Configure Internal Resource Access for VPN Users on FTD with HairPin Traffic

Contents

Issue

The goal is to enable full access for VPN users to internal network resources after successful VPN authentication usi
joined server) on Cisco Secure Firewall FTD.

The VPN setup is already operational; users can download and install the VPN client and authenticate successfully. T

Environment

- Product: Cisco Secure Firewall Firepower (FTD), version 7.6.0 (such as a CSF1220CX appliance)
- Management: Firepower Management Center (FMC), cloud-delivered FMC (cdFMC), or Firepower Device Manager (FDM)
- VPN: Configured with RADIUS authentication against a Windows domain-joined server (NPS)
- VPN Address Pool: 192.168.250.1 - 192.168.250.200
- Target Internal Subnet Example: 192.168.95.0/24
- Software Version: 9.22.1 (as referenced in workflow)
- Relevant interfaces: 'outside' interface for VPN ingress
- RDP and Active Directory access required over VPN connection

Resolution

These steps detail the configuration required to permit VPN users to access internal resources (such as RDP and Acti

Step 1: Add an access-list entry to allow the VPN address pool to access internal resources.

```
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
```

Step 2: Add an access-list rule to allow internal resources to send return traffic to the VPN pool:

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

These rules can later be tightened to restrict specific sources and destinations as needed.

Step 3: Configure NAT Exemption or Hairpin NAT for VPN Traffic

There are two common approaches:

- *Option A: NAT Exemption for VPN Pool to Internal Subnet*

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

- *Option B: Hairpin NAT for VPN Pool on Same Interface (no-proxy-arp)*

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

- *Option C: Dynamic Hairpin NAT for VPN Pool on Outside Interface*

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

The correct method depends on whether internal resources are on the same physical interface (requiring hairpin NAT

Step 4: Use the `packet-tracer` command to simulate traffic flows from the VPN pool to internal resources and validate if the traffic is permi

```
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
```

Note: The packet-tracer output for the WebVPN phase could show a "DROP" for VPN traffic on the outside interface. This is expected

Additional Notes:

- It is possible that packet captures in the Threat Defense UI only show incoming requests. If no drops are obser
  list rules.
- When SSH is not available, all troubleshooting can be performed via the Threat Defense UI features in cdFMC
- It is possible that some modifications are needed on adjacent devices for end-to-end connectivity.

Cause

The root cause was insufficient access policy and NAT configuration for VPN-to-internal and internal-to-VPN pool traffic. The default configuration did not allow for full bidirectional communication from the VPN pool to internal resources and back, nor did it handle hairpin NAT requirements for traffic ingressing and egressing on the same interface.

Related Content

- Configure NAT Exemption on FTD
- Cisco Technical Support & Downloads