. Per assistenza nel processo di valutazione, fare riferimento a Valutazione dei rischi per la vulnerabilità della sicurezza.

Utilizzo di autenticazione, autorizzazione e accounting

Il framework AAA (Authentication, Authorization, and Accounting) è essenziale per proteggere i dispositivi di rete. La struttura AAA fornisce l'autenticazione delle sessioni di gestione e può inoltre limitare gli utenti a comandi specifici definiti dall'amministratore e registrare tutti i comandi immessi da tutti gli utenti. Per ulteriori informazioni su come usare il protocollo AAA, vedere la sezione Autenticazione, autorizzazione e accounting di questo documento.

Raccolta e monitoraggio centralizzati dei log

Per conoscere gli eventi esistenti, emergenti e storici relativi agli incidenti di sicurezza, l'organizzazione deve disporre di una strategia unificata per la registrazione e la correlazione degli eventi. Questa strategia deve sfruttare la registrazione da tutti i dispositivi di rete e utilizzare funzionalità di correlazione preconfigurate e personalizzabili.

Dopo l'implementazione della registrazione centralizzata, è necessario sviluppare un approccio strutturato per l'analisi dei registri e il monitoraggio degli incidenti. In base alle esigenze dell'organizzazione, questo approccio può variare da una semplice analisi diligente dei dati di registro ad un'analisi avanzata basata su regole.

Usa protocolli sicuri quando possibile

Molti protocolli vengono utilizzati per trasportare dati sensibili relativi alla gestione della rete. Ove possibile, è necessario utilizzare protocolli di protezione. Un protocollo sicuro include l'uso del protocollo SSH anziché Telnet, in modo che i dati di autenticazione e le informazioni di gestione vengano crittografati. Inoltre, quando si copiano i dati di configurazione, è necessario utilizzare protocolli di trasferimento file sicuri. Un esempio è l'uso del protocollo SCP (Secure Copy Protocol) al posto del protocollo FTP o TFTP.

Maggiore visibilità del traffico con NetFlow

NetFlow consente di monitorare i flussi di traffico nella rete. Originariamente progettato per esportare informazioni sul traffico in applicazioni di gestione di rete, NetFlow può essere usato anche per mostrare le informazioni sul flusso su un router. Questa funzionalità consente di visualizzare in tempo reale il traffico che attraversa la rete. Indipendentemente dal fatto che le informazioni di flusso vengano esportate in un raccoglitore remoto, è consigliabile configurare i dispositivi di rete per NetFlow in modo che possano essere utilizzati in modo reattivo, se necessario.

Gestione della configurazione

La gestione della configurazione è un processo mediante il quale vengono proposte, esaminate, approvate e distribuite le modifiche alla configurazione. Nel contesto di una configurazione di dispositivo Cisco ASA, altri due aspetti della gestione della configurazione sono critici: archiviazione della configurazione e sicurezza.

È possibile utilizzare gli archivi di configurazione per eseguire il rollback delle modifiche apportate

ai dispositivi di rete. In un contesto di protezione, è possibile utilizzare gli archivi di configurazione anche per determinare quali modifiche alla protezione sono state apportate e quando sono state apportate. Insieme ai dati di registro AAA, queste informazioni possono essere utili per il controllo della sicurezza dei dispositivi di rete.

La configurazione di un dispositivo Cisco ASA contiene molti dettagli riservati. Nomi utente, password e contenuto degli elenchi di controllo di accesso sono esempi di questo tipo di informazioni. Il repository usato per archiviare le configurazioni dei dispositivi Cisco ASA deve essere protetto. Un accesso non sicuro a queste informazioni può compromettere la sicurezza dell'intera rete.

Piano di gestione

Il piano di gestione è costituito da funzioni che consentono di raggiungere gli obiettivi di gestione della rete. Ciò include sessioni di gestione interattive che usano SSH, nonché la raccolta di statistiche con SNMP o NetFlow. Se si considera la sicurezza di un dispositivo di rete, è fondamentale proteggere il piano di gestione. Se un problema di sicurezza può compromettere le funzioni del piano di gestione, potrebbe essere impossibile ripristinare o stabilizzare la rete.

