Veelgestelde vragen over Network Address Translation (NAT)

Inhoud

Inleiding

Dit document bevat antwoorden op veelgestelde vragen over netwerkadresomzetting (NAT).

Generieke NAT

V. Wat is NAT?

A. Netwerkadresomzetting (NAT) is ontwikkeld voor het behoud van IP-adressen. Hiermee kunnen private IP-netwerken niet-geregistreerde IP-adressen gebruiken om verbinding te maken met het internet. NAT verbindt doorgaans twee netwerken via een router en zet de private (niet algemeen unieke) adressen in het interne netwerk om naar wettelijke adressen voordat pakketten naar een ander netwerk worden doorgestuurd.

Hierbij kan NAT worden geconfigureerd om slechts één adres voor het gehele netwerk aan de buitenwereld aan te kondigen. Dit zorgt voor extra security doordat het gehele interne netwerk effectief achter dat adres wordt verborgen. NAT biedt security en adresbehoud en wordt doorgaans geïmplementeerd in omgevingen met externe toegang.

V. Hoe werkt NAT?

A. NAT staat één apparaat, zoals een router, toe om als agent tussen het internet (of openbaar netwerk) en een lokaal netwerk (of private netwerk) te fungeren. Hierbij is slechts één uniek IP-adres nodig om een gehele groep computers te vertegenwoordigen aan alles buiten hun netwerk.

V. Hoe configureer ik NAT?

A. Om traditionele NAT te configureren, moet u ten minste één interface op een router (externe NAT) en een andere interface op de router (interne NAT) configureren en moeten een reeks regels voor het omzetten van de IP-adressen in de pakketheaders (en payloads, indien gewenst) worden geconfigureerd. Om NAT Virtual Interface (NVI) te configureren, heeft u ten minste één interface nodig die is geconfigureerd met NAT en dezelfde reeks regels als hierboven genoemd.

Raadpleeg Configuratiehandleiding Cisco IOS IP-adresseringsservices of NAT Virtual Interface configureren voor meer informatie.

V. Wat zijn de belangrijkste verschillen tussen NAT-implementaties van de Cisco IOS®-software en de Cisco PIX security applicatie?

A. Op Cisco IOS-software gebaseerde NAT verschilt niet fundamenteel van de NAT-functie in de Cisco PIX security applicatie. De belangrijkste verschillen omvatten de verschillende verkeerstypen die in de implementaties worden ondersteund. Raadpleeg Voorbeelden van NAT-configuraties voor meer informatie over de configuratie van NAT op Cisco PIX-apparaten (inclusief de ondersteunde verkeerstypen).

V. Op welke Cisco-routinghardware is Cisco IOS NAT beschikbaar? Hoe kan de hardware worden besteld?

A. Met de tool Cisco Feature Navigator kunnen klanten een functie (NAT) identificeren en nagaan in welke release en hardware-versie deze Cisco IOS-softwarefunctie beschikbaar is. Raadpleeg Cisco Feature Navigator om deze tool te gebruiken.

V. Vindt NAT voor of na routing plaats?

A. De volgorde waarin de transacties met NAT worden verwerkt, is afhankelijk van het feit of een pakket van het interne netwerk naar het externe netwerk gaat of andersom. Omzetting van intern naar extern vindt plaats na routing, omzetting van extern naar intern vindt plaats vóór routing. Raadpleeg Volgorde van NAT-bewerkingen voor meer informatie.

V. Kan NAT worden geïmplementeerd in een openbare wireless LAN-omgeving?

A. Ja. De functie NAT - Static IP Support (NAT-ondersteuning voor statische IP) biedt ondersteuning voor gebruikers met statische IP-adressen die hiermee een IP-sessie kunnen opzetten in een openbare wireless LAN-omgeving.

V. Ondersteunt NAT TCP-taakverdeling voor servers op het interne netwerk?

A. Ja. Met NAT kunt u een virtuele host op het interne netwerk instellen voor het coördineren van de workloadverdeling tussen echte hosts.

V. Kan ik het aantal NAT-omzettingen beperken?

A. Ja. Met de functie Rate-Limiting NAT Translation (NAT-omzettingen beperken) kunt u het maximumaantal gelijktijdige NAT-verwerkingen op een router beperken. Met deze functie heeft u niet alleen meer controle op de manier waarop NAT-adressen worden gebruikt, maar kunnen ook de effecten van virussen, wormen en denial-of-service aanvallen worden beperkt.

