Fehlerbehebung bei der Konfiguration der ASA Network Address Translation (NAT)

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Network Address Translation (NAT)-Konfiguration auf der Cisco Adaptive Security Appliance (ASA)-Plattform beschrieben.

Voraussetzungen

Anforderungen

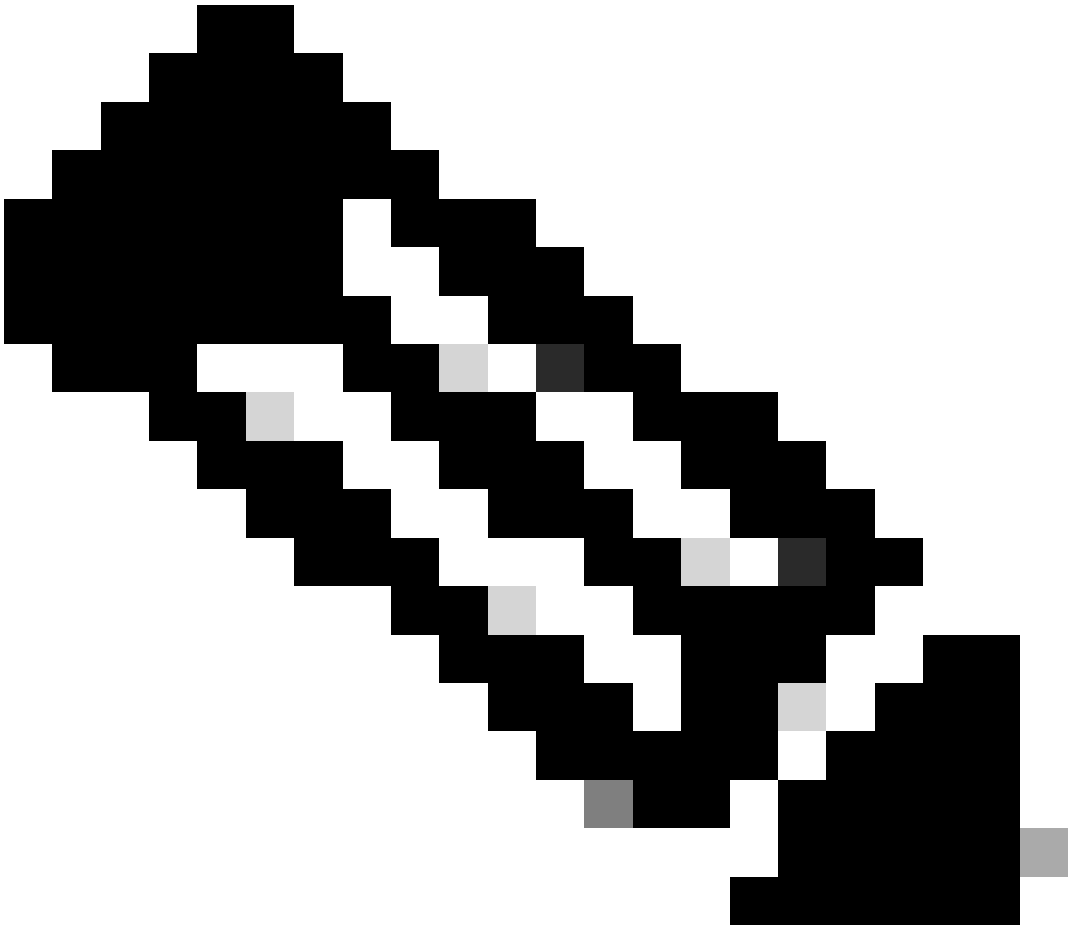
Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf ASA Version 8.3 und höher.

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.

Fehlerbehebung bei der NAT-Konfiguration auf der ASA



> Hinweis: Einige grundlegende Beispiele für NAT-Konfigurationen, darunter ein Video mit einer grundlegenden NAT-Konfiguration, finden Sie im Abschnitt Zugehörige Informationen am Ende dieses Dokuments.

Bei der Fehlerbehebung von NAT-Konfigurationen ist es wichtig zu wissen, wie die NAT-Konfiguration auf der ASA zum Erstellen der NAT-Richtlinientabelle verwendet wird.

Diese Konfigurationsfehler sind für die Mehrzahl der NAT-Probleme verantwortlich, mit denen ASA-Administratoren konfrontiert sind:

- Die NAT-Konfigurationsregeln sind ungültig. So wird beispielsweise eine manuelle NAT-Regel oben in der NAT-Tabelle platziert, wodurch spezifischere Regeln, die weiter unten in der NAT-Tabelle platziert werden, nie getroffen werden.
- Die in der NAT-Konfiguration verwendeten Netzwerkobjekte sind zu breit gefasst. Dadurch stimmt der Datenverkehr versehentlich mit diesen NAT-Regeln überein und verpasst

spezifischere NAT-Regeln.

Mit dem Packet Tracer-Dienstprogramm können die meisten NAT-bezogenen Probleme auf der ASA diagnostiziert werden. Im nächsten Abschnitt finden Sie weitere Informationen dazu, wie die NAT-Konfiguration zum Erstellen der NAT-Richtlinientabelle verwendet wird und wie Sie spezifische NAT-Probleme beheben und beheben.

Darüber hinaus kann der Befehl show nat detail verwendet werden, um zu ermitteln, welche NAT-Regeln von neuen Verbindungen betroffen sind.

Verwendung der ASA-Konfiguration zum Erstellen der NAT-Richtlinientabelle

Alle von der ASA verarbeiteten Pakete werden anhand der NAT-Tabelle ausgewertet. Diese Evaluierung beginnt am oberen Rand (Abschnitt 1) und läuft nach unten, bis eine NAT-Regel zugeordnet wird.

Wenn eine NAT-Regel zugeordnet wurde, wird diese im Allgemeinen auf die Verbindung angewendet, und es werden keine NAT-Richtlinien mehr mit dem Paket abgeglichen. Im Folgenden werden jedoch einige Vorbehalte erläutert.