Piano di gestione della protezione avanzata

Il piano di gestione viene utilizzato per accedere, configurare e gestire un dispositivo, nonché per monitorarne le operazioni e la rete in cui viene distribuito. Il piano di gestione è il piano che riceve e invia traffico per le operazioni di queste funzioni. Questo elenco di protocolli viene utilizzato dal management plane:

- Simple Network Management Protocol
- Protocollo Secure Shell
- Protocollo di trasferimento file
- Protocollo Trivial File Transfer
- Secure Copy Protocol
- TACACS+
- RAGGIO
- NetFlow
- Protocollo orario di rete
- Syslog
- ICMP
- PMI

Nota: l'attivazione di TELNET non è consigliata in quanto si tratta di testo normale.

Gestione password

Le password controllano l'accesso alle risorse o ai dispositivi. A tale scopo, è necessario definire una password o un segreto utilizzato per autenticare le richieste. Quando si riceve una richiesta di

accesso a una risorsa o a un dispositivo, la richiesta viene contestata per la verifica della password e dell'identità e l'accesso può essere concesso, negato o limitato in base al risultato. Come buona norma per la sicurezza, le password devono essere gestite con un server di autenticazione TACACS+ o RADIUS. Tuttavia, si noti che, in caso di errore dei servizi TACACS+ o RADIUS, è ancora necessaria una password configurata localmente per l'accesso privilegiato. Un dispositivo può inoltre includere altre informazioni sulla password nella propria configurazione, ad esempio una chiave NTP, una stringa della community SNMP o una chiave del protocollo di routing.

ASA 9.7(1) ha introdotto l'hashing PBKDF2 per le password locali. Il nome utente locale e le password enable di tutte le lunghezze vengono memorizzati nella configurazione utilizzando un hash PBKDF2 (Password-Based Key Derivation Function 2). In precedenza, le password composte da almeno 32 caratteri utilizzavano il metodo di hashing basato su MD5. Le password già esistenti continuano a utilizzare l'hash basato su MD5 a meno che non venga immessa una nuova password. Per le linee guida per il downgrade, vedere il capitolo Software and Configurations nella Guida generale alla configurazione delle operazioni.

Abilita servizio HTTP

Per utilizzare ASDM, è necessario abilitare il server HTTPS e consentire le connessioni HTTPS all'appliance ASA. L'appliance di sicurezza consente un massimo di 5 istanze ASDM simultanee per contesto, se disponibili, con un massimo di 32 istanze ASDM tra tutti i contesti. Per configurare l'accesso ASDM, utilizzare:

```
http server enable <port>
```

Selezionare solo gli indirizzi IP da includere nell'elenco degli ACL. Consentire un accesso ampio non è una buona pratica.

```
http 0.0.0.0 0.0.0.0 <interface>
```

Configura controllo di accesso ASDM:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

```
// Set server version
ASA(config)# ssl server-version tlsv1 tlsv1.1 tlsv.1.2

// Set client version
```

```
ASA(config) # ssl client-version tlsv1 tlsv1.1 tlsv.1.2
```

Sull'appliance ASA, questi cifrari sono abilitati nell'ordine mostrato per impostazione predefinita.

```
ciscoasa(config)# ssl cipher ?

configure mode commands/options:
  default   Specify the set of ciphers for outbound connections
  dtlsv1    Specify the ciphers for DTLSv1 inbound connections
  dtlsv1.2  Specify the ciphers for DTLSv1.2 inbound connections
  tlsv1     Specify the ciphers for TLSv1 inbound connections
  tlsv1.1   Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2   Specify the ciphers for TLSv1.2 inbound connections
ciscoasa(config)# ssl cipher dtlsv1 ?

configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration string.
```

Il valore predefinito è igh.

- La parola chiave all specifica l'utilizzo di tutti i cifrari: hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- La parola chiave custom specifica una stringa di configurazione cifratura personalizzata, separata da due punti.
- La parola chiave fips specifica solo cifrari conformi a FIPS: hmac-sha1 hmac-sha2-256
- La parola chiave high specifica solo i cifrari ad alta resistenza (impostazione predefinita): hmac-sha2-256
- La parola chiave low specifica i cifrari a bassa, media e alta resistenza: hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- La parola chiave medium specifica i cifrari a media e alta resistenza: hmac-sha1 hmac-sha1-96hmac-sha2-256

Per impostazione predefinita, l'appliance ASA usa un certificato autofirmato temporaneo che cambia a ogni riavvio. Se si sta cercando un singolo certificato, è possibile utilizzare questo collegamento per generare un certificato autofirmato permanente.

