Häufig gestellte Fragen zu Network Address Translation (NAT)

Inhalt

Einleitung

Dieses Dokument enthält Antworten auf häufig gestellte Fragen zur Network Address Translation (NAT).

Allgemeine NAT

Frage: Was ist NAT?

A. Network Address Translation (NAT) wurde für die Erhaltung von IP-Adressen entwickelt. Es ermöglicht privaten IP-Netzwerken, die nicht registrierte IP-Adressen verwenden, eine Verbindung zum Internet herzustellen. NAT arbeitet auf einem Router, der normalerweise zwei Netzwerke miteinander verbindet, und übersetzt die privaten (nicht global eindeutigen) Adressen im internen Netzwerk in gültige Adressen, bevor Pakete an ein anderes Netzwerk weitergeleitet werden.

Im Rahmen dieser Funktion kann NAT so konfiguriert werden, dass der Außenwelt nur eine Adresse für das gesamte Netzwerk angekündigt wird. Dies erhöht die Sicherheit, da das gesamte interne Netzwerk hinter dieser Adresse verborgen wird. NAT bietet die doppelte Funktionalität von Sicherheit und Adresserhaltung und wird in der Regel in Remote-Zugriffsumgebungen implementiert.

F. Wie funktioniert NAT?

A. Grundsätzlich ermöglicht NAT einem einzelnen Gerät, wie einem Router, als Agent zwischen dem Internet (oder öffentlichen Netzwerk) und einem lokalen Netzwerk (oder privaten Netzwerk) zu agieren, was bedeutet, dass nur eine einzige eindeutige IP-Adresse erforderlich ist, um eine

ganze Gruppe von Computern für etwas außerhalb ihres Netzwerks darzustellen.

Frage: Wie konfiguriere ich NAT?

A. Um herkömmliche NAT zu konfigurieren, müssen Sie mindestens eine Schnittstelle auf einem Router (NAT extern) und eine weitere Schnittstelle auf dem Router (NAT intern) sowie einen Satz von Regeln für die Übersetzung der IP-Adressen in den Paket-Headern (und Payloads, falls gewünscht) konfigurieren. Für die Konfiguration der virtuellen NAT-Schnittstelle (NAT Virtual Interface, NVI) ist mindestens eine Schnittstelle erforderlich, für die NAT aktiviert wurde. Außerdem müssen die oben genannten Regeln eingehalten werden.

Weitere Informationen finden Sie im Cisco IOS IP Addressing Services Configuration Guide oder Configuring the NAT Virtual Interface.

F. Worin bestehen die Hauptunterschiede zwischen der Cisco IOS®-Software und der Cisco PIX Security Appliance-Implementierung von NAT?

A.: Die softwarebasierte Cisco IOS NAT unterscheidet sich nicht grundlegend von der NAT-Funktion der Cisco PIX Security Appliance. Die Hauptunterschiede bestehen in den verschiedenen Datenverkehrstypen, die in den Implementierungen unterstützt werden. Weitere Informationen zur Konfiguration von NAT auf Cisco PIX-Geräten (einschließlich der unterstützten Datenverkehrstypen) finden Sie unter NAT-Konfigurationsbeispiele.

Frage: Auf welcher Cisco Routing-Hardware ist Cisco IOS NAT verfügbar? Wie kann die Hardware bestellt werden?

A.: Mit dem Cisco Feature Navigator können Kunden eine Funktion (NAT) identifizieren und feststellen, für welche Version und welche Hardwareversion diese Cisco IOS Software-Funktion verfügbar ist. Informationen zur Verwendung dieses Tools finden Sie im Cisco Feature Navigator.

Frage: Kommt NAT vor oder nach dem Routing vor?

A. Die Reihenfolge, in der die Transaktionen mithilfe von NAT verarbeitet werden, hängt davon ab, ob ein Paket vom internen Netzwerk zum externen Netzwerk oder vom externen Netzwerk zum internen Netzwerk gelangt. Die Umwandlung von innen nach außen erfolgt nach dem Routing, die Umwandlung von außen nach innen vor dem Routing. Weitere Informationen finden Sie unter NAT Order of Operation (NAT-Reihenfolge der Vorgänge).

Frage: Kann NAT in einer öffentlichen WLAN-Umgebung bereitgestellt werden?

Antwort: Ja. Die Funktion NAT - Static IP Support unterstützt Benutzer mit statischen IP-Adressen, sodass diese eine IP-Sitzung in einer öffentlichen Wireless LAN-Umgebung einrichten können.

Frage: Führt NAT einen TCP-Lastenausgleich für Server im internen Netzwerk durch?

Antwort: Ja. Mithilfe von NAT können Sie einen virtuellen Host im internen Netzwerk einrichten, der die Lastverteilung zwischen realen Hosts koordiniert.

Frage: Kann ich die Anzahl der NAT-Übersetzungen mit einer Rate begrenzen?

Antwort: Ja. Die Funktion zur RATE-basierten Übersetzung bietet die Möglichkeit, die maximale Anzahl gleichzeitiger NAT-Vorgänge auf einem Router zu begrenzen. Zusätzlich zur besseren Kontrolle über die Verwendung von NAT-Adressen kann die Funktion zur verzögerungsfreien NAT-Übersetzung eingesetzt werden, um die Auswirkungen von Viren, Würmern und Denial-of-Service-Angriffen zu begrenzen.

Frage: Wie wird das Routing für IP-Subnetze oder -Adressen gelernt oder propagiert, die von NAT verwendet werden?

A. Das Routing für von NAT erstellte IP-Adressen wird in folgenden Fällen abgefragt:

- Der interne globale Adresspool wird vom Subnetz eines Next-Hop-Routers abgeleitet.
- Der statische Routeneintrag wird auf dem Next-Hop-Router konfiguriert und im Routing-Netzwerk neu verteilt.

Wenn die interne globale Adresse mit der lokalen Schnittstelle abgeglichen wird, installiert NAT einen IP-Alias und einen ARP-Eintrag. In diesem Fall führt der Router **Proxy-ARP** für diese Adressen aus. Wenn dieses Verhalten nicht erwünscht ist, verwenden Sie das Schlüsselwort *no-alias*.

Wenn ein NAT-Pool konfiguriert ist, kann die *Add-Route*-Option für die automatische Routen-Einschleusung verwendet werden.

Frage: Wie viele parallele NAT-Sitzungen werden in Cisco IOS NAT unterstützt?

Antwort: Der Grenzwert für NAT-Sitzungen wird durch den verfügbaren DRAM im Router begrenzt. Jede NAT-Übersetzung nimmt in DRAM etwa 312 Byte auf. 10.000 Übersetzungen (mehr, als normalerweise auf einem einzigen Router bearbeitet würden) benötigen demnach etwa 3 MB. Aus diesem Grund verfügt eine typische Routing-Hardware über mehr als genug Speicher, um Tausende von NAT-Übersetzungen zu unterstützen.