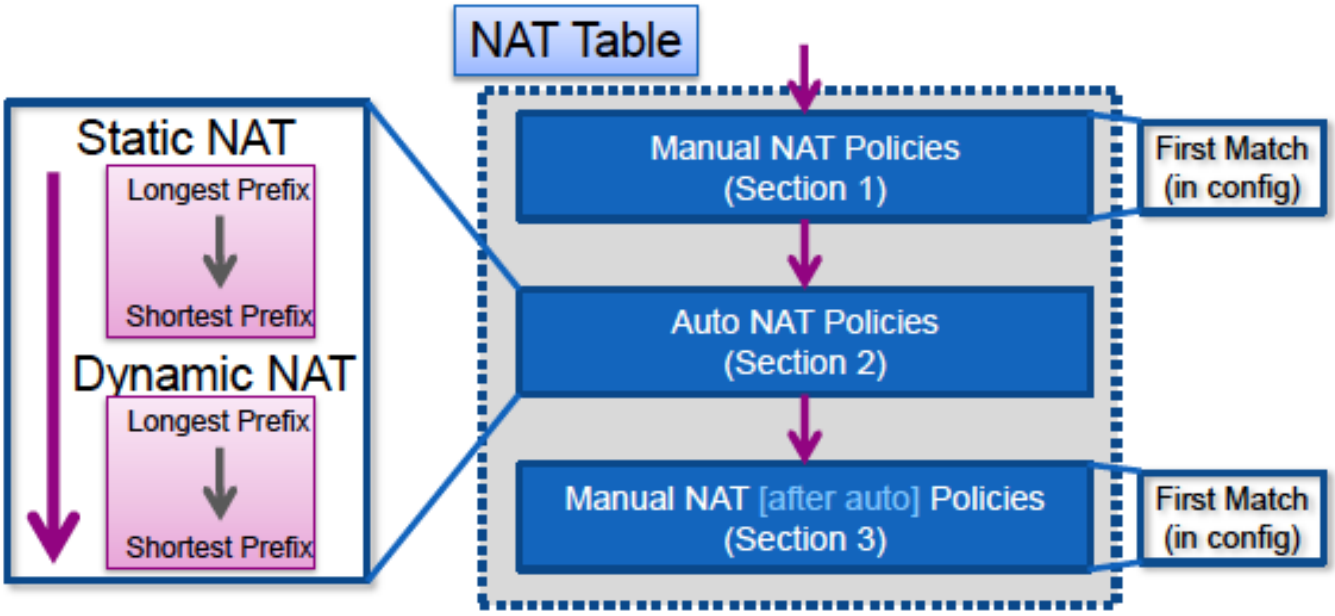
Die NAT-Richtlinientabelle

Die NAT-Richtlinie auf der ASA basiert auf der NAT-Konfiguration.

Die ASA NAT-Tabelle ist in drei Abschnitte unterteilt:

Abschnitt 1	Manuelle NAT-Richtlinien Diese werden in der Reihenfolge verarbeitet, in der sie in der Konfiguration angezeigt werden.
Abschnitt 2	Auto NAT-Richtlinien Diese werden basierend auf dem NAT-Typ (statisch oder dynamisch) und der Präfixlänge (Subnetzmaske) im Objekt verarbeitet.
Abschnitt 3	Manuelle NAT-Richtlinien nach dem Start Diese werden in der Reihenfolge verarbeitet, in der sie in der Konfiguration angezeigt werden.

Dieses Diagramm zeigt die verschiedenen NAT-Abschnitte und ihre Anordnung:



NAT-Regelübereinstimmung

Abschnitt 1

- Ein Datenfluss wird zuerst anhand von Abschnitt 1 der NAT-Tabelle ausgewertet, der mit der ersten Regel beginnt.
  - Wenn die Quell- und Ziel-IP-Adresse des Pakets mit den Parametern der manuellen NAT-Regel übereinstimmen, wird die Übersetzung angewendet, der Prozess wird gestoppt, und es werden keine weiteren NAT-Regeln in einem Abschnitt ausgewertet.
  - Wenn keine NAT-Regel zugeordnet wird, wird der Datenfluss anhand von Abschnitt 2 der NAT-Tabelle ausgewertet.