ASA supporta TLS versione 1.2 per la trasmissione sicura dei messaggi per ASDM, VPN senza client e VPN AnyConnect. Questi comandi sono stati introdotti o modificati: ssl client-version, ssl

server-version, ssl cipher, ssl trust-point, ssl dh-group, show ssl, show ssl cipher, show vpn-sessiondb.

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
```

```
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

Abilitazione SSH

L'ASA consente le connessioni SSH all'appliance ASA a scopo di gestione. L'ASA consente un massimo di 5 connessioni SSH simultanee per contesto, se disponibili, con un massimo di 100 connessioni divise tra tutti i contesti.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

Il tipo di coppia di chiavi predefinito è General Key. La dimensione predefinita del modulo è 1024. La quantità di spazio della NVRAM per archiviare le coppie di chiavi varia in base alla piattaforma ASA. È possibile raggiungere un limite se si generano più di 30 coppie di chiavi.

Per rimuovere le coppie di chiavi del tipo indicato (rsa o dsa):

```
crypto key zeroize { rsa | eddsa | ecdsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

Configurare SSH per l'accesso remoto ai dispositivi:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Per scambiare le chiavi con il metodo di scambio chiavi Diffie-Hellman (DH) Group 1, DH Group 14 o Curve25519, usare il comando ssh key-exchange in modalità di configurazione globale, a partire da 9.1(2). ASA supporta dh-group14-sha1 per SSH.

```
ASA(config)#ssh key-exchange group dh-group14-sha256
```

Configura timeout per sessioni di accesso

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

Gestione password

Le password controllano l'accesso alle risorse o ai dispositivi. A tale scopo, è necessario definire una password o un segreto utilizzato per autenticare le richieste. Quando si riceve una richiesta di accesso a una risorsa o a un dispositivo, la richiesta viene contestata per la verifica della password e dell'identità e l'accesso può essere concesso, negato o limitato in base al risultato. Come buona norma per la sicurezza, le password devono essere gestite con un server di autenticazione TACACS+ o RADIUS. Tuttavia, si noti che, in caso di errore dei servizi TACACS+ o RADIUS, è ancora necessaria una password configurata localmente per l'accesso privilegiato. Un dispositivo può inoltre includere altre informazioni sulla password nella propria configurazione, ad esempio una chiave NTP, una stringa della community SNMP o una chiave del protocollo di routing.

Configura utente locale e password crittografata

```
username <local_username> password <local_password> encrypted
```

Configura abilitazione password

```
enable password <enable_password> encrypted
```

Configurazione dell'autenticazione AAA per la modalità di abilitazione

```
ASA(config)#aaa authentication enable console LOCAL
```

Autenticazione, autorizzazione e accounting

Il framework AAA (Authentication, Authorization, and Accounting) è fondamentale per proteggere l'accesso interattivo ai dispositivi di rete. La struttura AAA fornisce un ambiente altamente configurabile che può essere personalizzato in base alle esigenze della rete.

Autenticazione TACACS+

TACACS+ è un protocollo di autenticazione che l'ASA può utilizzare per autenticare gli utenti di gestione su un server AAA remoto. Questi utenti possono accedere al dispositivo ASA tramite SSH, HTTPS, telnet o HTTP.

L'autenticazione TACACS+, o più in generale l'autenticazione AAA, consente di usare i singoli account utente per ciascun amministratore di rete. Quando non si dipende da una singola password condivisa, la sicurezza della rete è migliorata e la responsabilità è rafforzata.

RADIUS è un protocollo simile a TACACS+; tuttavia, cripta solo la password inviata attraverso la rete. Al contrario, TACACS+ cripta l'intero payload TCP, che include sia il nome utente che la password. Per questo motivo, TACACS+ può essere usato al posto di RADIUS quando TACACS+ è supportato dal server AAA. Per un confronto più dettagliato dei due protocolli, fare riferimento a TACACS+ e RADIUS Comparison.

L'autenticazione TACACS+ può essere abilitata su un dispositivo Cisco ASA con una configurazione simile a quella dell'esempio seguente:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

Firma e verifica dell'immagine ASA

A partire dalla versione software 9.3.1, le immagini ASA sono ora firmate con una firma digitale. La firma digitale viene verificata dopo l'avvio dell'ASA.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Embedded Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
Computed Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
CCO Hash      SHA-512: 1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
Signature Verified


ASA(config)# verify /signature running
Requesting verify signature of the running image...

Starting image verification
Hash Computation:    100% Done!
Computed Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c


Get key records from key storage: PrimaryASA, key_store_type: 6
Embedded Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c

Returned. rc: 0, status: 1
The digital signature of the running image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
 Signer Information
 Common Name : abraxas
 Organization Unit : ASAv
 Organization Name : CiscoSystems
 Certificate Serial Number : 550DBBD5
 Hash Algorithm : SHA2 512
 Signature Algorithm : 2048-bit RSA
 Key Version : A
```