Frage: Welche Routing-Leistung kann bei Verwendung von Cisco IOS NAT erwartet werden?

A.: Cisco IOS NAT unterstützt Cisco Express Forwarding Switching, Fast Switching und Process Switching. Ab Version 12.4T wird Fast Switching Path nicht mehr unterstützt. Für die Cat6k-Plattform ist die Switching-Reihenfolge Netflow (HW-Switching-Pfad), CEF, Process Path.

Die Leistung hängt von mehreren Faktoren ab:

- Die Art der Anwendung und die Art des Datenverkehrs
- Ob IP-Adressen eingebettet sind
- Austausch und Prüfung mehrerer Nachrichten
- Quell-Port erforderlich
- Die Anzahl der Übersetzungen
- Andere Anwendungen, die zu diesem Zeitpunkt ausgeführt werden
- Der Typ der Hardware und des Prozessors

Frage: Kann Cisco IOS NAT auf Subschnittstellen angewendet werden?

Antwort: Ja. Quell- und/oder Ziel-NAT-Übersetzungen können auf alle Schnittstellen oder Subschnittstellen mit einer IP-Adresse angewendet werden (einschließlich Dialer-Schnittstellen). NAT kann nicht mit einer virtuellen Wireless-Schnittstelle konfiguriert werden. Die virtuelle Wireless-Schnittstelle ist zum Zeitpunkt des Schreibens in den NVRAM nicht vorhanden. Daher verliert der Router nach dem Neustart die NAT-Konfiguration auf der virtuellen Wireless-Schnittstelle.

Frage: Kann Cisco IOS NAT mit Hot Standby Router Protocol (HSRP) verwendet werden, um redundante Verbindungen zu einem ISP bereitzustellen?

Antwort: Ja. NAT bietet ein redundantes HSRP. Sie unterscheidet sich jedoch von SNAT (Stateful NAT). NAT mit HSRP ist ein Stateless-System. Die aktuelle Sitzung wird nicht aufrechterhalten, wenn ein Fehler auftritt. Während der statischen NAT-Konfiguration (wenn ein Paket keiner STATIC-Regelkonfiguration entspricht) wird das Paket ohne Übersetzung durchgestellt.

Frage: Unterstützt Cisco IOS NAT eingehende Übersetzungen auf einer Frame Relay-Schnittstelle? Werden ausgehende Übersetzungen auf der Ethernet-Seite unterstützt?

Antwort: Ja. Die Kapselung spielt bei NAT keine Rolle. NAT kann durchgeführt werden, wenn eine Schnittstelle über eine IP-Adresse verfügt und die Schnittstelle "NAT inside" oder "NAT outside" ist. NAT muss innen und außen funktionieren. Wenn Sie NVI verwenden, muss mindestens eine NAT-fähige Schnittstelle vorhanden sein. Siehe Wie konfiguriere ich NAT? für weitere Informationen.

Frage: Kann ein einzelner NAT-fähiger Router es einigen Benutzern ermöglichen, NAT zu verwenden, und anderen Benutzern, die sich auf derselben Ethernet-Schnittstelle befinden, weiterhin ihre eigenen IP-Adressen?

Antwort: Ja. Dies kann durch die Verwendung einer Zugriffsliste erreicht werden, die den Satz von Hosts oder Netzwerken beschreibt, die NAT erfordern. Alle Sitzungen auf demselben Host werden entweder übersetzt oder über den Router weitergeleitet und nicht übersetzt.

Zugriffslisten, erweiterte Zugriffslisten und Routenpläne können verwendet werden, um *Regeln* zu definieren, nach denen IP-Geräte übersetzt werden. Die Netzwerkadresse und die entsprechende Subnetzmaske müssen immer angegeben werden. Das Schlüsselwort *any* darf nicht anstelle der Netzwerkadresse oder Subnetzmaske verwendet werden. Bei einer statischen NAT-Konfiguration werden Pakete, die keiner statischen Regelkonfiguration entsprechen, ohne Übersetzung durchgestellt.

Frage: Wie viele Übersetzungen können maximal pro globaler IP-Adresse erstellt werden, wenn PAT konfiguriert wird (Überlastung)?

A. PAT (overloading) unterteilt die verfügbaren Ports pro globaler IP-Adresse in drei Bereiche: 0-511, 512-1023 und 1024-65535. PAT weist jeder UDP- oder TCP-Sitzung einen eindeutigen Quellport zu. Es wird versucht, den gleichen Port-Wert der ursprünglichen Anforderung zuzuweisen. Wenn der ursprüngliche Quell-Port jedoch bereits verwendet wurde, beginnt der Scanvorgang am Anfang des bestimmten Port-Bereichs, um den ersten verfügbaren Port zu

finden, und weist ihn der Konversation zu. Es gibt eine Ausnahme für die Codebasis 12.2S. 12.2S-CodeBase verwendet eine andere Port-Logik, und es gibt keine Port-Reservierung.

F. Wie funktioniert PAT?

A. PAT funktioniert entweder mit einer globalen IP-Adresse oder mit mehreren Adressen.

PAT mit einer IP-Adresse

Bedingung	Beschreibung
1	NAT/PAT überprüft den Datenverkehr und ordnet ihn einer Übersetzungsregel zu.
2	Die Regel entspricht einer PAT-Konfiguration.
3	Wenn PAT den Datenverkehrstyp kennt und wenn dieser Datenverkehrstyp über "einen Satz spezifischer Ports oder Ports, die er aushandelt" verfügt, die er verwenden wird, legt PAT diese beiseite und weist sie nicht als eindeutige Kennungen zu.
4	Wenn eine Sitzung ohne spezielle Port-Anforderungen versucht, eine Verbindung herzustellen, übersetzt PAT die IP-Quelladresse und überprüft die Verfügbarkeit des ursprünglichen Quell-Ports (z. B. 433). **Hinweis:** Für das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP) sind die Bereiche: 1-511, 512-1023, 1024-65535. Bei Internet Control Message Protocol (ICMP) beginnt die erste Gruppe bei 0.
5	Wenn der angeforderte Quellport verfügbar ist, weist die PAT den Quellport zu, und die Sitzung wird fortgesetzt.
6	Wenn der angeforderte Quellport nicht verfügbar ist, beginnt PAT mit der Suche am Anfang der entsprechenden Gruppe (beginnend bei 1 für TCP- oder UDP-Anwendungen und von 0 für ICMP).
7	Wenn ein Port verfügbar ist, wird er zugewiesen, und die Sitzung wird fortgesetzt.
8	Wenn keine Ports verfügbar sind, wird das Paket verworfen.