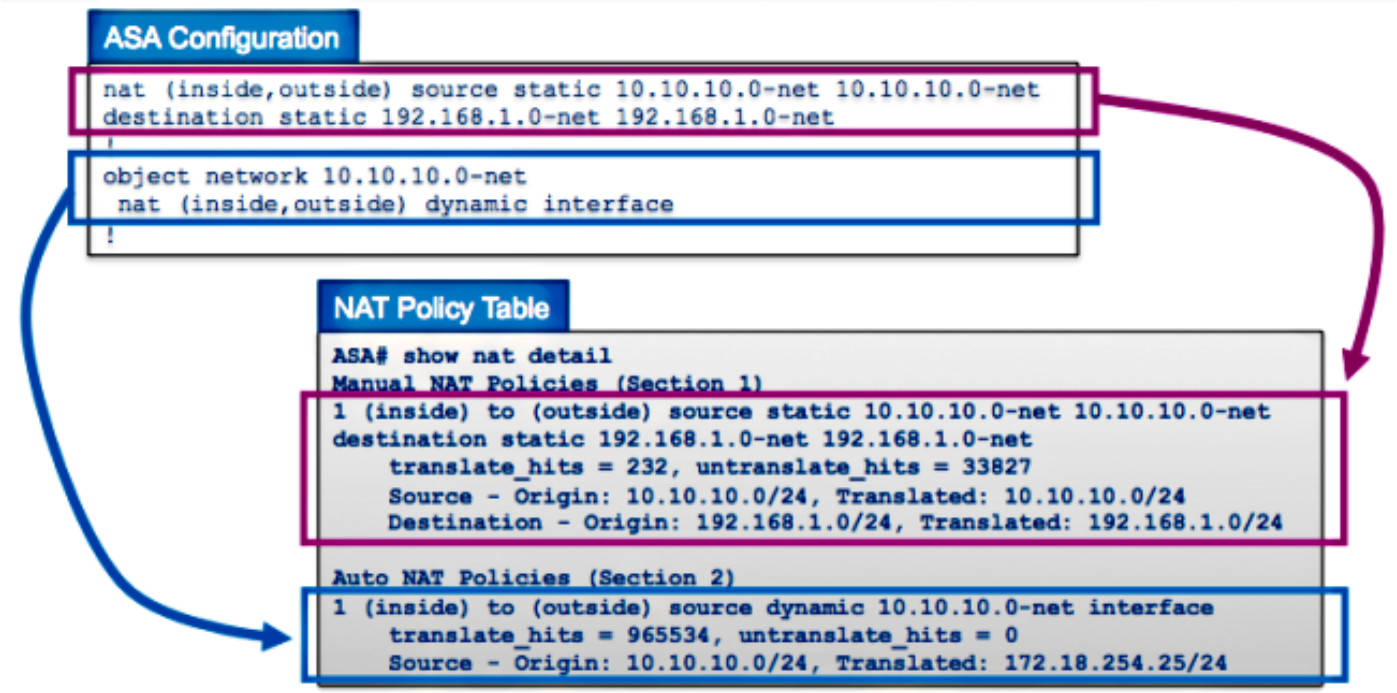
Abschnitt 2

- Ein Datenfluss wird anhand der NAT-Regeln von Abschnitt 2 in der zuvor angegebenen Reihenfolge ausgewertet, d. h. zuerst anhand der statischen NAT-Regeln und dann anhand der dynamischen NAT-Regeln.
  - Wenn eine Übersetzungsregel entweder mit der Quell- oder Ziel-IP-Adresse des Datenflusses übereinstimmt, kann die Übersetzung angewendet werden, und die übrigen Regeln können weiterhin ausgewertet werden, um festzustellen, ob sie mit der anderen IP-Adresse im Datenfluss übereinstimmen. Beispielsweise kann eine Auto-NAT-Regel die Quell-IP-Adresse und eine andere Auto-NAT-Regel das Ziel übersetzen.
  - Wenn der Datenfluss mit einer automatischen NAT-Regel übereinstimmt, wird die NAT-Suche gestoppt, wenn das Ende von Abschnitt 2 erreicht ist, und die Regeln in Abschnitt 3 werden nicht ausgewertet.
  - Wenn keine NAT-Regel aus Abschnitt 2 mit dem Datenfluss abgeglichen wird, wird die Suche nach Abschnitt 3 fortgesetzt.

Abschnitt 3

- Das Verfahren in Abschnitt 3 ist im Wesentlichen das gleiche wie in Abschnitt 1. Wenn die Quell- und Ziel-IP-Adresse des Pakets mit den Parametern der manuellen NAT-Regel übereinstimmen, wird die Übersetzung angewendet, der Prozess wird gestoppt, und es werden keine weiteren NAT-Regeln in einem Abschnitt ausgewertet.

Dieses Beispiel zeigt, wie die ASA NAT-Konfiguration mit zwei Regeln (eine manuelle NAT-Anweisung und eine automatische NAT-Konfiguration) in der NAT-Tabelle dargestellt wird:



Beheben von NAT-Problemen

Packet Tracer-Dienstprogramm verwenden

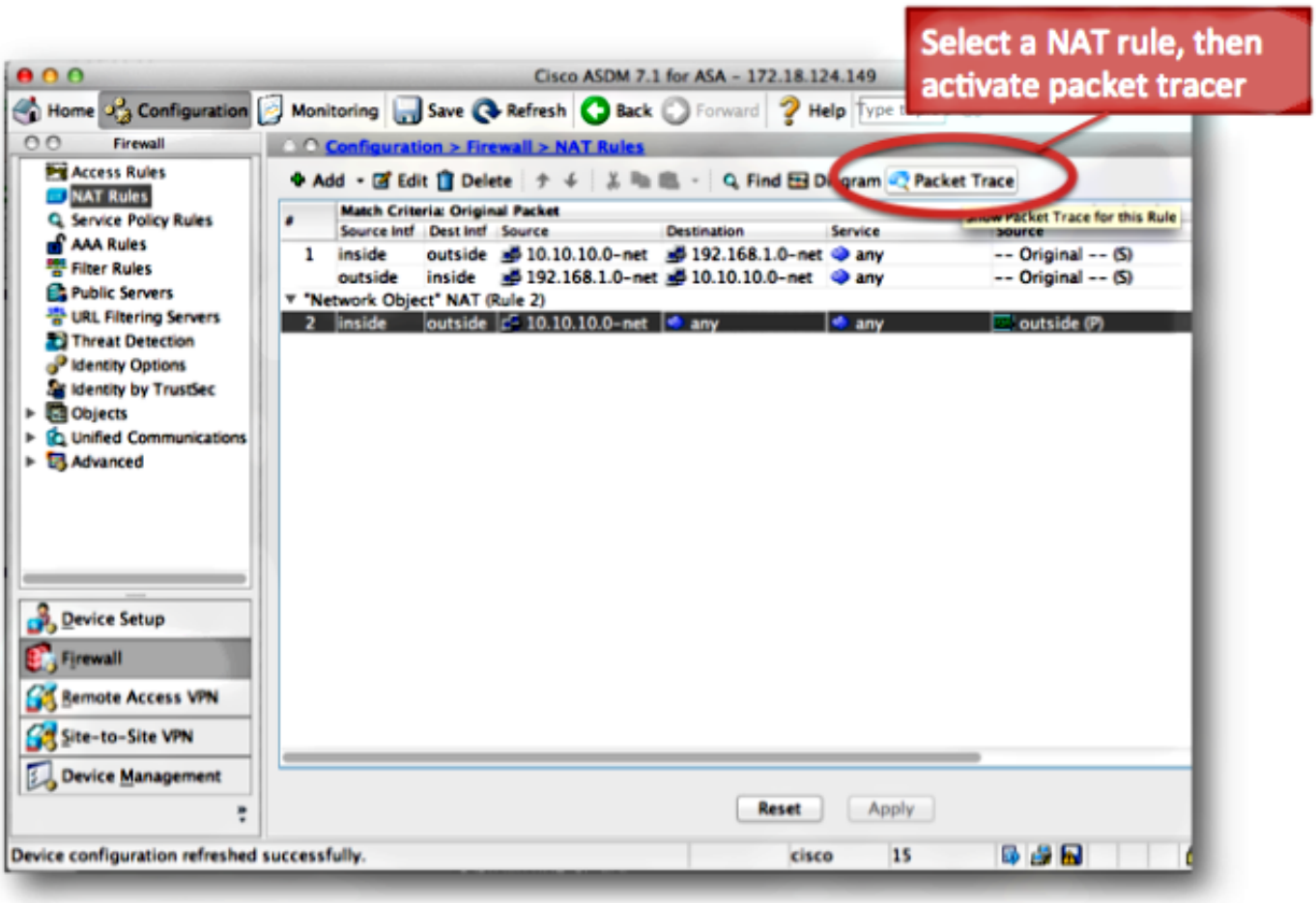
Um Probleme mit NAT-Konfigurationen zu beheben, verwenden Sie das Paket-Tracer-Dienstprogramm, um zu überprüfen, ob ein Paket die NAT-Richtlinie erreicht. Packet Tracer ermöglicht Ihnen die Angabe eines Beispielpakets, das an die ASA gesendet wird. Die ASA gibt an, welche Konfiguration auf das Paket angewendet wird und ob dies zulässig ist.