V. Hoe wordt de routing geleerd of verspreid voor IP-subnetten of -adressen die door NAT worden gebruikt?

A. Routing voor IP-adressen gemaakt door NAT wordt geleerd indien:

- De interne algemene adresgroep wordt afgeleid van het subnet van een next-hop router.
- De statische routevermelding wordt geconfigureerd in de volgende hop-router en wordt geherdistribueerd binnen het routingnetwerk.

Wanneer het interne algemene adres wordt gematcht met de lokale interface, installeert NAT een IP-alias en een ARP-vermelding, waarbij de router **proxy-arp** uitvoert voor deze adressen. Als dit gedrag ongewenst is, gebruikt u het trefwoord **no-alias.**

Wanneer een NAT-groep wordt geconfigureerd, kan de optie **add-route worden gebruikt voor automatic route-invoeging.**

V. Hoeveel gelijktijdige NAT-sessies worden er ondersteund in Cisco IOS NAT?

A. De limiet voor het aantal NAT-sessies wordt bepaald door de hoeveelheid beschikbare DRAM in de router. Elke NAT-omzetting vereist ongeveer 312 bytes DRAM. 10.000 omzettingen (meer dan doorgaans op één router worden verwerkt) vereist dus ongeveer 3 MB. Typische routinghardware heeft dan ook meer dan voldoende geheugen voor duizenden NAT-omzettingen.

V. Welke routingprestaties kunnen worden verwacht bij gebruik van Cisco IOS NAT?

A. Cisco IOS NAT ondersteunt Cisco Express Forwarding-switching, fast-switching en proces-switching. In release 12.4T en hoger wordt fast-switchingpad niet langer ondersteund. Op het Cat6k-platform is de switchingvolgorde NetFlow (HW-switchingpad), CEF, procespad.

De prestaties hangen af van verschillende factoren:

- Het type toepassing en het type verkeer
- Of IP-adressen ingesloten zijn
- Uitwisseling en controle van meerdere berichten
- Vereiste bronpoort
- Het aantal omzettingen
- Andere toepassingen die op dat moment actief zijn
- Het type hardware en processor

V. Kan Cisco IOS NAT op subinterfaces worden toegepast?

A. Ja. NAT-omzettingen voor bron en/of bestemming kunnen worden toegepast op elke interface of subinterfaces met een IP-adres (inclusief snelkiezerinterfaces). NAT kan niet worden geconfigureerd met een wireless virtuele interface. Er bestaat geen wireless virtuele interface op het moment van schrijven naar NVRAM. Na opnieuw opstarten verliest de router dan ook de NAT-configuratie op de wireless virtuele interface.

V. Kan Cisco IOS NAT worden gebruikt met het Hot Standby Router Protocol (HSRP) om redundante links naar een ISP te bieden?

A. Ja. NAT biedt HSRP-redundantie. Maar deze verschilt van SNAT (Stateful NAT). NAT met HSRP is een stateless systeem. De huidige sessie blijft niet behouden wanneer een fout optreedt. Tijdens statische NAT-configuratie (wanneer een pakket niet voldoet aan een STATISCHE regelconfiguratie) wordt het pakket zonder omzetting verzonden.

V. Ondersteunt Cisco IOS NAT inkomende omzettingen op een Frame Relay-interface? Ondersteunt Cisco IOS NAT uitgaande omzettingen aan de Ethernet-zijde?

A. Ja. Insluiting is niet van belang voor NAT. NAT kan worden uitgevoerd wanneer er een IP-adres op een interface bestaat en de interface interne of externe NAT betreft. NAT is mogelijk als er een interne en een externe kant is. Als u NVI gebruikt, moet er ten minste één NAT-interface zijn. Zie Hoe configureer ik NAT? voor meer informatie.

V. Kan één NAT-router sommige gebruikers toestaan om NAT te gebruiken en andere gebruikers op dezelfde Ethernet-interface om hun eigen IP-adres te blijven gebruiken?

A. Ja. Dit kan door een toegangslijst te gebruiken die de reeks hosts of netwerken beschrijft die NAT nodig hebben. Alle sessies op dezelfde host worden omgezet of worden via de router doorgegeven en niet omgezet.