PAT mit mehreren IP-Adressen

Bedingung	Beschreibung
1-7	Die ersten sieben Bedingungen entsprechen denen einer einzelnen IP-Adresse.

8	Wenn in der entsprechenden Gruppe keine Ports für die erste IP-Adresse verfügbar sind, geht NAT zur nächsten IP-Adresse im Pool über und versucht, den ursprünglich angeforderten Quell-Port zuzuweisen.
9	Wenn der angeforderte Quellport verfügbar ist, weist NAT den Quellport zu und die Sitzung wird fortgesetzt.
10	Wenn der angeforderte Quell-Port nicht verfügbar ist, beginnt NAT mit der Suche am Anfang der entsprechenden Gruppe (beginnend bei 1 für TCP- oder UDP-Anwendungen und von 0 für ICMP).
11	Wenn ein Port verfügbar ist, wird dieser zugewiesen und die Sitzung wird fortgesetzt.
12	Wenn keine Ports verfügbar sind, wird das Paket verworfen, es sei denn, es ist eine andere IP-Adresse im Pool verfügbar.

Frage: Was sind NAT-IP-Pools?

A.: NAT-IP-Pools sind ein Bereich von IP-Adressen, die bei Bedarf für die NAT-Umwandlung zugewiesen werden. Zum Definieren eines Pools wird der Konfigurationsbefehl verwendet:

ip nat pool <*name*> <*start-ip*> <*end-ip*> **{netmask** <*netmask*> | **prefix-length** <*prefix-length*>**} [type {rotary}]**

Beispiel 1

Das folgende Beispiel wird zwischen internen Hosts, die entweder vom Netzwerk 192.168.1.0 oder 192.168.2.0 adressiert sind, in das global eindeutige Netzwerk 10.69.233.208/28 übersetzt:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Beispiel 2

Im folgenden Beispiel soll eine virtuelle Adresse definiert werden, deren Verbindungen auf einen Satz echter Hosts verteilt sind. Der Pool definiert die Adressen der echten Hosts. Die Zugriffsliste definiert die virtuelle Adresse. Wenn noch keine Übersetzung existiert, werden TCP-Pakete von der seriellen Schnittstelle 0 (der externen Schnittstelle), deren Ziel mit der Zugriffsliste übereinstimmt, in eine Adresse aus dem Pool umgewandelt.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

Frage: Wie viele NAT-IP-Pools können maximal konfiguriert werden (ip nat pool "name")?

Antwort: In der Praxis ist die maximale Anzahl konfigurierbarer IP-Pools durch die im jeweiligen Router verfügbare Menge an DRAM begrenzt. (Cisco empfiehlt, eine Poolgröße von 255 zu konfigurieren.) Jeder Pool darf maximal 16 Bit umfassen. Ab Version 12.4(11)T führt IOS die CCE (Common Classification Engine) ein. Dadurch wurde NAT auf maximal 255 Pools begrenzt. In der 12.2S-Codebasis gibt es keine Einschränkung hinsichtlich der maximalen Pools.

Frage: Was ist der Vorteil von route-map und ACL in einem NAT-Pool?

A. Eine Routenübersicht schützt unerwünschte externe Benutzer, um zu den internen Benutzern/Servern zu gelangen. Darüber hinaus kann basierend auf der Regel eine einzelne interne IP-Adresse verschiedenen internen globalen Adressen zugeordnet werden. Weitere Informationen finden Sie unter NAT Support for Multiple Pools Using Route Maps (NAT-Unterstützung für mehrere Pools mit Routenzuordnungen).

Frage: Was bedeutet "Überlappung" von IP-Adressen im Kontext von NAT?

A. Überlappende IP-Adressen beziehen sich auf eine Situation, in der zwei Standorte, die eine Verbindung herstellen möchten, beide dasselbe IP-Adressschema verwenden. Dies ist kein ungewöhnliches Ereignis; Es kommt häufig vor, wenn Unternehmen fusionieren oder übernommen werden. Ohne spezielle Unterstützung können sich die beiden Standorte nicht miteinander verbinden und Sitzungen aufbauen. Bei der überlappenden IP-Adresse kann es sich um eine öffentliche Adresse handeln, die einem anderen Unternehmen zugewiesen wurde, um eine private Adresse, die einem anderen Unternehmen zugewiesen wurde, oder um eine Adresse aus dem in RFC 1918 definierten Bereich privater Adressen .

Private IP-Adressen können nicht geroutet werden und erfordern NAT-Übersetzungen, um Verbindungen mit der Außenwelt zu ermöglichen. Die Lösung umfasst das Abfangen von DNS-Namensabfragemöglichkeiten von außen nach innen, das Einrichten einer Übersetzung für die externe Adresse und das Reparieren der DNS-Antwort, bevor diese an den internen Host weitergeleitet wird. Ein DNS-Server muss auf beiden Seiten des NAT-Geräts vorhanden sein, damit Benutzer, die eine Verbindung zwischen beiden Netzwerken wünschen, eine Lösung erhalten.

NAT ist in der Lage, den Inhalt von DNS-*A*- und *PTR*-Datensätzen zu überprüfen und eine Adressumwandlung durchzuführen, wie in Using NAT in Overlapping Networks (Überlappende Netzwerke) dargestellt.

F. Was sind statische NAT-Übersetzungen?

A. Statische NAT-Übersetzungen weisen eine 1:1-Zuordnung zwischen lokalen und globalen Adressen auf. Benutzer können auch statische Adressumsetzungen auf Port-Ebene konfigurieren und den Rest der IP-Adresse für andere Umsetzungen verwenden. Dies geschieht in der Regel bei der Port Address Translation (PAT).

Das folgende Beispiel zeigt die Konfiguration von routemap, um die Umwandlung von Außen nach Innen für statische NAT zu ermöglichen:

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
```

F. Was versteht man unter NAT-*Überlastung*? ist dies PAT?

Antwort: Ja. NAT-Überlastung ist PAT, d. h. die Verwendung eines Pools mit einem Bereich von einer oder mehreren Adressen oder die Verwendung einer Schnittstellen-IP-Adresse in Kombination mit dem Port. Wenn Sie überladen, erstellen Sie eine vollständig erweiterte Übersetzung. Hierbei handelt es sich um einen Eintrag in der Übersetzungstabelle, der die IP-Adresse und die Quell-/Ziel-Port-Informationen enthält. Diese werden üblicherweise als PAT (Overloading) bezeichnet.

PAT (oder Overloading) ist eine Funktion von Cisco IOS NAT, mit der *interne (*interne lokale) private Adressen in eine oder mehrere *externe (*interne globale, üblicherweise registrierte) IP-Adressen übersetzt werden. Eindeutige Quell-Port-Nummern bei jeder Übersetzung werden verwendet, um zwischen den Gesprächen zu unterscheiden.

F. Was sind dynamische NAT-Übersetzungen?

A. Bei dynamischen NAT-Übersetzungen können Benutzer eine dynamische Zuordnung zwischen lokalen und globalen Adressen einrichten. Die dynamische Zuordnung erfolgt durch Definition der zu übersetzenden lokalen Adressen und des Adresspools oder der Schnittstellen-IP-Adresse, aus dem bzw. der die globalen Adressen zugewiesen werden sollen, sowie durch Zuordnung der beiden Adressen.

F. Was ist ALG?

A. ALG ist ein Application Layer Gateway (ALG). NAT führt einen Übersetzungsdienst für jeden TCP/UDP-Datenverkehr (Transmission Control Protocol/User Datagram Protocol) durch, der keine Quell- und/oder Ziel-IP-Adressen im Anwendungsdatenstrom überträgt.

Diese Protokolle umfassen FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, Telnet, Archiv, finger, NTP, NFS, rlogin, rsh, rcp. Für bestimmte Protokolle, die IP-Adressinformationen in die Nutzlast einbetten, ist die Unterstützung eines Application Level Gateway (ALG) erforderlich.

Weitere Informationen finden Sie unter Using Application Level Gateways with NAT (Verwenden von Gateways auf Anwendungsebene mit NAT).

Frage: Ist es möglich, eine Konfiguration mit statischen und dynamischen NAT-Übersetzungen zu erstellen?

Antwort: Ja. Dieselbe IP-Adresse kann jedoch nicht für die statische NAT-Konfiguration oder im Pool für die dynamische NAT-Konfiguration verwendet werden. Alle öffentlichen IP-Adressen müssen eindeutig sein. Beachten Sie, dass globale Adressen, die in statischen Übersetzungen verwendet werden, nicht automatisch ausgeschlossen werden, wenn dynamische Pools dieselben globalen Adressen enthalten. Dynamische Pools müssen erstellt werden, um von statischen Einträgen zugewiesene Adressen auszuschließen. Weitere Informationen finden Sie unter Konfigurieren statischer und dynamischer NAT gleichzeitig.

Frage: Wenn eine Traceroute über einen NAT-Router durchgeführt wird, sollte die Traceroute die NAT-Global-Adresse anzeigen, oder sollte sie die NAT-Local-Adresse preisgeben?

A. Traceroute von außen sollte immer die globale Adresse zurückgeben.

Frage: Wie weist PAT einen Port zu?

A. NAT bietet zusätzliche Port-Funktionen: Port-Map.

- Bei "Full-range" kann NAT alle Ports unabhängig vom Standard-Port-Bereich verwenden.
- Port-Map ermöglicht NAT das Reservieren eines benutzerdefinierten Port-Bereichs für eine bestimmte Anwendung.

Weitere Informationen finden Sie unter Benutzerdefinierte Quellportbereiche für PAT.

Ab Version 12.4(20)T2 führt NAT eine Port-Randomisierung für L3/L4 und symmetrische Ports ein.

- Die Port-Randomisierung ermöglicht NAT die zufällige Auswahl eines beliebigen globalen Ports für die Quell-Port-Anforderung.
- Symmetric-port ermöglicht NAT die *endpunktunabhängige* Unterstützung.

F. Was ist der Unterschied zwischen IP-Fragmentierung und TCP-Segmentierung?

A. Die IP-Fragmentierung erfolgt auf Layer 3 (IP). Die TCP-Segmentierung erfolgt auf Layer 4 (TCP). IP-Fragmentierung tritt auf, wenn Pakete, die größer als die Maximum Transmission Unit (MTU) einer Schnittstelle sind, von dieser Schnittstelle gesendet werden. Diese Pakete müssen entweder fragmentiert oder verworfen werden, wenn sie über die Schnittstelle gesendet werden. Wenn das Don't Fragment (DF)-Bit nicht im IP-Header des Pakets festgelegt ist, wird das Paket fragmentiert. Wenn das DF-Bit im IP-Header des Pakets festgelegt ist, wird das Paket verworfen, und dem Sender wird eine ICMP-Fehlermeldung mit dem Next-Hop-MTU-Wert zurückgegeben. Alle Fragmente eines IP-Pakets enthalten dieselbe Ident-Nummer im IP-Header, sodass der Empfänger die Fragmente wieder in das ursprüngliche IP-Paket einbauen kann. Weitere Informationen finden Sie unter Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec (Lösen von IP-Fragmentierung, MTU, MSS und PMTUD-Problemen mit GRE und IPsec).

Die TCP-Segmentierung findet statt, wenn eine Anwendung auf einer Endstation Daten sendet. Die Anwendungsdaten werden in Abschnitte unterteilt, die TCP als am besten dimensioniert

ansieht. Diese von TCP an IP weitergeleitete Dateneinheit wird als Segment bezeichnet. TCP-Segmente werden in IP-Datagrammen gesendet. Diese IP-Datagramme können dann zu IP-Fragmenten werden, wenn sie das Netzwerk durchlaufen und auf Verbindungen mit niedrigerer MTU stoßen, als sie durchlaufen können.