Im nächsten Beispiel wird ein Beispiel-TCP-Paket angegeben, das in die interne Schnittstelle gelangt und für einen Host im Internet bestimmt ist. Das Dienstprogramm zur Paketverfolgung zeigt an, dass das Paket mit einer dynamischen NAT-Regel übereinstimmt und in die externe IP-Adresse 172.16.123.4 übersetzt wird:

```
<#root>

ASA#

packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80


...(output omitted)...
```

```
Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:

object network 10.10.10.0-net
 nat (inside,outside) dynamic interface


Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow



ASA#
```

Wählen Sie die NAT-Regel aus, und klicken Sie auf Packet Trace (Paketverfolgung), um die Paketverfolgung im Cisco Adaptive Security Device Manager (ASDM) zu aktivieren. Dabei werden die in der NAT-Regel angegebenen IP-Adressen als Eingaben für das Tool zur Paketverfolgung verwendet:

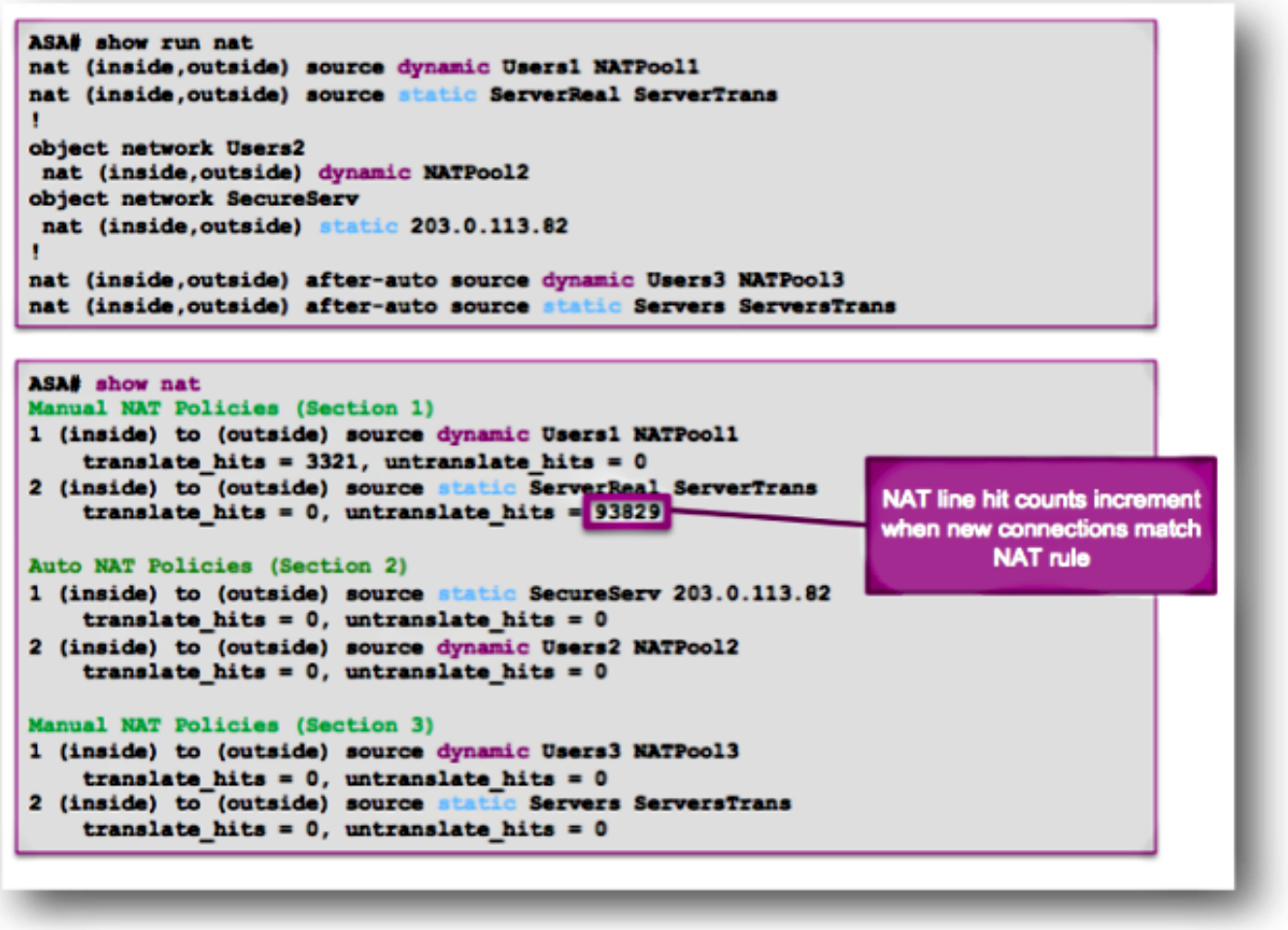


Anzeigen der Ausgabe des Befehls Show Nat

Die Ausgabe des Befehls show nat detail kann verwendet werden, um die NAT-Richtlinientabelle anzuzeigen. Insbesondere können die Zähler translate_hits und untranslate_hits verwendet werden, um zu bestimmen, welche NAT-Einträge auf dem ASA verwendet werden.

Wenn Sie feststellen, dass Ihre neue NAT-Regel keine translate_hits oder untranslate_hits enthält, bedeutet dies, dass entweder der Datenverkehr nicht an der ASA ankommt, oder dass eine andere Regel mit einer höheren Priorität in der NAT-Tabelle mit dem Datenverkehr übereinstimmt.

Nachfolgend sind die NAT-Konfiguration und die NAT-Richtlinientabelle einer anderen ASA-Konfiguration aufgeführt:



Im vorherigen Beispiel sind auf dieser ASA sechs NAT-Regeln konfiguriert. Die Ausgabe von show nat zeigt, wie diese Regeln zum Erstellen der NAT-Richtlinientabelle verwendet werden, sowie die Anzahl von translate_hits und untranslate_hits für jede Regel.