Toegangslijsten, uitgebreide toegangslijsten en routekaarten kunnen worden gebruikt om *regels* te definiëren voor het omzetten van IP-apparaten. Het netwerkadres en het juiste subnetmasker moeten altijd worden opgegeven. Het trefwoord **any moet niet worden gebruikt in plaats van het netwerkadres of het subnetmasker.** Wanneer een pakket niet voldoet aan een STATISCHE regelconfiguratie, wordt het bij statische NAT-configuratie zonder enige omzetting doorgegeven.

V. Wat is bij het configureren voor PAT (overloading) het maximumaantal omzettingen dat per intern algemeen IP-adres mogelijk is?

A. Met PAT (overloading) worden de beschikbare poorten per algemeen IP-adres verdeeld in drie bereiken: 0-511, 512-1023 en 1024-65535. Voor elke UDP- of TCP-sessie wordt met PAT een unieke bronpoort toegewezen. Met PAT wordt geprobeerd dezelfde poortwaarde van de oorspronkelijke aanvraag toe te wijzen. Als de oorspronkelijke bronpoort echter al gebruikt is, wordt er gescand vanaf het begin van het specifieke poortbereik om de eerste beschikbare poort te vinden en deze aan het gesprek toe te wijzen. Er geldt een uitzondering voor codebasis 12.2S. Codebasis 12.2S gebruikt een andere poortlogica en er is geen sprake van poortreservering.

V. Hoe werkt PAT?

A. PAT werkt met één algemeen IP-adres of meerdere adressen.

PAT met één IP-adres

Voor waar de	Beschrijving
1	NAT/PAT controleert het verkeer en matcht het met een omzettingsregel.

2	Regel komt overeen met een PAT-configuratie.
3	Als het verkeerstype bekend is en als dat verkeerstype ‘een reeks specifieke poorten heeft of poorten waarover wordt onderhandeld’, worden deze met PAT terzijde gezet en niet toegewezen als unieke identificatie.
4	Als een sessie zonder speciale poortvereisten een verbinding naar buiten (de externe kant) tot stand probeert te brengen, wordt met PAT het IP-bronadres omgezet en wordt op beschikbaarheid van de oorspronkelijke bronpoort gecontroleerd (bijvoorbeeld 433). **Opmerking:** Op Transmission Control Protocol (TCP) en User Datagram Protocol (UDP) zijn de volgende bereiken van toepassing: 1-511, 512-1023 en 1024-65535. Bij Internet Control Message Protocol (ICMP) start de eerste groep bij 0.
5	Als de aangevraagde bronpoort beschikbaar is, wordt met PAT de bronpoort toegewezen en de sessie voortgezet.
6	Als de aangevraagde bronpoort niet beschikbaar is, wordt met PAT vanaf het begin van de relevante groep gezocht (beginnend bij 1 voor TCP- of UDP-toepassingen en bij 0 voor ICMP-toepassingen).
7	Als een poort beschikbaar is, wordt deze toegewezen en wordt de sessie voortgezet.
8	Als er geen poorten beschikbaar zijn, wordt het pakket verwijderd (afgewezen).

PAT met meerdere IP-adressen

Voor waarde	Beschrijving
1-7	De eerste zeven voorwaarden zijn hetzelfde als bij PAT met één IP-adres.
8	Als er geen poorten beschikbaar zijn in de relevante groep op het eerste IP-adres, gaat NAT naar het volgende IP-adres in de groep en wordt geprobeerd de oorspronkelijke aangevraagde bronpoort toe te wijzen.
9	Als de aangevraagde bronpoort beschikbaar is, wordt met NAT de bronpoort toegewezen en de sessie voortgezet.
10	Als de aangevraagde bronpoort niet beschikbaar is, wordt met NAT vanaf het begin van de relevante groep gezocht (beginnend bij 1 voor TCP- of UDP-toepassingen en bij 0 voor ICMP-

	toepassingen).
11	Als een poort beschikbaar is, wordt deze toegewezen en wordt de sessie voortgezet.
12	Als er geen poorten beschikbaar zijn, wordt het pakket verwijderd (afgewezen), tenzij er een ander IP-adres in de groep beschikbaar is.

