Konfigurieren des internen Ressourcenzugriffs für VPN-Benutzer auf FTD mit HairPin-Datenverkehr

Inhalt

Problem

Das Ziel besteht darin, nach erfolgreicher VPN-Authentifizierung über RADIUS (gegen einen Windows-Domänenserver) auf Cisco Secure Firewall FTD einen uneingeschränkten Zugriff für VPN-Benutzer auf interne Netzwerkressourcen zu ermöglichen.

Das VPN-Setup ist bereits betriebsbereit. Benutzer können den VPN-Client herunterladen und installieren und sich erfolgreich authentifizieren. Der Schwerpunkt des Problems liegt auf der Konfiguration der erforderlichen Zugriffskontroll- und NAT-Regeln, um den erforderlichen Zugriff auf interne Ressourcen über das VPN zu ermöglichen.

Umwelt

- Produkt: Cisco Secure Firewall FirePOWER (FTD), Version 7.6.0 (z. B. eine CSF1220CX-Appliance)
- Management: FirePOWER Management Center (FMC), Cloud-basiertes FMC (cdFMC) oder FirePOWER Device Manager (FDM)
- VPN: Konfiguration mit RADIUS-Authentifizierung für einen Windows-Server mit Domänenbeitritt (NPS)
- VPN-Adresspool: 192.168.250.1 - 192.168.250.200
- Beispiel für ein internes Ziel-Subnetz: 192.168.95.0/24
- Softwareversion: 9.22.1 (wie im Workflow angegeben)
- Relevante Schnittstellen: externe Schnittstelle für VPN-Eingang
- RDP- und Active Directory-Zugriff über VPN-Verbindung erforderlich

Auflösung

In diesen Schritten wird die Konfiguration beschrieben, die erforderlich ist, um VPN-Benutzern den Zugriff auf interne Ressourcen (z. B. RDP und Active Directory) in Cisco FTD zu ermöglichen. Dies umfasst das Erstellen von Zugriffsrichtlinienregeln, das Konfigurieren von NAT-Ausnahmen und der Festlegung von NAT für VPN-Datenverkehr sowie die Verwendung von Befehlen zur Fehlerbehebung zur Validierung der Konfiguration.

Schritt 1: Fügen Sie einen Zugriffslisteneintrag hinzu, damit der VPN-Adresspool auf interne

Ressourcen zugreifen kann.

```
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
```

Schritt 2: Fügen Sie eine Zugriffslistenregel hinzu, damit interne Ressourcen zurückfließenden Datenverkehr an den VPN-Pool senden können:

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

Diese Regeln können später verschärft werden, um bestimmte Quellen und Ziele nach Bedarf einzuschränken.

Schritt 3: Konfigurieren der NAT-Ausnahme oder der Hairpin-NAT für den VPN-Datenverkehr

Es gibt zwei gemeinsame Ansätze:

- ◦ Option A: NAT-Ausnahme für VPN-Pool zu internem Subnetz

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

- ◦ Option B: Hairpin NAT für VPN-Pool auf derselben Schnittstelle (kein Proxy-ARP)

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

- ◦ Option C: Dynamic Hairpin NAT für VPN-Pool an externer Schnittstelle

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

Die richtige Methode hängt davon ab, ob sich die internen Ressourcen auf derselben physischen Schnittstelle (die Hairpin-NAT erfordert) oder auf unterschiedlichen Schnittstellen (NAT-Ausnahme) befinden.

Schritt 4: Verwenden Sie den `Paket-Tracer`-Befehl, um Datenverkehrsflüsse vom VPN-Pool zu internen Ressourcen zu simulieren und zu überprüfen, ob der Datenverkehr gemäß der

beabsichtigten Regel, NAT und Route zulässig ist.

```
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
```

Hinweis: Die Paketverfolgungsausgabe für die WebVPN-Phase könnte ein "DROP" für VPN-Datenverkehr an der externen Schnittstelle anzeigen. Dies ist ein erwartetes Verhalten für reinen Textdatenverkehr an der externen Schnittstelle und kann weiterhin zur Validierung von NAT verwendet werden.

Zusätzliche Hinweise:

- Es ist möglich, dass bei der Paketerfassung in der Threat Defense-Benutzeroberfläche nur eingehende Anforderungen angezeigt werden. Wenn keine Verwerfungen festgestellt werden, der Datenverkehr jedoch nicht die interne Ressource erreicht, überprüfen Sie die NAT und die Zugriffslistenregeln.
- Wenn SSH nicht verfügbar ist, kann die gesamte Fehlerbehebung über die Benutzeroberflächenfunktionen von Threat Defense in cdFMC durchgeführt werden. Die Befehlsverwendung ist jedoch begrenzt.
- Es ist möglich, dass einige Änderungen an benachbarten Geräten erforderlich sind, um eine End-to-End-Verbindung herzustellen.

Ursache

Die Ursache hierfür waren unzureichende Zugriffsrichtlinien und NAT-Konfigurationen für den Datenverkehr zwischen VPN und internen VPN-Pools. Die Standardkonfiguration erlaubte keine vollständige bidirektionale Kommunikation vom VPN-Pool zu internen Ressourcen und zurück und bewältigte auch nicht die Hairpin NAT-Anforderungen für den ein- und ausgehenden Datenverkehr auf derselben Schnittstelle.

Verwandte Inhalte

- Konfigurieren der NAT-Ausnahme für FTD
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.