Hairpin mit FirePOWER Management Center konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die erforderlichen Schritte, um Hairpin erfolgreich auf einem Firepower Threat Defense (FTD) mit Firepower Management Center (FMC) zu konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Management Center (FMC)
- Firepówer Threat Defence (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER Management Center Virtual 7.2.4
- Firepower Threat Defense Virtual 7.2.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

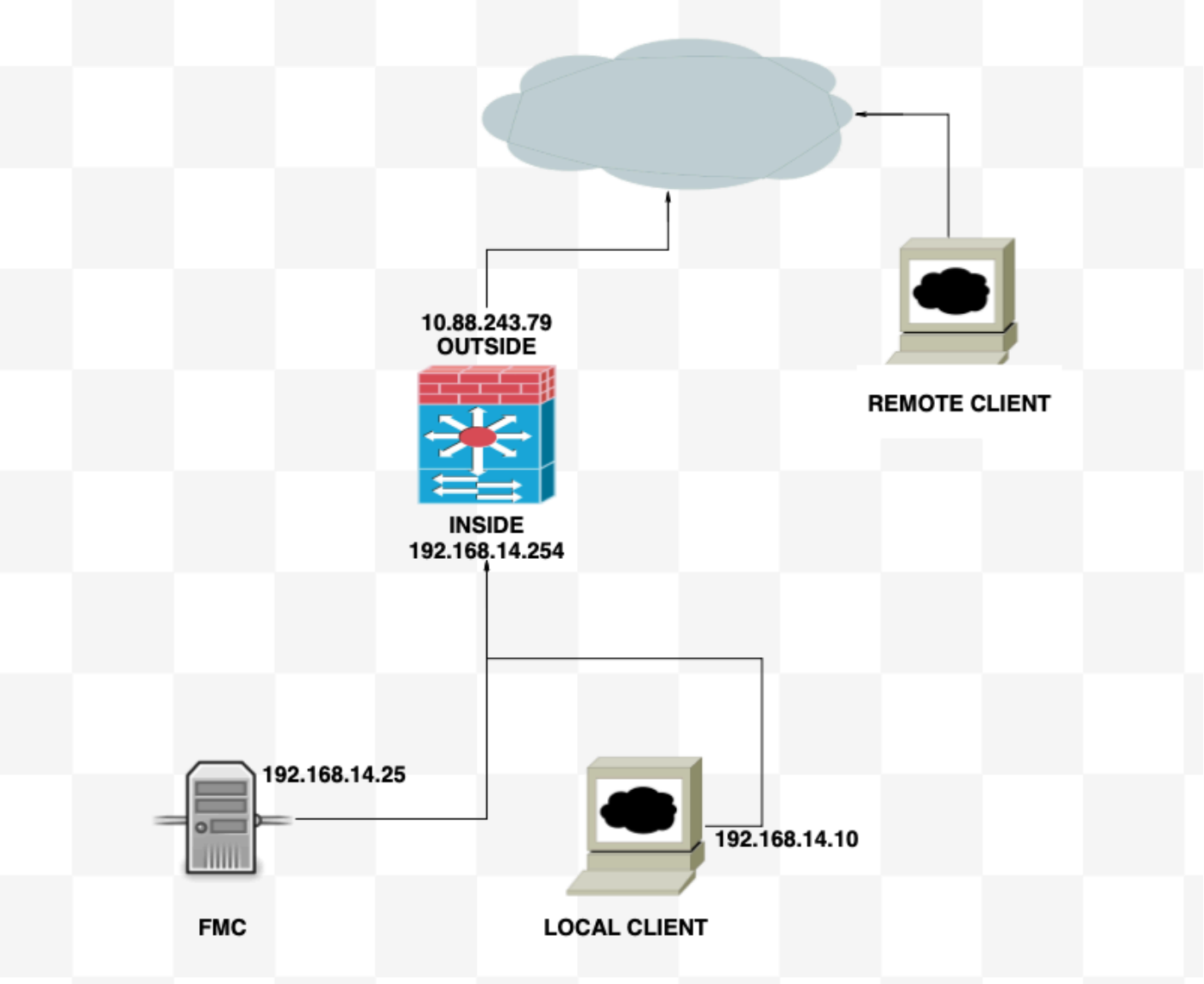
Konfigurieren

Der Begriff "Hairpin" wird verwendet, weil der Datenverkehr vom Client zum Router (oder zur Firewall, die NAT implementiert) gelangt und dann nach der Übersetzung wie ein Hairpin zum internen Netzwerk zurückgeleitet wird, um auf die private IP-Adresse des Servers zuzugreifen.

Diese Funktion ist nützlich für Netzwerkdienste wie Web-Hosting innerhalb eines lokalen Netzwerks, bei denen die Benutzer des lokalen Netzwerks unter Verwendung derselben URL oder IP-Adresse auf den internen Server zugreifen müssen, die externe Benutzer verwenden würden. Es gewährleistet einen einheitlichen Zugriff auf Ressourcen, unabhängig davon, ob die Anforderung von innerhalb oder außerhalb des lokalen Netzwerks stammt.