V. Wat zijn NAT IP-adresgroepen?

A. NAT IP-adresgroepen zijn reeksen IP-adressen die voor NAT-omzetting worden toegewezen, indien nodig. Om een groep te definiëren, wordt de volgende configuratieopdracht gebruikt:

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

Voorbeeld 1

In het volgende voorbeeld wordt omgezet tussen interne hosts vanaf het netwerk-IP-adres 192.168.1.0 of 192.168.2.0 naar het algemene unieke netwerk-IP-adres 10.69.233.208/28:

```
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
```

Voorbeeld 2

In het volgende voorbeeld wordt een virtueel adres gedefinieerd waarbij verbindingen daarnaar worden gedistribueerd naar een reeks echte hosts. De groep definieert de adressen van de echte hosts. De toegangslijst definieert het virtuele adres. Als een omzetting niet al bestaat, worden TCP-pakketten vanaf seriële interface 0 (de buiteninterface) waarvan de bestemming overeenkomt met de toegangslijst omgezet naar een adres uit de groep .

```
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
```

V. Wat is het maximumaantal configureerbare NAT IP-adresgroepen (ip nat pool "name")?

A. In de praktijk wordt het maximumaantal configureerbare IP-adresgroepen beperkt door de hoeveelheid beschikbare DRAM in de betreffende router. (Cisco raadt aan maximaal 255 groepen te configureren.) Elke groep mag niet meer dan 16 bits groot zijn. In release 12.4(11)T en hoger introduceert IOS CCE (Common Classification Engine). Dit heeft NAT beperkt tot maximaal 255 groepen. In codebase 12.2S is er geen beperking met betrekking tot het maximumaantal groepen.

V. Wat is het voordeel van het gebruik van een routekaart in plaats van een toegangscontrolelijst bij een NAT-groep?

A. Een routekaart voorkomt dat ongewenste externe gebruikers de interne gebruikers/servers bereiken. Bovendien kan met een routekaart één intern IP-adres aan verschillende interne algemene adressen worden toegewezen op basis van de regel. Raadpleeg NAT Support for Multiple Pools Using Route Maps (NAT-ondersteuning voor meerdere groepen met routekaarten) voor meer informatie.

V. Wat is 'overlapping' van IP-adressen in de context van NAT?

A. IP-adresoverlapping verwijst naar een situatie waarbij twee locaties die onderling verbinding willen maken hetzelfde IP-adresschema gebruiken. Dit is niet ongebruikelijk; het gebeurt vaak wanneer bedrijven fuseren of worden overgenomen. Zonder speciale ondersteuning kunnen de twee locaties geen verbinding maken en sessies opzetten. Het overlappende IP-adres kan een openbaar adres zijn dat aan een ander bedrijf is toegewezen, een privéadres dat aan een ander bedrijf is toegewezen of kan afkomstig zijn uit het bereik van privéadressen zoals gedefinieerd in RFC 1918.

Privé-IP-adressen zijn niet routeerbaar en vereisen NAT-omzettingen om verbindingen met de buitenwereld mogelijk te maken. De oplossing omvat het onderscheppen van responsen op DNS-query's (Domain Name System) van de externe kant naar de interne kant, het creëren van een omzetting voor het externe adres en het bepalen van de DNS-respons voordat deze naar de interne host wordt doorgestuurd. Een DNS-server moet aan beide zijden van het NAT-apparaat worden ingeschakeld voor gebruikers die een verbinding tussen beide netwerken willen.

NAT kan adresomzetting op de inhoud van DNS *A*- en *PTR*-records controleren en uitvoeren, zoals in NAT gebruiken in overlappende netwerken wordt getoond.

V. Wat zijn statische NAT-omzettingen?

A. Bij statische NAT-omzettingen is een één-op-één toewijzing tussen lokale en algemene adressen van toepassing. Gebruikers kunnen ook statische adresomzettingen naar poortniveau configureren en de rest van het IP-adres voor andere omzettingen gebruiken. Dit gebeurt meestal wanneer PAT (Port Address Translation) wordt toegepast.