Diese Trefferzähler erhöhen sich nur einmal pro Verbindung. Nachdem die Verbindung über die ASA hergestellt wurde, erhöhen nachfolgende Pakete, die mit der aktuellen Verbindung übereinstimmen, die NAT-Leitungen nicht (ähnlich wie die Zugriffslisten-Trefferzählung auf der ASA).

Translate_hits: Die Anzahl neuer Verbindungen, die der NAT-Regel in Vorwärtsrichtung entsprechen.

"Weiterleitungsrichtung" bedeutet, dass die Verbindung über die ASA in Richtung der in der NAT-Regel angegebenen Schnittstellen aufgebaut wurde.

Wenn eine NAT-Regel angibt, dass der interne Server in die externe Schnittstelle übersetzt wird, lautet die Reihenfolge der Schnittstellen in der NAT-Regel "nat (inside,outside)...". Wenn dieser Server eine neue Verbindung zu einem Host außerhalb des Servers initiiert, wird der Zähler translate_hit inkrementiert.

Untranslate_hits: Die Anzahl der neuen Verbindungen, die der NAT-Regel in umgekehrter Richtung entsprechen.

Wenn eine NAT-Regel angibt, dass der interne Server in die externe Schnittstelle übersetzt wird, lautet die Reihenfolge der Schnittstellen in der NAT-Regel "nat (inside,outside)..."; wenn ein Client außerhalb der ASA eine neue Verbindung mit dem internen Server initiiert, wird der Zähler untranslate_hit inkrementiert.

Auch hier gilt: Wenn Sie feststellen, dass Ihre neue NAT-Regel keine translate_hits oder untranslate_hits hat, bedeutet dies, dass entweder der Datenverkehr nicht bei der ASA ankommt, oder dass eine andere Regel mit einer höheren Priorität in der NAT-Tabelle mit dem Datenverkehr übereinstimmt.

Methodik zur Behebung von NAT-Problemen

Verwenden Sie die Paketverfolgung, um sicherzustellen, dass ein Beispielpaket mit der korrekten NAT-Konfigurationsregel auf der ASA übereinstimmt. Verwenden Sie den Befehl show nat detail, um zu ermitteln, welche NAT-Richtlinienregeln betroffen sind. Wenn eine Verbindung mit einer anderen NAT-Konfiguration übereinstimmt als erwartet, beheben Sie den Fehler mit den folgenden Fragen:

- Gibt es eine andere NAT-Regel, die Vorrang vor der NAT-Regel hat, für die der Datenverkehr bestimmt war?
- Gibt es eine andere NAT-Regel mit zu breiten Objektdefinitionen (die Subnetzmaske ist zu kurz, z. B. 255.0.0.0), sodass dieser Datenverkehr mit der falschen Regel übereinstimmt?
- Stimmen die manuellen NAT-Richtlinien nicht überein, sodass das Paket mit der falschen Regel übereinstimmt?
- Ist Ihre NAT-Regel falsch konfiguriert, sodass die Regel nicht mit Ihrem Datenverkehr übereinstimmt?

Im nächsten Abschnitt finden Sie Beispiele für Probleme und Lösungen.

Häufige Probleme mit NAT-Konfigurationen

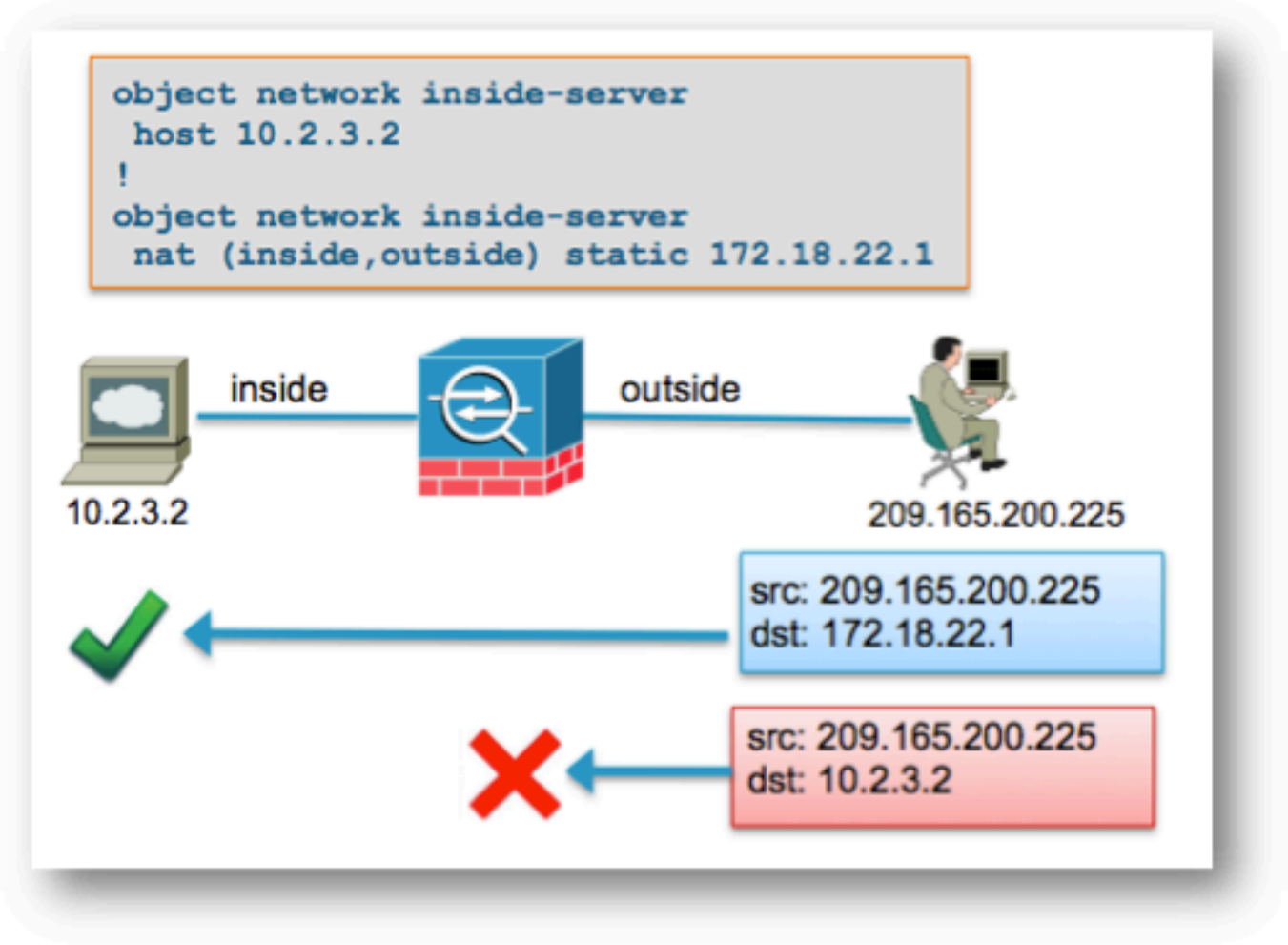
Nachfolgend sind einige häufige Probleme aufgeführt, die bei der Konfiguration von NAT auf der ASA auftreten können.