Configura fuso orario

```
clock timezone GMT <hours offset>
```

Configurazione NTP

Il Network Time Protocol (NTP) non è un servizio particolarmente pericoloso, ma qualsiasi servizio non necessario può rappresentare un vettore di attacco. Se si utilizza NTP, è importante configurare in modo esplicito un'origine ora attendibile e utilizzare l'autenticazione corretta. Per gli scopi del syslog, ad esempio durante le indagini forensi su potenziali attacchi, nonché per una connettività VPN efficace quando si dipende dai certificati per l'autenticazione di fase 1, è

necessario disporre di tempo accurato e affidabile.

- Fuso orario NTP: quando si configura il protocollo NTP, è necessario configurare il fuso orario in modo che i timestamp possano essere correlati correttamente. Di solito ci sono due approcci per configurare il fuso orario per i dispositivi in una rete con una presenza globale. Un metodo consiste nel configurare tutti i dispositivi di rete con l'ora UTC (Coordinated Universal Time), in precedenza denominata GMT (Greenwich Mean Time). L'altro approccio consiste nel configurare i dispositivi di rete con il fuso orario locale. ntp server indirizzo_ip [id_chiave] [nome_interfaccia_origine] [preferisci]
- Autenticazione NTP: se si configura l'autenticazione NTP, questa assicura che i messaggi NTP vengano scambiati tra peer NTP attendibili. Abilita l'autenticazione tramite il comando ntp authentication, imposta l'ID della chiave trusted per il server. Se si abilita l'autenticazione, l'ASA comunica con un server NTP solo se usa la chiave attendibile corretta nei pacchetti. Per abilitare l'autenticazione con un server NTP, utilizzare il comando ntp authentication in modalità di configurazione globale.

```
ASA(config)#ntp authenticate
```

Servizio server DHCP (se non in uso)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Nota: l'ASA non supporta il CDP.

Control-Plane Access-list

Le regole di controllo d'accesso per il traffico di gestione diretto (definito da comandi come http, ssh o telnet) hanno la precedenza su un elenco degli accessi applicato con l'opzione control-plane. Pertanto, il traffico di gestione autorizzato può entrare anche se esplicitamente negato dall'elenco degli accessi diretto.

```
access-list <name> in interface <Interface_name> control-plane
```

Da ASA

Di seguito sono elencati i protocolli che possono essere utilizzati per copiare/trasferire i file sull'appliance ASA.

Testo non crittografato:

- FTP
- HTTP
- TFTP
- PMI

Sicuro:

- HTTPS
- Secure Copy Client (SCP) ASA supporta il client SCP per il trasferimento di file da e verso un server SCP.

Per il traffico in transito

Numero di sequenza TCP

Ogni connessione TCP dispone di due ISDN: uno generato dal client e uno generato dal server. L'ASA rende casuale l'ISN della rete TCP SYN, passando in entrambe le direzioni, in entrata e in uscita.

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

Se necessario, è possibile disabilitare l'assegnazione casuale dei numeri di sequenza iniziali TCP. Ad esempio:

- Se anche un altro firewall in linea sta utilizzando a caso i numeri di sequenza iniziali, non è necessario che entrambi eseguano questa azione, anche se questa azione non influisce sul traffico.
- Se si usa il multi-hop eBGP tramite l'ASA e i peer eBGP usano MD5. La casualizzazione interrompe il checksum MD5.
- Se si usa un dispositivo WAAS che richiede all'appliance ASA di non casualizzare i numeri di sequenza delle connessioni.