In het volgende voorbeeld wordt getoond hoe u een routekaart configureert om omzetting van de externe kant naar de interne kant voor statische NAT toe te staan:

```
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
```

V. Wat wordt bedoeld met het begrip NAT *overloading*; is dat PAT?

A. Ja. NAT overloading is PAT, waarbij een groep met een reeks van een of meer adressen wordt gebruikt, of een interface-IP-adres in combinatie met de poort wordt gebruikt. Bij overloading is sprake van een volledige omzetting. Dit is een vermelding in de omzettingstabel met informatie over IP-adres en bron-/bestemmingspoort. Dit wordt PAT of overloading genoemd.

PAT (of overloading) is een functie van Cisco IOS NAT die wordt gebruikt om *interne* (interne lokale) privéadressen om te zetten naar één of meer *externe* (externe algemene, doorgaans geregistreerde) IP-adressen. Unieke bronpoortnummers bij elke omzetting worden gebruikt om onderscheid te maken tussen de gesprekken.

V. Wat zijn dynamische NAT-omzettingen?

A. Bij dynamische NAT-omzettingen kunnen gebruikers dynamische toewijzing tussen lokale en algemene adressen instellen. Dynamische toewijzing wordt uitgevoerd door de lokale adressen te definiëren die moeten worden omgezet en de groep met adressen of het interface-IP-adres te definiëren waarvandaan algemene adressen worden toegewezen en de twee vervolgens te koppelen.

V. Wat is ALG?

A. ALG is een Application Layer Gateway (ALG). NAT voert omzetting uit op TCP/UDP-verkeer (Transmission Control Protocol/User Datagram Protocol) dat geen IP-adres van bron en/of bestemming in de toepassingsdatastroom bevat.

Deze protocollen omvatten FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh en rcp. Specifieke protocollen die IP-adresinformatie in de payload insluiten, vereisen ondersteuning van een Application Layer Gateway (ALG).

Raadpleeg Application Layer Gateways gebruiken met NAT voor meer informatie.

V. Is het mogelijk een configuratie te creëren met zowel statische als dynamische NAT-omzettingen?

A. Ja. Het is echter niet mogelijk hetzelfde IP-adres te gebruiken voor de statische NAT-configuratie of in de groep voor dynamische NAT-configuratie. Alle openbare IP-adressen moeten uniek zijn. De algemene adressen die in statische omzettingen worden gebruikt, worden niet automatisch uitgesloten bij dynamische groepen die deze algemene adressen bevatten. Er moeten dynamische groepen worden gecreëerd om adressen uit te sluiten die via statische vermeldingen zijn toegewezen. Raadpleeg Statische en dynamische NAT gelijktijdig configureren voor meer informatie.

V. Wanneer een traceroute wordt uitgevoerd via een NAT-router, moet de traceroute dan het algemene NAT-adres tonen of het lokale NAT-adres?

A. Traceroute vanaf de externe kant moet altijd het algemene adres retourneren.

V. Hoe worden via PAT poorten toegewezen?

A. NAT voegt extra poortfuncties toe: full-range en port-map.

- Met full-range kan NAT alle poorten gebruiken, ongeacht het standaard poortbereik.
- Met port-map kan NAT een door de gebruiker gedefinieerd poortbereik reserveren voor een specifieke toepassing.

Raadpleeg Door gebruiker gedefinieerde bronpoortbereiken voor PAT voor meer informatie.

In release 12.4(20)T2 en hoger introduceert NAT poortrandomisatie voor L3/L4 en het kenmerk symmetric-port.

- Met poortrandomisatie kan NAT willekeurig een algemeen poort selecteren voor de bronpoortaanvraag.
- Met symmetric-port kan NAT *endpointonafhankelijke* ondersteuning bieden.

V. Wat is het verschil tussen IP-fragmentatie en TCP-segmentatie?

A. IP-fragmentatie vindt plaats op Layer 3 (IP); TCP-segmentatie vindt plaats op Layer 4 (TCP). IP-fragmentatie vindt plaats wanneer pakketten die groter zijn dan de maximale verzendeenheid (MTU) van een interface vanuit die interface worden verzonden. Deze pakketten moeten worden gefragmenteerd of afgewezen wanneer deze vanuit de interface worden verzonden. Als het DF-bit (niet fragmenteren) niet in de IP-header van het pakket is ingesteld, wordt het pakket gefragmenteerd. Als het DF-bit wel in de IP-header van het pakket is ingesteld, wordt het pakket verwijderd (afgewezen) en wordt een ICMP-foutmelding met MTU-waarde next-hop geretourneerd naar de verzender. Alle fragmenten van een IP-pakket hebben dezelfde Ident in de IP-header, zodat de laatste ontvanger het oorspronkelijke IP-pakket opnieuw kan samenstellen aan de hand van de fragmenten. Raadpleeg Problemen met IP-fragmentatie, MTU, MSS en PMTUD met GRE en IPsec oplossen voor meer informatie.