TCP segmentiert diese Daten zunächst in TCP-Segmente (basierend auf dem TCP-MSS-Wert) und fügt den TCP-Header hinzu und übergibt dieses TCP-Segment an IP. Anschließend fügt IP einen IP-Header hinzu, um das Paket an den Remote-End-Host zu senden. Wenn das IP-Paket mit dem TCP-Segment größer ist als die IP-MTU an einer ausgehenden Schnittstelle auf dem Pfad zwischen den TCP-Hosts, fragmentiert die IP-Adresse das IP/TCP-Paket, um es anzupassen. Diese IP-Paketfragmente werden auf dem Remote-Host von der IP-Schicht wieder zusammengesetzt, und das gesamte TCP-Segment (das ursprünglich gesendet wurde) wird an die TCP-Schicht übergeben. Die TCP-Schicht hat keine Ahnung, dass die IP das Paket während der Übertragung fragmentiert hatte.

NAT unterstützt IP-Fragmente, aber keine TCP-Segmente.

Frage: Unterstützt NAT Out-of-Order-Vorgänge für die IP-Fragmentierung und TCP-Segmentierung?

A. NAT unterstützt aufgrund der **virtuellen Reassemblierung** der **IP** nur Out-of-Order-IP-Fragmente.

F. Wie debugge ich IP-Fragmentierung und TCP-Segmentierung?

A. NAT verwendet dieselbe Debug-CLI für die IP-Fragmentierung und die TCP-Segmentierung: **debug ip nat frag**.

Frage: Wird NAT MIB unterstützt?

A. Nein. Es gibt keine unterstützte NAT MIB, einschließlich CISCO-IETF-NAT-MIB.

Frage: Was ist *TCP-Timeout*, und in welcher Beziehung steht es zum NAT TCP-Timer?

A. Wenn der Drei-Wege-Handshake nicht abgeschlossen ist und NAT ein TCP-Paket erkennt, startet NAT einen 60-Sekunden-Timer. Wenn der Drei-Wege-Handshake abgeschlossen ist, verwendet NAT standardmäßig einen 24-Stunden-Timer für einen NAT-Eintrag. Wenn ein End-Host ein RESET sendet, ändert NAT den Standard-Timer von 24 Stunden auf 60 Sekunden. Bei FIN ändert NAT den Standard-Timer von 24 Stunden auf 60 Sekunden, wenn FIN und FIN-ACK empfangen werden.

Frage: Kann ich die Zeit ändern, die eine NAT-Übersetzung benötigt, um ein Timeout aus der NAT-Übersetzungstabelle zu erhalten?

Antwort: Ja. Sie können die NAT-Timeoutwerte für alle Einträge oder für verschiedene Arten von NAT-Übersetzungen ändern (z. B. udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout und arp-ping-timeout).

F. Wie kann ich verhindern, dass das Lightweight Directory Access Protocol (LDAP)

zusätzliche Bytes an jedes LDAP-Antwortpaket anhängt?

A. Die LDAP-Einstellungen fügen die zusätzlichen Bytes (LDAP-Suchergebnisse) hinzu, während Nachrichten vom Typ "Search-Res-Entry" verarbeitet werden. LDAP fügt jedem LDAP-Antwortpaket 10 Byte Suchergebnisse hinzu. Falls diese 10 zusätzlichen Bytes an Daten dazu führen, dass das Paket die Maximum Transmission Unit (MTU) in einem Netzwerk überschreitet, wird das Paket verworfen. In diesem Fall empfiehlt Cisco, dieses LDAP-Verhalten mit dem Befehl CLI **no ip nat service append-ldap-search-res** zu deaktivieren, damit die Pakete gesendet und empfangen werden können.

Frage: Welche Routenempfehlung wird für die interne globale/externe lokale IP-Adresse im NAT-Feld empfohlen?

A. Im Feld für die NAT-Konfiguration muss eine Route für die globale interne IP-Adresse für Funktionen wie NAT-NVI angegeben werden. Entsprechend sollte auch im NAT-Feld eine Route für die externe lokale IP-Adresse angegeben werden. In diesem Fall erfordert jedes Paket von einer Ein- zur Auswärtsrichtung unter Verwendung der statischen Regel von außen diese Art von Route. In solchen Szenarien sollte neben der Bereitstellung der Route für IG/OL auch die Next-Hop-IP-Adresse konfiguriert werden. Wenn die nächste Hop-Konfiguration fehlt, wird dies als Konfigurationsfehler betrachtet und führt zu undefiniertem Verhalten.

NVI-NAT ist nur im Ausgabefunktionspfad vorhanden. Wenn Sie das Subnetz direkt mit NAT-NVI oder der externen, auf dem Gerät konfigurierten NAT-Übersetzungsregel verbunden haben, müssen Sie in diesen Szenarien eine Next-Hop-IP-Dummy-IP-Adresse und einen zugehörigen ARP für den Next-Hop angeben. Dies ist erforderlich, damit die zugrunde liegende Infrastruktur das Paket zur Übersetzung an NAT übergeben kann.

Frage: Unterstützt Cisco IOS NAT ACLs mit dem Schlüsselwort "log"?

A. Wenn Sie Cisco IOS NAT für die dynamische NAT-Übersetzung konfigurieren, wird eine ACL verwendet, um übersetzbare Pakete zu identifizieren. Die aktuelle NAT-Architektur unterstützt keine ACLs mit dem Schlüsselwort "log".

Voice-NAT

Frage: Unterstützt NAT das Skinny Client Control Protocol (SCCP) v17, das zusammen mit Cisco Unified Communications Manager (CUCM) v7 ausgeliefert wird?

A. CUCM 7 und alle Standardtelefonlasten für CUCM 7 unterstützen SCCPv17. Die verwendete SCCP-Version wird durch die höchste gemeinsame Version zwischen CUCM und dem Telefon bei der Telefonregistrierung bestimmt.

NAT unterstützt SCCP v17 noch nicht. Bis NAT-Unterstützung für SCCP v17 implementiert ist, muss die Firmware auf Version 8-3-5 oder niedriger heruntergestuft werden, damit SCCP v16 ausgehandelt wird. Das NAT-Problem tritt bei der Telefonauslastung von CUCM6 nicht auf, solange SCCP v16 verwendet wird. Cisco IOS unterstützt derzeit die SCCP-Version 17 nicht.