Decremento TTL

per impostazione predefinita, non diminuisce il valore TTL nell'intestazione IP, per cui l'ASA non viene visualizzata come hop del router quando si esegue il comando traceroute.

dnsguard

Impone una risposta DNS per query. Può essere abilitato usando il comando in modalità di configurazione globale.

```
ASA(config)#dns-guard
```

Configurazione dei controlli di frammentazione della catena di frammenti

Per gestire ulteriormente la frammentazione dei pacchetti e migliorare la compatibilità con NFS, usare il comando fragment in modalità di configurazione globale.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Configura ispezione protocollo

I motori di ispezione sono necessari per i servizi che incorporano le informazioni sull'indirizzo IP nel pacchetto dati utente o che aprono i canali secondari sulle porte assegnate dinamicamente. Questi protocolli richiedono che l'ASA esegua un'ispezione approfondita del pacchetto anziché passarlo sul percorso rapido. Di conseguenza, i motori di ispezione possono influire sul throughput complessivo. Per informazioni dettagliate sull'ispezione del protocollo a livello di applicazione, consultare la guida alla configurazione di ASA 9.4.

Il controllo sull'appliance ASA può essere abilitato con questo comando.

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

Per impostazione predefinita, ASA ha global_policy abilitato a livello globale.

Configura inoltro percorso inverso unicast

```
ip verify reverse-path interface <interface_name>
```

Quando il traffico viene interrotto a causa di un controllo RPF, viene visualizzato un contatore di rilascio asp sugli incrementi ASA.

<#root>

```
ASA(config)# show asp drop

Frame drop:
  Invalid TCP Length (invalid-tcp-hdr-length)                  21
  Reverse-path verify failed (rpf-violated)                    90


// Check Reverse path statistics

ASA(config)# sh ip verify statistics
interface inside: 11 unicast rpf drops


interface outside: 79 unicast rpf drops
```

Rilevamento delle minacce

Threat Detection fornisce agli amministratori del firewall gli strumenti necessari per identificare, comprendere e arrestare gli attacchi prima che raggiungano l'infrastruttura di rete interna. A tal fine, la funzione si basa su una serie di trigger e statistiche differenti, che sono descritti in dettaglio in queste sezioni.

Per una spiegazione dettagliata del rilevamento delle minacce sull'appliance ASA, consultare il documento sulla funzionalità e configurazione del rilevamento delle minacce dell'appliance ASA.

Filtro botnet

Il filtro del traffico BotNet monitora le richieste e le risposte DNS (Domain Name Server) tra i client DNS interni e i server DNS esterni. Quando viene elaborata una risposta DNS, il dominio associato alla risposta viene confrontato con il database dei domini dannosi noti. In caso di corrispondenza, qualsiasi ulteriore traffico verso l'indirizzo IP presente nella risposta DNS viene bloccato.

Il malware è un software dannoso installato su un host sconosciuto. Il malware che tenta di eseguire attività di rete come l'invio di dati privati (password, numeri di carte di credito, sequenze di tasti o dati proprietari) può essere rilevato dal filtro Traffico Botnet quando il malware avvia una connessione a un indirizzo IP notoriamente non valido. Il filtro traffico Botnet controlla le connessioni in entrata e in uscita confrontandole con un database dinamico di nomi di dominio e indirizzi IP noti e non validi (l'elenco degli indirizzi bloccati), quindi registra o blocca qualsiasi attività sospetta.

È inoltre possibile aggiungere al database dinamico Cisco gli indirizzi di elenco bloccati desiderati aggiungendoli a un elenco statico bloccato. Se il database dinamico include indirizzi di elenchi bloccati che si ritiene non possano essere inseriti nell'elenco di indirizzi bloccati, è possibile immetterli manualmente in un elenco statico consentito. Gli indirizzi elenco consentiti continuano a generare messaggi syslog, ma poiché si utilizzano solo messaggi syslog elenco bloccati, si tratta di messaggi informativi. Per informazioni dettagliate, consultare il documento sulla configurazione del filtro del traffico Botnet.

Aggiunte cache ARP per subnet non connesse

Per impostazione predefinita, l'ASA non risponde al protocollo ARP per gli indirizzi IP delle subnet non connessi direttamente. Se sull'appliance ASA si dispone di un IP NAT che non appartiene alla stessa IP subnet dell'interfaccia ASA, è possibile abilitare arp allow-nonconnected sull'appliance ASA su proxy-ARP per l'IP NATted.

```
arp permit-nonconnected
```

Si consiglia sempre di avere il routing corretto sui dispositivi a monte e a valle in modo che NAT funzioni senza abilitare il comando precedente.