In diesem Beispiel muss auf ein FMC über die IP-Adresse der externen Schnittstelle des FTD zugegriffen werden.

Diagramm

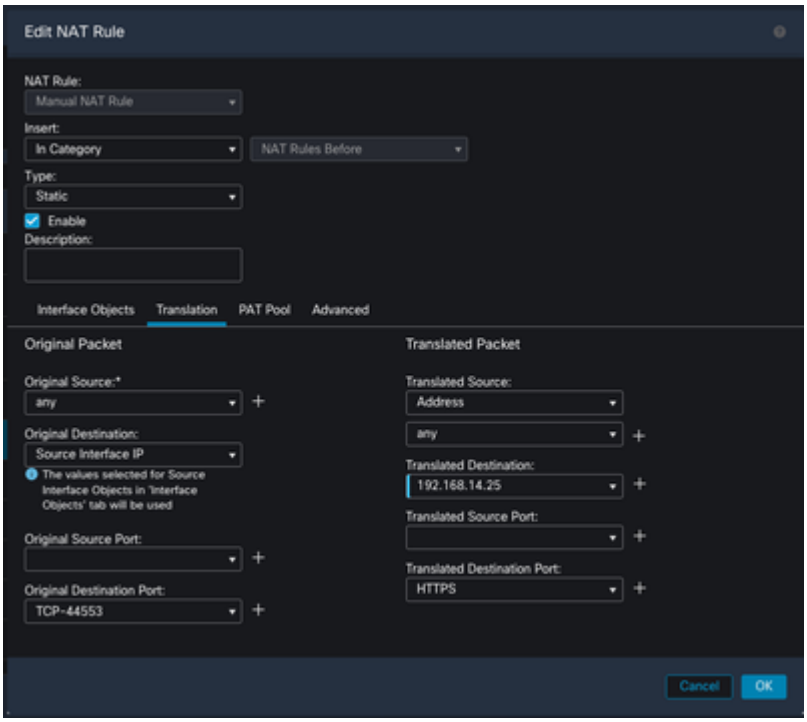


Schritt 1: Konfigurieren der externen internen NAT

Als erster Schritt muss eine statische NAT konfiguriert werden. In diesem Beispiel werden die Ziel-IP-Adresse und der Ziel-Port mithilfe der IP-Adresse der externen Schnittstelle umgewandelt, und das Port-Ziel lautet 44553.

Navigieren Sie vom FMC zu Device > NAT, um die vorhandene Richtlinie zu erstellen oder zu bearbeiten, und klicken Sie dann auf das Feld Add Rule (Regel hinzufügen).

- NAT-Regel: Manuelle NAT-Regel
- Originalquelle: Beliebig
- Ursprüngliches Ziel: IP der Quellschnittstelle
- Ursprünglicher Zielport: 44553
- Übersetztes Ziel: 192.168.14.25
- Übersetzter Ziel-Port: 443



Konfigurieren Sie die Richtlinie. Navigieren Sie zuRichtlinien > Zugriffskontrolle, um die vorhandene Richtlinie zu erstellen oder zu bearbeiten, und klicken Sie dann auf das Feld Regel hinzufügen.

Quellzone: Außen

Zielzone: Intern

Quellnetzwerk: Beliebig

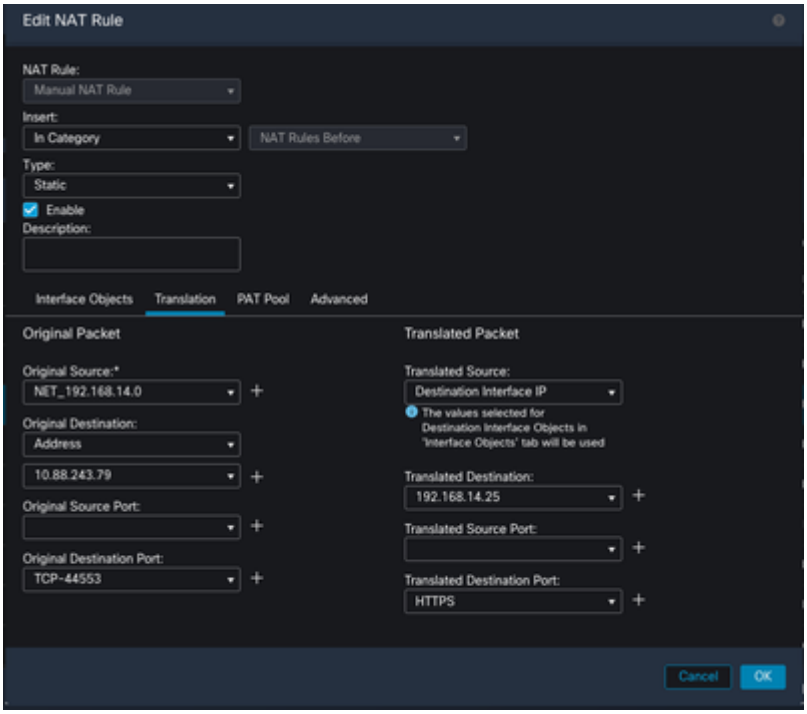
Zielnetzwerk: 10.88.243.79

Schritt 2: Konfigurieren der internen Nat (Hairpin)

Im zweiten Schritt muss eine statische NAT von innen nach innen konfiguriert werden. In diesem Beispiel werden die Ziel-IP-Adresse und der Ziel-Port mithilfe eines Objekts mit der IP-Adresse der externen Schnittstelle umgewandelt, und der Ziel-Port ist 44553.

