Hairpin auf ASA konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur erfolgreichen Konfiguration von Hairpin auf einer Cisco Adaptive Security Appliance (ASA) beschrieben

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- NAT-Konfiguration auf ASA
- ACL-Konfiguration auf ASA

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance-Software Version 9.18(4)22

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

Hairpin Network Address Translation (NAT), auch als NAT-Loopback oder NAT-Reflexion bezeichnet, ist eine Technik, die beim Netzwerk-Routing verwendet wird, bei der ein Gerät in einem privaten Netzwerk über eine öffentliche IP-Adresse auf ein anderes Gerät im gleichen privaten Netzwerk zugreifen kann.

Dies wird verwendet, wenn ein Server hinter einem Router gehostet wird und Sie Geräte im selben lokalen Netzwerk wie den Server für den Zugriff auf den Server mithilfe der öffentlichen IP-Adresse (die dem Router vom Internet Service Provider zugewiesen wurde) aktivieren möchten, genau wie ein externes Gerät.

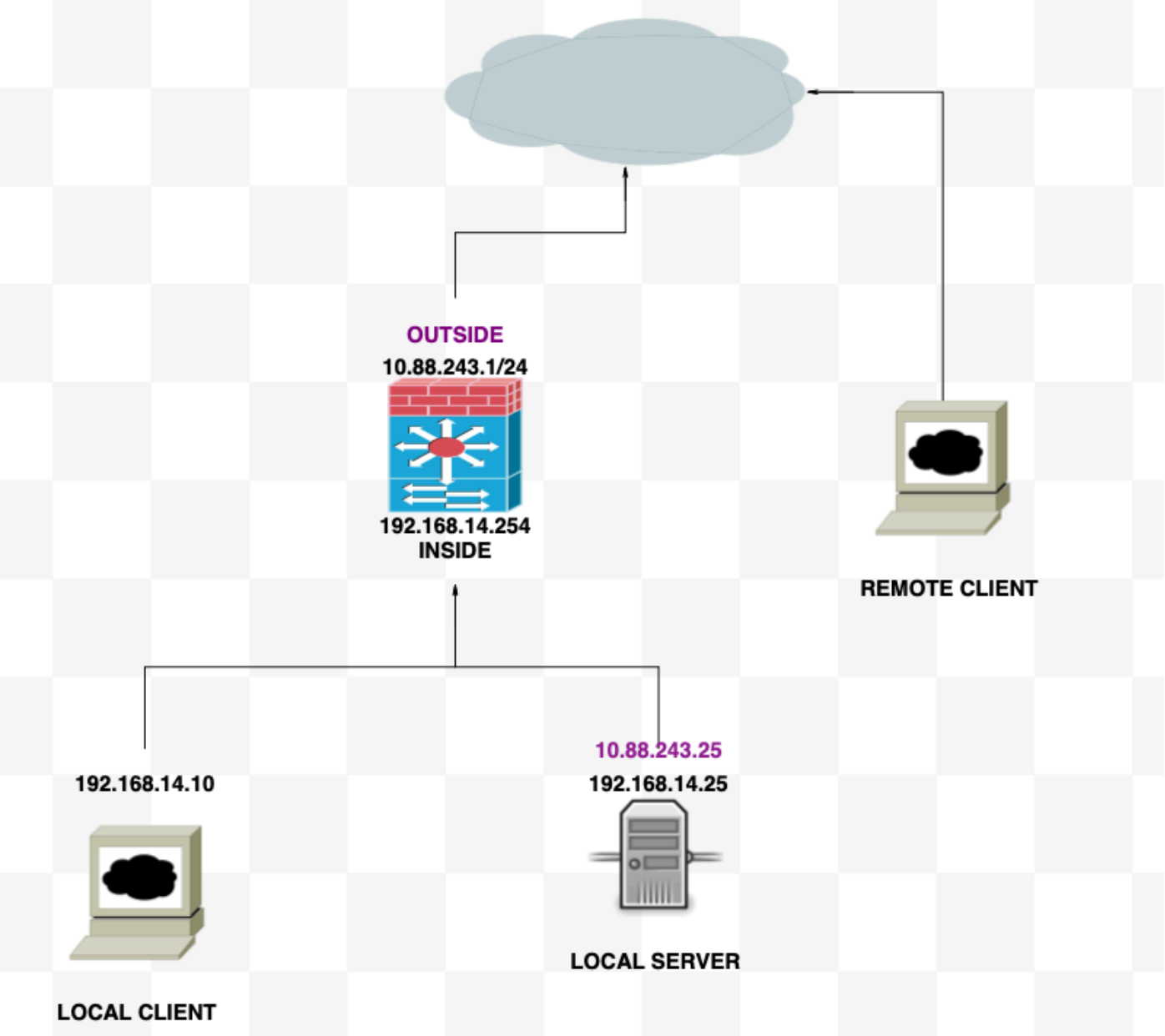
Der Begriff "Hairpin" wird verwendet, weil der Datenverkehr vom Client zum Router (oder zur Firewall, die NAT implementiert) gelangt und dann nach der Übersetzung wie ein Hairpin zum internen Netzwerk "zurückgeschaltet" wird, um auf die private IP-Adresse des Servers zuzugreifen.