Frage: Welche CUCM-/SCCP-/Firmware-Lastversionen werden von NAT

unterstützt?

A. NAT unterstützt CUCM 6.x und frühere Versionen. Diese CUCM-Versionen werden mit der Telefon-Firmware-Standardauslastung 8.3.x (oder früher) veröffentlicht, die SCCP v15 (oder früher) unterstützt.

NAT bietet keine Unterstützung für CUCM-Versionen 7.x oder höher. Diese CUCM-Versionen werden mit der standardmäßigen Firmware-Last für 8.4.x-Telefone veröffentlicht, die SCCP v17 (oder höher) unterstützt.

Wenn CUCM 7.x oder höher verwendet wird, muss eine ältere Firmware-Last auf dem CUCM TFTP-Server installiert werden, damit die Telefone eine Firmware-Last mit SCCP v15 oder früher verwenden, um von NAT unterstützt zu werden.

Frage: Was ist die Erweiterung der Service Provider-PAT-Portzuweisung für RTP und RTCP?

A. Die Funktion zur Portzuweisung für RTP und RTCP von Service Providern stellt sicher, dass für SIP-, H.323- und Skinny-Sprachanrufe eine Verbindung hergestellt wird. Bei den für RTP-Streams verwendeten Port-Nummern handelt es sich um gerade Port-Nummern, und die RTCP-Streams sind die nächstfolgende ungerade Port-Nummer. Die Portnummer wird in eine Nummer innerhalb des angegebenen Bereichs umgewandelt, die RFC-1889 entspricht. Bei einem Anruf mit einer Portnummer innerhalb dieses Bereichs wird eine PAT-Umwandlung in eine andere Portnummer innerhalb dieses Bereichs durchgeführt. Ebenso führt eine PAT-Übersetzung für eine Portnummer außerhalb dieses Bereichs nicht zu einer Übersetzung in eine Nummer innerhalb des angegebenen Bereichs.

Frage: Was ist SIP (Session Initiation Protocol), und können SIP-Pakete über NAT adressiert werden?

A. SIP (Session Initiation Protocol) ist ein ASCII-basiertes Steuerungsprotokoll auf Anwendungsebene, mit dem Anrufe zwischen zwei oder mehr Endpunkten eingerichtet, verwaltet und beendet werden können. SIP ist ein alternatives Protokoll, das von der Internet Engineering Task Force (IETF) für Multimediakonferenzen über IP entwickelt wurde. Die Cisco SIP-Implementierung ermöglicht unterstützten Cisco Plattformen die Signalisierung der Einrichtung von Sprach- und Multimedia-Anrufen über IP-Netzwerke.

SIP-Pakete können per NAT adressiert werden.

Frage: Was ist die gehostete NAT-Traversal-Unterstützung für den Session Border Controller (SBC)?

A.: Mit der Funktion Cisco IOS Hosted NAT Traversal for SBC kann ein Cisco IOS NAT SIP Application-Level Gateway (ALG)-Router als SBC auf einem Cisco Multiservice-IP-to-IP-Gateway agieren, wodurch eine reibungslose Bereitstellung von VoIP-Services gewährleistet wird.

Weitere Informationen finden Sie unter Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller.

Frage: Wie viele SIP-, Skinny- und H323-Anrufe kann ein Router mit NAT mit

Speicher und CPU verarbeiten?

A. Die Anzahl der Anrufe, die von einem NAT-Router verarbeitet werden, hängt von der auf dem Gerät verfügbaren Speicherkapazität und der Verarbeitungsleistung der CPU ab.

Frage: Unterstützt ein NAT-Router die TCP-Segmentierung von Skinny- und H323-Paketen?

A. IOS-NAT unterstützt die TCP-Segmentierung für H323 in 12.4 Mainline und TCP-Segmentierung für SKINNY ab 12.4(6)T.

Frage: Gibt es Probleme, auf die Sie bei der Verwendung einer NAT-Überlastungskonfiguration in einer Sprachbereitstellung achten sollten?

Antwort: Ja. Wenn Sie über NAT-Überlastungskonfigurationen und eine Bereitstellung von Sprachanwendungen verfügen, benötigen Sie die Registrierungsmeldung, um NAT zu durchlaufen und eine Verknüpfung für "out->in" zu erstellen, um dieses interne Gerät zu erreichen. Das interne Gerät sendet diese Registrierung regelmäßig, und die NAT aktualisiert diese Pin-Hole/Zuordnung anhand der Informationen in der Signalisierungsnachricht.

Frage: Gibt es bekannte Probleme, die durch den Befehl clear ip nat trans * oder den Befehl clear ip nat trans in einer Sprachbereitstellung verursacht werden?

A. Wenn Sie bei Sprachbereitstellungen den Befehl **clear ip nat trans *** oder den **Befehl clear ip nat trans erzwungen** ausgeben und eine dynamische NAT verwenden, löschen Sie die Pin-Hole/Zuordnung und müssen auf den nächsten Registrierungszyklus vom internen Gerät warten, um dies wiederherzustellen. Cisco empfiehlt, diese klaren Befehle nicht in einer Sprachbereitstellung zu verwenden.

Frage: Unterstützt NAT Lösungen am gleichen Standort?

A. Nein. Die am gleichen Standort implementierte Lösung wird derzeit nicht unterstützt. Die folgende Bereitstellung mit NAT (im selben Gerät) gilt als am selben Standort implementierte Lösung: CME/DSP-Farm/SCCP/H323

Frage: Unterstützt NVI Skinny ALG, H323 ALG und TCP SIP ALG?

A. Nein. Beachten Sie, dass das UDP SIP ALG (von den meisten Bereitstellungen verwendet) nicht betroffen ist.

NAT mit VRF/MPLS

Frage: Unterstützt ein NAT-Router jemals die NAT-Funktion, die den gleichen Adressraum in einer VRF-Instanz belegt wie die NAT-Funktion in einem globalen Adressraum? Derzeit erhalte ich diese Warnung: *"% ähnlicher statischer Eintrag (1.1.1.1 —> 22.2.2.2) existiert bereits",* wenn ich versuche, Folgendes zu konfigurieren:

```
72UUT(config)#ip nat inside
```

```
source static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static
1.1.1.1 22.2.2.2 vrf RED
```

A.: Legacy NAT unterstützt das Überladen der Adresskonfiguration über verschiedene VRFs. Sie müssten Überlappungen in der Regel mit der *Match-in-VRF*-Option konfigurieren und **ip nat inside/outside** in der gleichen VRF für Datenverkehr über diese spezielle VRF-Instanz einrichten. Die sich überschneidende Unterstützung beinhaltet nicht die globale Routing-Tabelle.

Sie müssen das *Match-in-VRF*-Schlüsselwort für die überlappenden VRF-Einträge für die statische NAT für verschiedene VRFs hinzufügen. Es ist jedoch nicht möglich, globale und VRF NAT-Adressen zu überschneiden.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

Frage: Unterstützt das Legacy-NAT VRF-Lite (NATting von einem VRF zu einem anderen VRF)?

A. Nein. Sie müssen NVI für NATting zwischen verschiedenen VRFs verwenden. Sie können Legacy NAT verwenden, um NAT von VRF zu global oder NAT mit derselben VRF-Instanz durchzuführen.

NAT NVI

F. Was ist NAT NVI?

A. NVI steht für NAT Virtual Interface. NAT kann zwischen zwei verschiedenen VRFs übersetzt werden. Diese Lösung sollte anstelle von Network Address Translation auf einem Stick verwendet werden.

Frage: Soll NAT NVI beim NAT zwischen einer Schnittstelle in global und einer Schnittstelle in einer VRF-Instanz verwendet werden?

A.: Cisco empfiehlt die Verwendung von Legacy-NAT für VRF für globale NAT (ip nat inside/out) und zwischen Schnittstellen derselben VRF-Instanz. NVI wird für NAT zwischen verschiedenen VRFs verwendet.

Frage: Wird die TCP-Segmentierung für NAT-NVI unterstützt?

A. Die TCP-Segmentierung für NAT-NVI wird nicht unterstützt.

Frage: Unterstützt NVI Skinny ALG, H323 ALG und TCP SIP ALG?

A. Nein. Beachten Sie, dass das UDP SIP ALG (von den meisten Bereitstellungen verwendet) nicht betroffen ist.

F. Wird die TCP-Segmentierung von SNAT unterstützt?

A. SNAT unterstützt keine TCP-ALGs (z. B. SIP, SKINNY, H323 oder DNS). TCP-Segmentierung wird daher nicht unterstützt. UDP SIP und DNS werden jedoch unterstützt.

SNAT

F. Was ist Stateful NAT (SNAT)?

A. Mit SNAT können zwei oder mehr Netzwerkadressenübersetzer als Übersetzungsgruppe arbeiten. Ein Mitglied der Übersetzungsgruppe verarbeitet Datenverkehr, für den eine Übersetzung der IP-Adressinformationen erforderlich ist. Darüber hinaus informiert es den Backup-Übersetzer über aktive Datenflüsse, sobald diese auftreten. Der Backup-Übersetzer kann dann die Informationen des aktiven Übersetzers nutzen, um doppelte Einträge in der Übersetzungstabelle vorzubereiten. Wenn der aktive Übersetzer durch einen kritischen Fehler behindert wird, kann der Datenverkehr daher schnell auf das Backup umgeschaltet werden. Der Datenverkehrsfluss wird fortgesetzt, da dieselben Netzwerkadressenumwandlungen verwendet werden und der Status dieser Umwandlungen zuvor definiert wurde.

Frage: Wird die TCP-Segmentierung mit SNAT unterstützt?

A. SNAT unterstützt keine TCP-ALGs (z. B. SIP, SKINNY, H323 oder DNS). TCP-Segmentierung wird daher nicht unterstützt. UDP SIP und DNS werden jedoch unterstützt.

Frage: Unterstützt SNAT asymetrisches Routing?

A. Asymetrisches Routing unterstützt NAT, indem es als Warteschlange aktiviert wird. Standardmäßig ist "as-queueing" aktiviert. Ab 12.4(24)T wird jedoch das Warteschlangenmanagement nicht mehr unterstützt. Kunden müssen sicherstellen, dass Pakete ordnungsgemäß geroutet werden und eine angemessene Verzögerung hinzugefügt wird, damit das asymmetrische Routing ordnungsgemäß funktioniert.

NAT-PT (v6 bis v4)

F. Was ist NAT-PT?

A. NAT-PT ist die Übersetzung von v4 in v6 für NAT. Die Protokollübersetzung (NAT-PT) ist ein IPv6-IPv4-Übersetzungsmechanismus, der in RFC 2765 und RFC 2766 definiert ist und Geräten, die nur IPv6 verwenden, die Kommunikation mit Geräten, die nur IPv4 verwenden, ermöglicht.

Frage: Wird NAT-PT im Cisco Express Forwarding (CEF)-Pfad unterstützt?

A. NAT-PT wird im CEF-Pfad nicht unterstützt.

Frage: Welche ALGs werden in NAT-PT unterstützt?

A.: NAT-PT unterstützt TFTP/FTP und DNS. In NAT-PT werden Sprache und SNAT nicht unterstützt.

Frage: Unterstützt ASR 1004 NAT-PT?

A. Aggregation Services Router (ASR) verwenden NAT64.

Plattformabhängig Cisco 7300/7600/6000

Frage: Ist Stateful NAT (SNAT) für Catalyst 6500 im SX-Zug verfügbar?

Antwort: SNAT ist für Catalyst 6500 im SX-Zug nicht verfügbar.

Frage: Wird VRF-kompatibles NAT in der Hardware auf der 6000 unterstützt?

A.: VRF-kompatible NAT wird von der Hardware auf dieser Plattform nicht unterstützt.

Frage: Unterstützen der 7600 und der Cat6000 VRF-kompatible NAT?

Antwort: Auf der 65xx/76xx-Plattform wird VRF-kompatibles NAT nicht unterstützt, und die CLIs werden blockiert.

Hinweis: Sie können ein Design implementieren, indem Sie ein FWSM nutzen, das im transparenten Modus für virtuellen Kontext ausgeführt wird.

Plattformabhängig Cisco 850

Frage: Unterstützt der Cisco 850 Skinny NAT ALG in Version 12.4T?

A. Nein. Skinny NAT ALG wird in 12.4T auf der 850-Serie nicht unterstützt.

NAT-Bereitstellung

Frage: Wie implementiere ich NAT?

A. NAT ermöglicht privaten IP-Netzwerken, die nicht registrierte IP-Adressen verwenden, eine Verbindung mit dem Internet herzustellen. NAT übersetzt die private Adresse (RFC1918) im internen Netzwerk in zulässige routbare Adressen, bevor Pakete in ein anderes Netzwerk weitergeleitet werden.

Frage: Wie implementiere ich NAT mit Sprachfunktionen?

Antwort: Dank der NAT-Unterstützung für Sprachfunktionen können in SIP eingebettete Nachrichten, die über einen mit Network Address Translation (NAT) konfigurierten Router übertragen werden, zurück in das Paket übersetzt werden. Ein Application Layer Gateway (ALG) wird zusammen mit NAT zur Übersetzung der Sprachpakete verwendet.

Frage: Wie kann ich NAT in MPLS-VPNs integrieren?

A.: Dank der Funktion zur NAT-Integration in MPLS-VPNs können mehrere MPLS-VPNs für die Zusammenarbeit auf einem einzelnen Gerät konfiguriert werden. NAT kann unterscheiden, von welchem MPLS-VPN es IP-Datenverkehr empfängt, selbst wenn die MPLS-VPNs alle dasselbe

IP-Adressierungsschema verwenden. Dank dieser Erweiterung können mehrere MPLS-VPN-Kunden Services gemeinsam nutzen und gleichzeitig sicherstellen, dass jedes MPLS-VPN vollständig vom anderen VPN getrennt ist.

Frage: Unterstützt die statische NAT-Zuordnung HSRP für hohe Verfügbarkeit?

A. Wenn eine ARP-Abfrage (Address Resolution Protocol) für eine Adresse ausgelöst wird, die mit einer statischen NAT-Zuordnung (Network Address Translation) konfiguriert wurde und dem Router gehört, antwortet NAT mit der BIA-MAC-Adresse auf der Schnittstelle, auf die der ARP verweist. Zwei Router fungieren als HSRP Active und Standby. Die internen NAT-Schnittstellen müssen aktiviert und konfiguriert werden, um einer Gruppe anzugehören.