Navigieren Sie vom FMC zu Device > NAT, um die vorhandene Richtlinie zu bearbeiten, und klicken Sie dann auf das Feld Add Rule (Regel hinzufügen).

- NAT-Regel: Manuelle NAT-Regel
- Originalquelle: 192.168.14.0/24
- Ursprüngliches Ziel: Adresse 10.88.243.79
- Ursprünglicher Zielport: 44553
- Übersetzte Quelle: IP-Zielschnittstelle
- Übersetztes Ziel: 192.168.14.25
- Übersetzter Ziel-Port: 443



Konfigurieren Sie die Richtlinie. Navigieren Sie zu Richtlinien > Zugriffskontrolle, um die vorhandene Richtlinie zu bearbeiten, und klicken Sie dann auf das Feld Regel hinzufügen.

Quellzone: Beliebig

Zielzone: Beliebig

Quellnetzwerk: 192.168.14.0/24

Zielnetzwerk: 10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	Any
2	Hairpin	Any	Any	NET_192.168.14	10.88.243.79

Überprüfung

Führen Sie vom lokalen Client ein Telnet mit der Ziel-IP und dem Ziel-Port aus:

Wenn die Fehlermeldung "telnet cannot connect to remote host: Zeitüberschreitung bei der Verbindungsanforderung", ist irgendwann während der Konfiguration ein Fehler aufgetreten.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

Die Meldung "Connected" (Verbunden) zeigt an, dass die Konfiguration erfolgreich war.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

Fehlerbehebung

Wenn bei der Network Address Translation (NAT) Probleme auftreten, verwenden Sie diese schrittweise Anleitung, um häufige Probleme zu beheben.

Schritt 1: Konfigurationsprüfung der NAT-Regeln

- NAT-Regeln überprüfen: Stellen Sie sicher, dass alle NAT-Regeln in FMC korrekt konfiguriert sind. Überprüfen Sie die Quell- und Ziel-IP-Adressen sowie die Ports auf ihre Richtigkeit.
- Schnittstellenzuweisung: Vergewissern Sie sich, dass die Quell- und Zielschnittstellen in der NAT-Regel korrekt zugewiesen sind. Eine falsche Zuordnung kann dazu führen, dass der Datenverkehr nicht richtig übersetzt oder weitergeleitet wird.
- NAT-Regelpriorität: Vergewissern Sie sich, dass die NAT-Regel an der Spitze jeder anderen Regel steht, die mit demselben Datenverkehr übereinstimmen kann. Regeln in FMC werden in sequenzieller Reihenfolge verarbeitet, sodass eine höher gelegene Regel Vorrang hat.

Phase 2: Überprüfung von Zugriffskontrollregeln (ACL)

- Prüfen von ACLs: Überprüfen Sie die Zugriffskontrolllisten, um sicherzustellen, dass sie für das Zulassen von NAT-Datenverkehr geeignet sind. ACLs müssen so konfiguriert werden, dass sie die umgewandelten IP-Adressen erkennen.
- Reihenfolge der Regeln: Vergewissern Sie sich, dass die Zugriffskontrollliste in der richtigen Reihenfolge angeordnet ist. Wie NAT-Regeln werden ACLs von oben nach unten verarbeitet, und die erste Regel, die mit dem Datenverkehr übereinstimmt, wird angewendet.
- Datenverkehrsberechtigungen: Überprüfen Sie, ob eine geeignete Zugriffskontrollliste vorhanden ist, um Datenverkehr vom internen Netzwerk zum umgewandelten Ziel zuzulassen. Wenn eine Regel fehlt oder falsch konfiguriert ist, kann der gewünschte Datenverkehr blockiert werden.

Schritt 3: Zusätzliche Diagnose

- Verwenden Sie Diagnosetools: Verwenden Sie die in FMC verfügbaren Diagnosetools, um den Datenverkehr zu überwachen und zu debuggen, der durch das Gerät geleitet wird. Dazu gehört das Anzeigen von Echtzeitprotokollen und Verbindungsereignissen.
- Verbindungen neu starten: In einigen Fällen können vorhandene Verbindungen Änderungen an NAT-Regeln oder ACLs erst erkennen, wenn sie neu gestartet werden. Bereinigen Sie vorhandene Verbindungen, um die Anwendung neuer Regeln zu erzwingen.

Von LINA:

<#root>

firepower#

clear xlate

- Übersetzung überprüfen: Verwenden Sie Befehle wie show xlate und show nat in der Befehlszeile, wenn Sie mit FTD-Geräten arbeiten, um sicherzustellen, dass NAT-Übersetzungen wie erwartet durchgeführt werden.

Von LINA:

<#root>

firepower#

show nat

<#root>

firepower#

show xlate

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.