Interne toegang tot bronnen configureren voor VPN-gebruikers op FTD met HairPin-verkeer

Inhoud

uitgeven

Het doel is om volledige toegang voor VPN-gebruikers tot interne netwerkbronnen mogelijk te maken na succesvolle VPN-verificatie met RADIUS (tegen een Windows-domein-gekoppelde server) op Cisco Secure Firewall FTD.

De VPN-installatie is al operationeel; gebruikers kunnen de VPN-client downloaden en installeren en zich met succes verifiëren. Het probleem is gericht op het configureren van de nodige toegangscontrole en NAT-regels om de vereiste interne bronnentoegang via de VPN mogelijk te maken.

milieu

- Product: Cisco Secure Firewall Firepower (FTD), versie 7.6.0 (zoals een CSF1220CX-toestel)
- Beheer: Firepower Management Center (FMC), door de cloud geleverde FMC (cdFMC) of Firepower Device Manager (FDM)
- VPN: geconfigureerd met RADIUS-verificatie tegen een Windows Domain-Join Server (NPS)
- VPN-adrespool: 192.168.250.1 - 192.168.250.200
- Voorbeeld intern subnet doel: 192.168.95.0/24
- Softwareversie: 9.22.1 (zoals vermeld in workflow)
- Relevante interfaces: 'outside' interface voor VPN-toegang
- Toegang tot RDP en Active Directory vereist via VPN-verbinding

resolutie

Deze stappen beschrijven de configuratie die nodig is om VPN-gebruikers toegang te geven tot interne bronnen (zoals RDP en Active Directory) op Cisco FTD. Dit omvat het maken van toegangsbeleidsregels, het configureren van NAT-vrijstellingen en hairpin NAT voor VPN-verkeer en het gebruik van opdrachten voor probleemoplossing om de configuratie te valideren.

Stap 1: Voeg een toegangslijstvermelding toe zodat de VPN-adrespool toegang heeft tot interne bronnen.

```
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
```

Stap 2: Voeg een regel voor de toegangslijst toe zodat interne bronnen retourverkeer naar de VPN-pool kunnen verzenden:

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

Deze regels kunnen later worden aangescherpt om specifieke bronnen en bestemmingen zo nodig te beperken.

Stap 3: NAT-vrijstelling of Hairpin NAT configureren voor VPN-verkeer

Er zijn twee gemeenschappelijke benaderingen:

- ◦ Optie A: NAT-vrijstelling voor VPN-pool naar intern subnet

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

- ◦ Optie B: Hairpin NAT voor VPN-pool op dezelfde interface (geen proxy-arp)

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

- ◦ Optie C: Dynamic Hairpin NAT voor VPN-pool op externe interface

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

De juiste methode hangt af van de vraag of de interne middelen zich op dezelfde fysieke interface bevinden (waarvoor een hairpin NAT vereist is) of op verschillende interfaces (NAT-vrijstelling).

Stap 4: Gebruik de `packet-tracer`-opdracht om verkeersstromen van de VPN-pool naar interne bronnen te simuleren en te valideren of het verkeer is toegestaan door de beoogde regel, NAT en route.

```
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
```

Opmerking: De packet-tracer-uitvoer voor de WebVPN-fase kan een "DROP" voor VPN-verkeer aan de buitenzijde van de interface tonen. Dit gedrag wordt verwacht voor platte tekstverkeer op de externe interface en kan nog steeds worden gebruikt om NAT te valideren.

Aanvullende opmerkingen:

- Het is mogelijk dat pakketopnames in de Threat Defense UI alleen inkomende verzoeken weergeven. Als er geen dalingen worden waargenomen, maar het verkeer de interne bron niet bereikt, controleert u NAT en toegangslijstregels.
- Wanneer SSH niet beschikbaar is, kan alle probleemoplossing worden uitgevoerd via de Threat Defense UI-functies in cdFMC, maar het gebruik van de opdracht is beperkt.
- Het is mogelijk dat sommige aanpassingen nodig zijn op aangrenzende apparaten voor end-to-end connectiviteit.

Oorzaak

De hoofdoorzaak was onvoldoende toegangsbeleid en NAT-configuratie voor VPN-naar-intern en intern-naar-VPN-poolverkeer. De standaardconfiguratie stond geen volledige bidirectionele communicatie toe van de VPN-pool naar interne bronnen en terug, noch behandelde het de haarspeldbehoeften van NAT voor het binnendringen en teruggaan van verkeer op dezelfde interface.

Verwante inhoud

- NAT-vrijstelling configureren voor FTD
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.