TCP-segmentatie vindt plaats wanneer een toepassing op een eindstation data verzendt. De toepassingsdata wordt opgedeeld in eenheden met een volgens TCP de beste grootte voor verzending. Een dergelijke eenheid die van TCP naar IP wordt doorgegeven, wordt een segment genoemd. TCP-segmenten worden verzonden in IP-datagrammen. De IP-datagrammen kunnen vervolgens IP-fragmenten worden wanneer deze het netwerk doorkruisen en lagere MTU-links aantreffen dan zij kunnen passeren.

TCP zal eerst deze data segmenteren in TCP-segmenten (gebaseerd op de TCP MSS-waarde), vervolgens de TCP-header toevoegen en dit TCP-segment doorgeven aan IP. IP voegt vervolgens een IP-header toe om het pakket naar de externe eindhost te verzenden. Als het IP-pakket met het TCP-segment groter is dan de IP MTU op een uitgaande interface op het pad tussen de TCP-hosts, zal IP het IP/TCP-pakket fragmenteren om het te laten passeren. Deze IP-pakketfragmenten worden op de externe host opnieuw samengevoegd door de IP-laag en het volledige TCP-segment (dat oorspronkelijk werd verzonden) wordt aan de TCP-laag overgedragen. De TCP-laag detecteert niet dat IP het pakket tijdens de verzending heeft gefragmenteerd.

NAT ondersteunt IP-fragmenten maar geen TCP-segmenten.

V. Ondersteunt NAT ‘verkeerde volgorde’ bij IP-fragmentatie en TCP-segmentatie?

A. NAT ondersteunt alleen IP-fragmenten in verkeerde volgorde vanwege **ip virtual-reassembly**.

V. Hoe kunnen fouten met IP-fragmentatie en TCP-segmentatie worden opgespoord?

A. Met NAT wordt voor zowel IP-fragmentatie als TCP segmentatie dezelfde opdrachtregelinterface voor foutopsporing gebruikt: **debug ip nat frag**.

V: Is er een ondersteunde NAT MIB?

A. Nee. Er is geen ondersteunde NAT MIB, inclusief CISCO-IETF-NAT-MIB.

V. Wat is *TCP-time-out* en wat is het verband met de NAT TCP-timer?

A. Als de drierichtings-handshake niet is voltooid en NAT een TCP-pakket waarneemt, wordt een timer van 60 seconden gestart. Wanneer de drierichtings-handshake is voltooid, wordt standaard een timer van 24 uur voor een NAT-vermelding gebruikt. Als een eindhost een RESET-signaal verzendt, verandert NAT de standaardtimer van 24 uur in 60 seconden. Bij een FIN-signaal verandert NAT de standaardtimer van 24 uur in 60 seconden wanneer een FIN- en FIN-ACK-signaal wordt ontvangen.

V. Kan ik de hoeveelheid tijd die nodig is voordat een time-out van de NAT-omzetting optreedt instellen via de NAT-tabel?

A. Ja. U kunt de waarden voor NAT-time-out wijzigen voor alle vermeldingen of voor verschillende typen NAT-omzettingen (zoals udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout en arp-ping-timeout).

V. Hoe kan ik voorkomen dat Lightweight Directory Access Protocol (LDAP) extra bytes aan elk LDAP-antwoordpakket toevoegt?

A. De LDAP-instellingen voegen extra bytes (LDAP-zoekresultaten) toe tijdens het verwerken van berichten van het type Search-Res-Entry. LDAP voegt 10 bytes aan zoekresultaten toe aan elk LDAP-antwoordpakket. Als deze 10 extra bytes aan data ertoe leiden dat het pakket de maximale verzendeenheid (MTU) in een netwerk overschrijdt, wordt het pakket verwijderd (afgewezen). Cisco raadt u in dat geval aan dit LDAP-gedrag uit te schakelen via de opdrachtregelinterface met de opdracht **no ip nat service append-ldap-search-res** zodat de pakketten worden verzonden en ontvangen.