Problem: Datenverkehrsfehler aufgrund eines NAT-RPF-Fehlers (Reverse Path Failure): Asymmetrische NAT-Regeln wurden für Vorwärts- und Rückwärtsflüsse abgeglichen

Die NAT-RPF-Prüfung stellt sicher, dass eine Verbindung, die von der ASA in die Vorwärtsrichtung übersetzt wird, z. B. die TCP-Synchronisierung (SYN), durch dieselbe NAT-Regel in die Rückwärtsrichtung übersetzt wird, z. B. die TCP-SYN/Quittierung (ACK).

In der Regel wird dieses Problem durch eingehende Verbindungen verursacht, die an die lokale (unübersetzte) Adresse in einer NAT-Anweisung gerichtet sind. Grundsätzlich überprüft die NAT-RPF, ob die Verbindung vom Server zum Client in umgekehrter Richtung mit derselben NAT-Regel übereinstimmt. Wenn dies nicht der Fall ist, schlägt die NAT-RPF-Prüfung fehl.

Beispiel: 209.165.200.225



Wenn der externe Host unter 192.168.200.225 ein Paket direkt an die lokale (unübersetzte) IP-Adresse 10.2.3.2 sendet, verwirft die ASA das Paket und protokolliert dieses Syslog:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Lösung:

Stellen Sie zunächst sicher, dass der Host Daten an die richtige globale NAT-Adresse sendet. Wenn der Host Pakete an die richtige Adresse sendet, überprüfen Sie die NAT-Regeln, die von der Verbindung betroffen sind.

Überprüfen Sie, ob die NAT-Regeln korrekt definiert sind und ob die Objekte, auf die in den NAT-Regeln verwiesen wird, korrekt sind. Überprüfen Sie außerdem, ob die Reihenfolge der NAT-Regeln angemessen ist.

Verwenden Sie das Dienstprogramm zur Paketverfolgung, um die Details des abgelehnten Pakets

anzugeben. Die Paketverfolgung muss das wegen eines Fehlers bei der RPF-Prüfung verworfene Paket anzeigen.

Sehen Sie sich als Nächstes die Ausgabe des Packet Tracer an, um festzustellen, welche NAT-Regeln in der NAT- und der NAT-RPF-Phase betroffen sind.

Wenn ein Paket mit einer NAT-Regel in der NAT-RPF-Prüfphase übereinstimmt, die anzeigt, dass der Rückwärtsfluss eine NAT-Übersetzung auslösen würde, jedoch nicht mit einer Regel in der NAT-Phase übereinstimmt, die anzeigt, dass der Vorwärtsfluss KEINE NAT-Regel treffen würde, wird das Paket verworfen.

Diese Ausgabe entspricht dem Szenario aus dem vorherigen Diagramm, bei dem der externe Host den Datenverkehr fälschlicherweise an die lokale IP-Adresse des Servers und nicht an die globale (übersetzte) IP-Adresse sendet:

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Wenn das Paket an die korrekt zugeordnete IP-Adresse 172.18.22.1 gerichtet ist, stimmt das Paket mit der richtigen NAT-Regel in der UN-NAT-Phase in Vorwärtsrichtung überein. Dieselbe Regel gilt für die NAT-RPF-Prüfphase:

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
```

```
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:
```

ALLOW

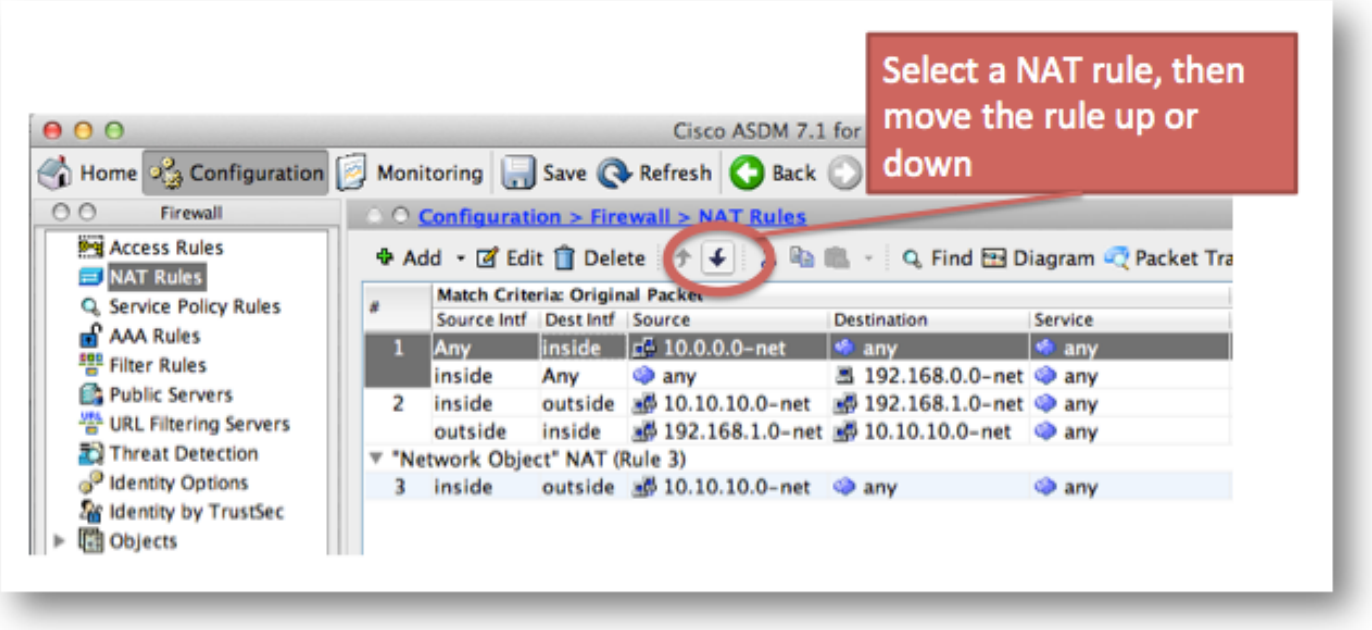
```
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

