Configurazione dell'accesso alle risorse interne per gli utenti VPN su FTD con HairPin Traffic

Sommario

Problema

L'obiettivo è consentire agli utenti VPN l'accesso completo alle risorse della rete interna dopo la corretta autenticazione VPN tramite RADIUS (su un server aggiunto al dominio Windows) su Cisco Secure Firewall FTD.

L'installazione della VPN è già operativa. Gli utenti possono scaricare e installare il client VPN e autenticarsi correttamente. Il problema riguarda la configurazione del controllo di accesso e delle regole NAT necessarie per consentire l'accesso alle risorse interne necessarie sulla VPN.

Ambiente

- Prodotto: Cisco Secure Firewall Firepower (FTD), versione 7.6.0 (ad esempio un accessorio CSF1220CX)
- Gestione: Firepower Management Center (FMC), FMC distribuito tramite cloud (cdFMC) o Firepower Device Manager (FDM)
- VPN: configurata con l'autenticazione RADIUS su un Server dei criteri di rete Windows
- Pool di indirizzi VPN: 192.168.250.1 - 192.168.250.200
- Esempio di subnet interna di destinazione: 192.168.95.0/24
- Versione del software: 9.2.1 (a cui si fa riferimento nel flusso di lavoro)
- Interfacce rilevanti: interfaccia "esterna" per ingresso VPN
- Accesso RDP e Active Directory richiesto tramite connessione VPN

Risoluzione

In questa procedura viene descritta in dettaglio la configurazione necessaria per consentire agli utenti VPN di accedere alle risorse interne (ad esempio RDP e Active Directory) su Cisco FTD. Sono incluse la creazione di regole per i criteri di accesso, la configurazione delle esenzioni NAT e del protocollo NAT hairpin per il traffico VPN e l'utilizzo dei comandi di risoluzione dei problemi per convalidare la configurazione.

Passaggio 1: aggiungere una voce all'elenco degli accessi per consentire al pool di indirizzi VPN di accedere alle risorse interne.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
```

```
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

Passaggio 2: Aggiungere una regola dell'elenco degli accessi per consentire alle risorse interne di inviare il traffico di ritorno al pool VPN:

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

Tali norme possono essere rese più rigorose per limitare le fonti e le destinazioni specifiche in base alle necessità.

Passaggio 3: configurare l'esenzione NAT o il protocollo NAT hairpin per il traffico VPN

Esistono due approcci comuni:

- ◦ Opzione A: Esenzione NAT per pool VPN su subnet interna

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ Opzione B: NAT hairpin per pool VPN sulla stessa interfaccia (no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ Opzione C: NAT con hairpin dinamico per pool VPN su interfaccia esterna

```
nat (outside,outside) dynamic VPN_Pool interface
```

Il metodo corretto dipende dal fatto che le risorse interne si trovino sulla stessa interfaccia fisica (che richiede un NAT hairpin) o su interfacce diverse (esenzione NAT).

Passaggio 4: utilizzare il comando `packet-tracer` per simulare i flussi di traffico dal pool VPN alle risorse interne e verificare se il traffico è autorizzato dalla regola, dal protocollo NAT e dal routing previsti.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
```

```
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

Nota: l'output packet-tracer per la fase WebVPN potrebbe mostrare un "DROP" per il traffico VPN sull'interfaccia esterna. Questo è il comportamento previsto per il traffico in testo normale sull'interfaccia esterna e può ancora essere usato per convalidare NAT.

Note aggiuntive:

- È possibile che le acquisizioni di pacchetti nell'interfaccia utente di difesa dalle minacce visualizzino solo le richieste in arrivo. Se non vengono rilevate perdite, ma il traffico non raggiunge la risorsa interna, controllare le regole NAT e dell'elenco degli accessi.
- Quando SSH non è disponibile, tutte le operazioni di risoluzione dei problemi possono essere eseguite tramite le funzionalità dell'interfaccia utente di Threat Defense in cdFMC, ma l'utilizzo dei comandi è limitato.
- È possibile che siano necessarie alcune modifiche sui dispositivi adiacenti per la connettività end-to-end.

Causa

La causa principale è stata l'insufficienza dei criteri di accesso e della configurazione NAT per il traffico da VPN a interno e da interno a VPN del pool. La configurazione predefinita non consente la comunicazione bidirezionale completa dal pool VPN alle risorse interne e viceversa, né gestisce i requisiti NAT hairpin per il traffico in entrata e in uscita sulla stessa interfaccia.

Contenuto correlato

- Configura esenzione NAT su FTD
- Supporto tecnico Cisco e download

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).