Registrazione e monitoraggio

Configurazione di SNMP

In questa sezione vengono evidenziati diversi metodi che possono essere utilizzati per proteggere la distribuzione di SNMP nei dispositivi ASA. È fondamentale proteggere correttamente il protocollo SNMP per proteggere la riservatezza, l'integrità e la disponibilità sia dei dati di rete che dei dispositivi di rete attraverso cui transitano tali dati. L'SNMP fornisce una vasta gamma di informazioni sullo stato dei dispositivi di rete. Tali informazioni possono essere protette da utenti malintenzionati che desiderano utilizzare questi dati per eseguire attacchi alla rete.

Stringhe della community SNMP

Le stringhe della community sono password che vengono applicate a un dispositivo ASA per limitare l'accesso, sia di sola lettura che di lettura/scrittura, ai dati SNMP sul dispositivo. Queste stringhe della community, come tutte le password, possono essere scelte con cura per evitare che siano insignificanti. Le stringhe della community possono essere modificate a intervalli regolari e in conformità con i criteri di sicurezza delle reti. Ad esempio, le stringhe possono essere modificate quando un amministratore di rete cambia ruolo o lascia la società.

Abilitazione dell'accesso in lettura SNMP

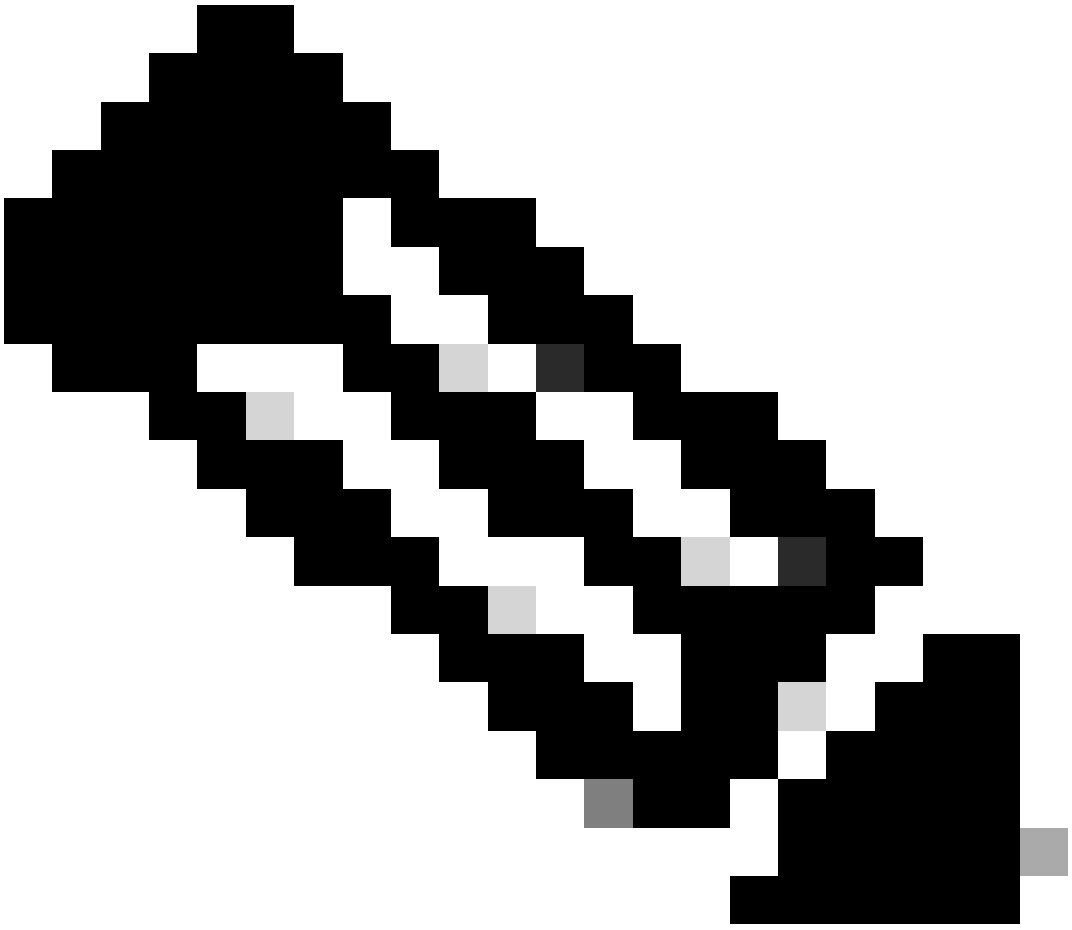
```
snmp-server host <interface_name> <remote_ip_address>
```