Zum Beispiel haben Sie einen Webserver in Ihrem lokalen Netzwerk mit einer privaten IP-Adresse. Sie möchten auf diesen Server über seine öffentliche IP-Adresse oder einen Domänennamen zugreifen, der in die öffentliche IP-Adresse aufgelöst wird, auch wenn Sie sich im selben lokalen Netzwerk befinden.

Ohne Hairpin NAT würde Ihr Router diese Anforderung nicht verstehen, da er erwartet, dass Anforderungen für die öffentliche IP-Adresse von außerhalb des Netzwerks kommen.

Hairpin NAT löst dieses Problem, indem es dem Router ermöglicht zu erkennen, dass die Anforderung zwar an eine öffentliche IP-Adresse gesendet wird, sie aber an ein Gerät im lokalen Netzwerk weitergeleitet werden muss.

Netzwerkdiagramm



Konfigurationen

Schritt 1: Erstellen der Objekte

- Internes Netzwerk:192.168.14.10
- Webserver: 192.168.14.25
- Öffentlicher Webserver: 10.88.243.25
- Port: 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

Schritt 2: Erstellen der NAT

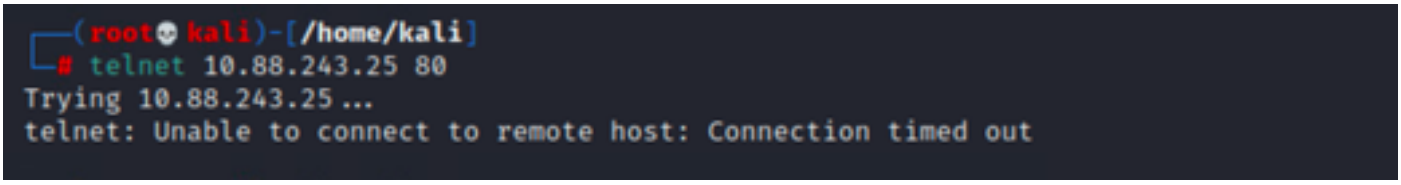
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

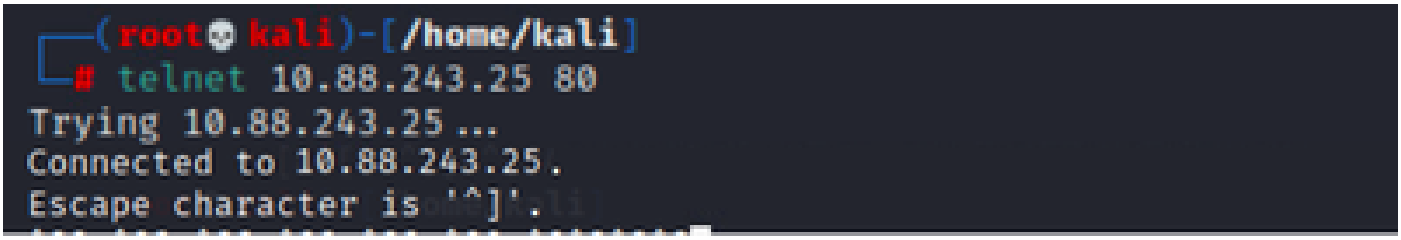
Überprüfung

Führen Sie vom lokalen Client eine Telnet-Ziel-IP mit dem Zielport aus:

Wenn die Meldung "telnet cannot to connect to remote host: Connection timed out" (Telnet kann keine Verbindung mit dem Remotehost herstellen) angezeigt wird, ist während der Konfiguration ein Fehler aufgetreten.



Aber wenn es "Connected" heißt, funktioniert es!



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 richtig 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 Rule Priority (NAT-Regelpriorität): Überprüfen Sie, ob die NAT-Regel höher priorisiert wird als jede andere Regel, die möglicherweise mit demselben Datenverkehr übereinstimmt. Regeln werden in einer sequenziellen Reihenfolge verarbeitet, sodass eine höher gelegene Regel Vorrang hat.

Schritt 2: Überprüfung von Zugriffskontrollregeln (ACL)

- Prüfen von ACLs: Überprüfen Sie die Zugriffskontrolllisten, um sicherzustellen, dass sie für die Genehmigung von NAT-Datenverkehr geeignet sind. ACLs müssen so konfiguriert werden, dass sie die umgewandelten IP-Adressen erkennen.
- Regelreihenfolge: 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: Vergewissern Sie sich, dass eine geeignete Zugriffskontrollliste vorhanden ist, um den Datenverkehr vom internen Netzwerk zum übersetzten 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 verfügbaren Diagnosetools, um den Datenverkehr, der das Gerät durchläuft, zu überwachen und zu debuggen. Dazu gehört das Anzeigen von Echtzeitprotokollen und Verbindungsereignissen.
- Verbindungen neu starten: In einigen Fällen erkennen vorhandene Verbindungen Änderungen an NAT-Regeln oder ACLs erst nach dem Neustart. Bereinigen Sie vorhandene Verbindungen, um die Anwendung neuer Regeln zu erzwingen.

<#root>

ciscoasa(config)#

```
 clear xlate
```

- Übersetzung überprüfen: Verwenden Sie Befehle wie "show xlate" und "show nat" in der Befehlszeile, wenn Sie mit ASA-Geräten arbeiten, um zu überprüfen, ob NAT-Übersetzungen wie erwartet durchgeführt werden.

<#root>

ciscoasa(config)#

 show xlate

<#root>

ciscoasa(config)#

 show nat

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.