Problem: Manuelle NAT-Regeln sind defekt, was zu falschen Paketübereinstimmungen führt

Die manuellen NAT-Regeln werden auf Grundlage ihrer Darstellung in der Konfiguration verarbeitet. Wenn eine sehr weit gefasste NAT-Regel zuerst in der Konfiguration aufgeführt wird, kann sie eine weitere, spezifischere Regel weiter unten in der NAT-Tabelle außer Kraft setzen. Verwenden Sie den Packet Tracer, um zu überprüfen, welche NAT-Regel für Ihren Datenverkehr gilt. Möglicherweise müssen Sie die manuellen NAT-Einträge in eine andere Reihenfolge ändern.

Lösung:

NAT-Regeln mit ASDM neu anordnen



Lösung:

NAT-Regeln können über die CLI neu bestellt werden, wenn Sie die Regel entfernen und unter einer bestimmten Zeilennummer wieder einfügen. Um eine neue Regel in eine bestimmte Zeile einzufügen, geben Sie die Zeilennummer ein, nachdem die Schnittstellen angegeben wurden.

Beispiel:

<#root>

```
ASA(config)#
```

nat (inside,outside) *1* source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net

Problem

Eine NAT-Regel ist zu breit gefasst und gleicht einigen Datenverkehr versehentlich ab. Manchmal werden NAT-Regeln erstellt, die zu breite Objekte verwenden. Wenn diese Regeln oben in der NAT-Tabelle (z. B. oben in Abschnitt 1) platziert werden, können sie mehr Datenverkehr als geplant aufnehmen und dazu führen, dass keine weiteren NAT-Regeln in der Tabelle getroffen werden.

Lösung

Verwenden Sie die Paketverfolgung, um zu ermitteln, ob der Datenverkehr einer Regel mit zu breiten Objektdefinitionen entspricht. In diesem Fall müssen Sie den Umfang dieser Objekte reduzieren oder die Regeln weiter nach unten in der NAT-Tabelle oder in den After-Auto-Abschnitt (Abschnitt 3) der NAT-Tabelle verschieben.

Problem

Eine NAT-Regel leitet den Datenverkehr zu einer falschen Schnittstelle um. NAT-Regeln können Vorrang vor der Routing-Tabelle haben, wenn sie bestimmen, welche Schnittstelle ein Paket an die ASA übergibt. Wenn ein eingehendes Paket mit einer übersetzten IP-Adresse in einer NAT-Anweisung übereinstimmt, wird die NAT-Regel verwendet, um die Ausgangsschnittstelle zu bestimmen.

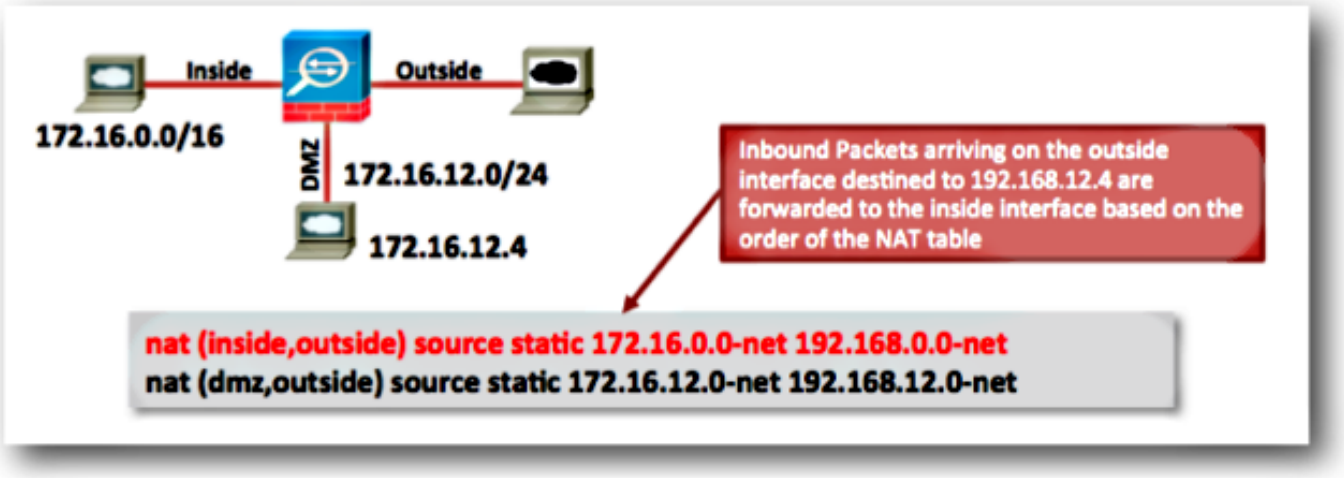
Die NAT-Umleitungsprüfung (die die Routing-Tabelle außer Kraft setzen kann) überprüft, ob eine NAT-Regel vorhanden ist, die die Zieladressenumwandlung für ein eingehendes Paket angibt, das an einer Schnittstelle eingeht.

Wenn es keine Regel gibt, die ausdrücklich festlegt, wie diese IP-Adresse des Paketziels übersetzt werden soll, wird die globale Routing-Tabelle zur Bestimmung der Ausgangsschnittstelle herangezogen.

Wenn es eine Regel gibt, die explizit angibt, wie die IP-Adresse des Paketziels übersetzt werden soll, zieht die NAT-Regel das Paket an die andere Schnittstelle in der Übersetzung, und die globale Routing-Tabelle wird effektiv umgangen.