Frage: Wie implementiere ich NAT NVI?

Antwort: Durch die NAT Virtual Interface (NVI)-Funktion müssen Sie eine Schnittstelle weder als interne noch als externe NAT konfigurieren.

Frage: Wie implementiere ich Load Balancing mit NAT?

A. Mit NAT lassen sich zwei Arten des Lastenausgleichs durchführen: können Sie den Lastenausgleich für eingehenden Datenverkehr zu einer Gruppe von Servern vornehmen, um die Last auf die Server zu verteilen, und Sie können den Lastenausgleich für den Datenverkehr der Benutzer zum Internet über zwei oder mehr ISPs vornehmen.

Weitere Informationen zum ausgehenden Lastenausgleich finden Sie unter IOS NAT Load-Balancing for Two ISP Connections.

Frage: Wie implementiere ich NAT in Verbindung mit IPSec?

A. Es besteht Unterstützung für IP Security (IPSec) Encapsulating Security Payload (ESP) über NAT und IPSec NAT Transparency.

Die Funktion "IPSec ESP through NAT" bietet die Möglichkeit, mehrere gleichzeitige IPSec ESP-Tunnel oder -Verbindungen über ein Cisco IOS NAT-Gerät zu unterstützen, das im Überlastungs- oder PAT-Modus (Port Address Translation) konfiguriert ist.

Die IPSec NAT-Transparenzfunktion ermöglicht die Übertragung von IPSec-Datenverkehr durch NAT- oder PAT-Punkte im Netzwerk, indem viele bekannte Kompatibilitätsprobleme zwischen NAT und IPSec behoben werden.

Frage: Wie implementiere ich NAT-PT?

A. NAT-PT (Network Address Translation - Protocol Translation) ist ein in RFC 2765 und RFC 2766 definierter IPv6-IPv4-Umwandlungsmechanismus, der Geräten mit ausschließlichem IPv6-Zugriff auf Geräte mit ausschließlichem IPv4-Zugriff und umgekehrt ermöglicht.

Frage: Wie implementiere ich Multicast NAT?

A. Es ist möglich, die Quell-IP für einen Multicast-Stream per NAT zu übermitteln. Eine Routing-Map kann nicht verwendet werden, wenn dynamische NAT für Multicast ausgeführt wird. Hierfür

wird nur eine Zugriffsliste unterstützt.

Weitere Informationen finden Sie unter Funktionsweise von Multicast NAT auf Cisco Routern. Die Multicast-Zielgruppe wird mithilfe einer Multicast Service Reflection-Lösung NATted zugewiesen.

Frage: Wie implementiere ich Stateful NAT (SNAT)?

A. SNAT ermöglicht einen kontinuierlichen Dienst für dynamisch zugeordnete NAT-Sitzungen. Statisch definierte Sitzungen profitieren von Redundanz ohne SNAT. Ohne SNAT müssten Sitzungen, die dynamische NAT-Zuordnungen verwenden, im Falle eines kritischen Fehlers abgebrochen und wieder hergestellt werden. Es wird nur die minimale SNAT-Konfiguration unterstützt. Künftige Bereitstellungen sollten erst nach Rücksprache mit Ihrem Cisco Account Team durchgeführt werden, um das Design im Hinblick auf aktuelle Einschränkungen zu validieren.

SNAT wird für die folgenden Szenarien empfohlen:

- Der Modus für Primär-/Backup-Vorgänge wird nicht empfohlen, da im Vergleich zu HSRP einige Funktionen fehlen.
- Für Failover-Szenarien und Konfiguration mit zwei Routern. Das heißt, wenn ein Router ausfällt, übernimmt der andere Router nahtlos. (Die SNAT-Architektur ist nicht für die Handhabung von Schnittstellen-Flaps konzipiert.)
- Ein nicht asymmetrisches Routing wird unterstützt. Asymmetrisches Routing kann nur durchgeführt werden, wenn die Latenz im Antwortpaket höher ist als die zwischen zwei SNAT-Routern, die die SNAT-Nachrichten austauschen.

Die SNAT-Architektur ist derzeit nicht auf Robustheit ausgelegt. Daher wird nicht erwartet, dass diese Tests erfolgreich sind:

- Löschen von NAT-Einträgen bei laufendem Datenverkehr
- Änderung von Schnittstellenparametern (wie Änderung der IP-Adresse, "shutdown"/"no-shutdown" usw.) bei laufendem Datenverkehr
- SNAT-spezifische Befehle **clear** oder **show** werden nicht korrekt ausgeführt und nicht empfohlen.Einige der SNAT-bezogenen Befehle **clear** und **show** sind:

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- Wenn der Benutzer Einträge löschen möchte, können die Befehle **clear ip nat trans forced** oder **clear ip nat trans *** verwendet werden.Wenn der Benutzer Einträge anzeigen möchte, können die Befehle **show ip nat translation**, **show ip nat translation verbose** und **show ip nat stats** verwendet werden. Wenn *der interne Service* konfiguriert ist, werden auch SNAT-spezifische Informationen angezeigt.
- Das Löschen von NAT-Übersetzungen am Backup-Router wird nicht empfohlen. Löschen Sie

immer die NAT-Einträge auf dem primären SNAT-Router.
- SNAT ist nicht HA; Daher sollten die Konfigurationen auf beiden Routern identisch sein. Auf beiden Routern sollte dasselbe Image ausgeführt werden. Stellen Sie außerdem sicher, dass die für beide SNAT-Router verwendete zugrunde liegende Plattform identisch ist.

NAT - Best Practices

Frage: Gibt es Best Practices für NAT?

Antwort: Ja. NAT Best Practices:

1. Wenn sowohl dynamische als auch statische NAT verwendet wird, sollte die ACL, die die Regel für dynamische NAT festlegt, die statischen lokalen Hosts ausschließen, damit es nicht zu Überschneidungen kommt.
2. Achten Sie darauf, ACL für NAT mit **permit ip any any zu** verwenden, da dies zu unvorhersehbaren Ergebnissen führen kann. Nach 12.4(20)T übersetzt NAT lokal generierte HSRP- und Routing-Protokollpakete, wenn diese über die externe Schnittstelle gesendet werden, sowie lokal verschlüsselte Pakete, die der NAT-Regel entsprechen.
3. Wenn sich die Netzwerke für NAT überschneiden, verwenden Sie das Schlüsselwort **match-in-vrf**.Sie müssen das **Match-in-VRF-**Schlüsselwort für die überlappenden VRF-Einträge für die statische NAT für verschiedene VRFs hinzufügen, es ist jedoch nicht möglich, globale und VRF-NAT-Adressen zu überlappen.
```
Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf


Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```
4. NAT-Pools mit demselben Adressbereich können nur in verschiedenen VRFs verwendet werden, wenn das **Match-in-VRF-**Schlüsselwort verwendet wird.Beispiele:

```
ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24
ip nat pool poolB 171.1.1.1 171.1.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

   Anmerkung: Obwohl die CLI-Konfiguration gültig ist, wird die Konfiguration ohne das **Match-in-VRF**-Schlüsselwort nicht unterstützt.
5. Beim Bereitstellen von ISPs-Lastenausgleich mit NAT-Schnittstellenüberlastung wird als Best Practice eine Routing-Map mit Schnittstellenabgleich-über-ACL-Abgleich verwendet.
6. Wenn Sie die Poolzuordnung verwenden, sollten Sie nicht zwei verschiedene Zuordnungen (ACL oder route-map) verwenden, um dieselbe NAT-Pooladresse zu verwenden.
7. Wenn im Failover-Szenario dieselben NAT-Regeln auf zwei verschiedenen Routern bereitgestellt werden, sollte HSRP-Redundanz verwendet werden.
8. Definieren Sie in der statischen NAT und in einem dynamischen Pool nicht dieselbe globale Adresse. Diese Wirkung kann zu unerwünschten Ergebnissen führen.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

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.