Abilitazione delle trap SNMP

```
snmp-server enable traps all
```

Configurazione di Syslog

Si consiglia di inviare le informazioni di registrazione a un server syslog remoto. Ciò rende possibile correlare e controllare gli eventi di rete e di sicurezza tra i dispositivi di rete in modo più efficace.



Nota: i messaggi Syslog vengono trasmessi in modo non affidabile da UDP e in formato non crittografato.

Per questo motivo, tutte le protezioni offerte da una rete per la gestione del traffico (ad esempio, la crittografia o l'accesso out-of-band) possono essere estese in modo da includere il traffico syslog. È possibile configurare l'invio dei log dall'appliance ASA alla destinazione seguente:

- ASDM
- Buffer
- Flash
- Email
- server FTP
- Server SNMP come trap
- server Syslogs

Configura livello di gravità registrazione console

```
logging console critical
```

È disponibile anche un syslog basato su TCP. Tutti i syslog possono essere inviati al server syslog in testo normale o crittografati in caso di TCP.

Testo normale

logging host interface_name syslog_ip [tcp/ porta

Crittografia

logging host interface_name syslog_ip [tcp/ porta | [protetto]

Se non è possibile stabilire una connessione TCP con il server syslogs, tutte le nuove connessioni possono essere negate. È possibile modificare questo comportamento predefinito immettendo il comando logging allow-hostdown.

Configura timestamp nei messaggi di log

La configurazione della registrazione dei timestamp consente di correlare gli eventi tra i dispositivi di rete. È importante implementare una configurazione di timestamp di registrazione corretta e coerente per garantire la correlazione dei dati di registrazione.

```
logging timestamp
```

Per ulteriori informazioni relative al syslog, consultare il documento sull'esempio di configurazione del syslog dell'appliance ASA.

Configurazione di NetFlow

In alcuni casi, è necessario identificare rapidamente e rintracciare il traffico di rete, in particolare durante la risposta a un problema o durante prestazioni di rete insoddisfacenti. NetFlow può fornire visibilità su tutto il traffico della rete. Inoltre, NetFlow può essere implementato con collector in grado di fornire analisi automatizzata e di analisi dei trend a lungo termine.

Cisco ASA supporta i servizi NetFlow versione 9. Le implementazioni ASA e ASASM di NSEL forniscono un metodo di tracciamento del flusso IP con conservazione dello stato che esporta solo i record che indicano eventi significativi in un flusso. Nel tracciamento del flusso con stato, i flussi tracciati attraversano una serie di modifiche dello stato. Gli eventi NSEL vengono utilizzati per esportare i dati relativi allo stato del flusso e vengono attivati dall'evento che ha causato la modifica dello stato.

Per ulteriori informazioni su Netflow sull'ASA, consultare la Cisco ASA NetFlow Implementation Guide:

Protezione della configurazione

Password nella configurazione

Tutte le password e le chiavi sono crittografate o offuscate. Il comando show running-config non rivela le password effettive.

Questo tipo di backup non può essere usato per il backup/ripristino su appliance ASA. Il backup utilizzato a scopo di ripristino viene eseguito utilizzando il comando more system:running-config. Le password di configurazione dell'ASA possono essere crittografate utilizzando una passphrase primaria. Per informazioni dettagliate, fare riferimento a Crittografia password.

Recupero password del servizio

La disattivazione di questa opzione può disabilitare il meccanismo di recupero della password e disabilitare l'accesso a ROMMON. L'unico modo per recuperare le password perse o dimenticate può essere che ROMMON cancelli tutti i file system, compresi i file di configurazione e le immagini. È possibile eseguire un backup della configurazione e disporre di un meccanismo per ripristinare le immagini dalla riga di comando di ROMMON.

Risoluzione dei problemi

Non sono disponibili informazioni sulla risoluzione dei problemi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).