Dieses Problem tritt am häufigsten bei eingehendem Datenverkehr auf, der an der externen Schnittstelle eingeht, und ist in der Regel auf unzulässige NAT-Regeln zurückzuführen, die Datenverkehr an unbeabsichtigte Schnittstellen umleiten.

Beispiel:



Lösungen:

Dieses Problem kann mit einer der folgenden Aktionen behoben werden:

- Ordnen Sie die NAT-Tabelle so an, dass der spezifischere Eintrag zuerst aufgeführt wird.
- Verwenden Sie nicht überlappende globale IP-Adressbereiche für die NAT-Anweisungen.

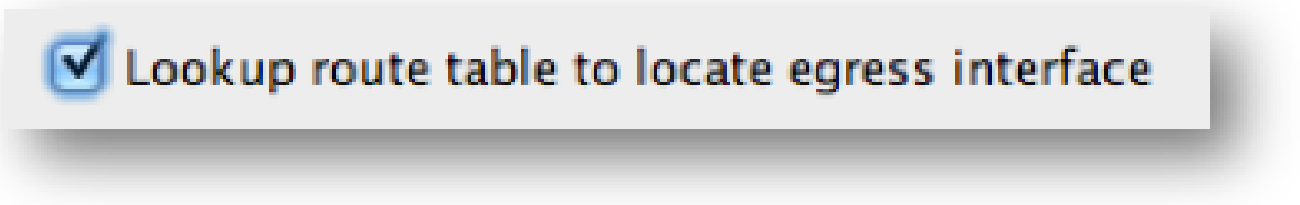
Wenn die NAT-Regel eine Identitätsregel ist (d. h. die IP-Adressen werden durch die Regel nicht geändert), kann das route-lookup-Schlüsselwort verwendet werden (dieses Schlüsselwort gilt nicht

für das vorherige Beispiel, da die NAT-Regel keine Identitätsregel ist).

Das route-lookup-Schlüsselwort veranlasst die ASA, eine zusätzliche Prüfung durchzuführen, wenn sie mit einer NAT-Regel übereinstimmt. Es wird geprüft, ob die Routing-Tabelle der ASA das Paket an die gleiche Ausgangsschnittstelle weiterleitet, an die es durch diese NAT-Konfiguration umgeleitet wird.

Wenn die Ausgangsschnittstelle der Routing-Tabelle nicht mit der NAT-Umleitungsschnittstelle übereinstimmt, wird die NAT-Regel nicht zugeordnet (die Regel wird übersprungen), und das Paket wird in der NAT-Tabelle weiter nach unten weitergeleitet, um von einer späteren NAT-Regel verarbeitet zu werden.

Die Route-Lookup-Option ist nur verfügbar, wenn es sich bei der NAT-Regel um eine NAT-Identitätsregel handelt, d. h. die IP-Adressen werden durch die Regel nicht geändert. Die Route-Lookup-Option kann per NAT-Regel aktiviert werden, wenn Sie die Route-Lookup-Funktion am Ende der NAT-Leitung hinzufügen oder das Kontrollkästchen Lookup route table to locate egress interface in der NAT-Regelkonfiguration in ASDM aktivieren:



Problem: Eine NAT-Regel veranlasst die ASA, das Address Resolution Protocol (ARP) für den Datenverkehr auf der zugeordneten Schnittstelle zu proxy.

Die ASA-Proxy-ARPs für den globalen IP-Adressbereich in einer NAT-Anweisung auf der globalen Schnittstelle. Diese Proxy-ARP-Funktion kann für jede NAT-Regel deaktiviert werden, wenn Sie das Schlüsselwort no-proxy-arp zur NAT-Anweisung hinzufügen.

Dieses Problem tritt auch dann auf, wenn das globale Adressen-Subnetz versehentlich viel größer erstellt wird, als es eigentlich sein sollte.

Lösung

Fügen Sie das Schlüsselwort no-proxy-arp zur NAT-Zeile hinzu, wenn möglich.

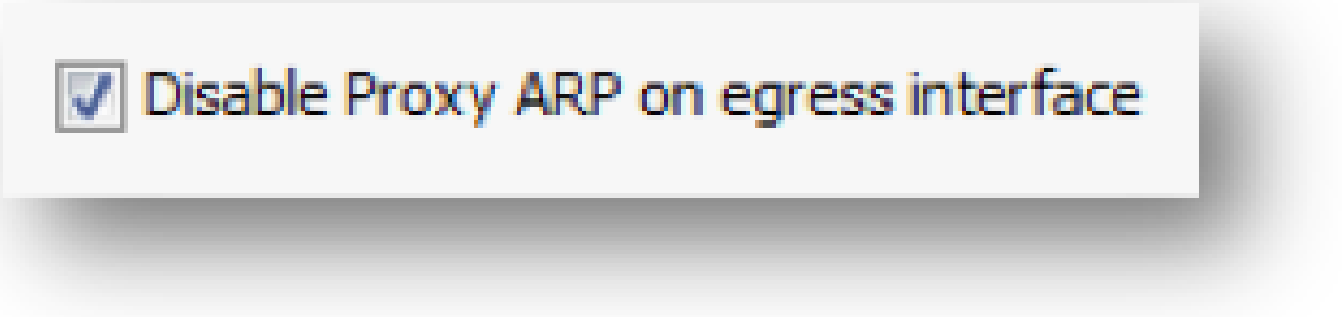
Beispiel:

<#root>

```
ASA(config)#

object network inside-server

ASA(config-network-object)#
```

```
nat (inside,outside) static 172.18.22.1 no-proxy-arp


ASA(config-network-object)#

end


ASA#
  ASA#

 show run nat


object network inside-server
 nat (inside,outside) static 172.18.22.1

no-proxy-arp


ASA#
```

Dies ist auch mit ASDM möglich. Aktivieren Sie in der NAT-Regel das Kontrollkästchen Disable Proxy ARP on Egress Interface (Proxy-ARP an Egress-Schnittstelle deaktivieren).



.

Zugehörige Informationen

- VIDEO: ASA-Port Forwarding für DMZ-Serverzugriff (Versionen 8.3 und 8.4)
- Grundlegende ASA NAT-Konfiguration: Webserver in der DMZ in ASA Version 8.3 und höher
- Buch 2: Konfigurationsleitfaden für die Firewall-CLI der Cisco ASA-Serie, 9.1
- 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.