V. Wat is de routeaanbeveling voor het interne algemene/externe lokale IP-adres op het NAT-apparaat?

A. Op het geconfigureerde NAT-apparaat moet een route voor het interne algemene IP-adres worden opgegeven voor functies zoals NAT-NVI. Er moet ook een route voor het externe lokale IP-adres op het NAT-apparaat worden opgegeven. Elk pakket afkomstig uit interne of externe richting die de externe statische regel gebruikt zal dan die route vereisen. In dergelijke scenario’s moet ook het IP-adres van de volgende hop worden geconfigureerd wanneer de route voor IG/OL

wordt verstrekt. Als de volgende hop-configuratie ontbreekt, wordt dit beschouwd als een configuratiefout en zal dat tot ongedefinieerd gedrag leiden.

NVI-NAT is alleen aanwezig in het pad voor de output-functie. Als u het subnet rechtstreeks heeft verbonden met NAT-NVI of de externe NAT-omzettingsregel die op het apparaat is geconfigureerd, moet u in die scenario's een dummy IP-adres van de volgende hop en een bijbehorende ARP voor de volgende hop verstrekken. Dit is nodig om de onderliggende infrastructuur het pakket voor omzetting aan NAT te laten overhandigen.

V. Ondersteunt Cisco IOS NAT ACL's met een trefwoord 'log'?

A. Wanneer u Cisco IOS NAT configureert voor dynamische NAT-omzetting, wordt een ACL (toegangscontrolelijst) gebruikt om pakketten te identificeren die kunnen worden omgezet. De huidige NAT-architectuur ondersteunt geen ACL's met een trefwoord 'log'.

NAT met spraak

V. Ondersteunt NAT het Skinny Client Control Protocol (SCCP) v17 dat wordt meegeleverd met Cisco Unified Communications Manager (CUCM) v7?

A. CUCM 7 en alle standaard telefoonconfiguraties voor CUCM 7 ondersteunen SCCP v17. De gebruikte SCCP-versie wordt bepaald door de hoogste gemeenschappelijke versie van CUCM en de telefoon wanneer de telefoon wordt geregistreerd.

NAT biedt nog geen ondersteuning voor SCCP v17. Totdat NAT-ondersteuning voor SCCP v17 is geïmplementeerd, moet de firmware worden gedowngraded naar versie 8-3-5 of lager zodat SCCP v16 wordt gebruikt. CUCM6 heeft geen last van het NAT-probleem dat optreedt met een telefoonlading zolang SCCP v16 wordt ingezet. Cisco IOS biedt momenteel geen ondersteuning voor SCCP v17.

V. Welke versies van CUCM/SCCP/firmware worden ondersteund door NAT?

A. NAT ondersteunt CUCM-versie 6.x en lager. Deze CUCM-versies worden vrijgegeven met de standaard 8.3.x (of lagere) telefoonfirmware die SCCP v15 (of lager) ondersteunt.

NAT biedt geen ondersteuning voor CUCM-versie 7.x of lager. Deze CUCM-versie wordt vrijgegeven met de standaard 8.4.x telefoonfirmware die SCCP v17 (of hoger) ondersteunt.

Als CUCM-versie 7.x of hoger wordt gebruikt, moet een oudere firmwarelading op de CUCM TFTP-server zijn geïnstalleerd, zodat de telefoons een firmwarelading met SCCP v15 of lager gebruiken voor ondersteuning door NAT.

V. Wat is Service Provider PAT Port Allocation Enhancement for RTP and RTCP (Verbeterde toewijzing van PAT-poorten voor RTP en RTCP voor serviceproviders)?

A. De functie Service Provider PAT Port Allocation Enhancement for RTP and RTCP ondersteunt SIP-, H.323- en Skinny-spraakoproepen. De poortnummers die worden gebruikt voor RTP-stromen zijn even poortnummers; de poortnummers die worden gebruikt voor RTCP-stromen zijn de daaropvolgende oneven poortnummers. Het poortnummer wordt omgezet naar een nummer

binnen het bereik dat is opgegeven in navolging van RFC-1889. Een oproep met een poortnummer binnen het bereik leidt tot PAT-omzetting naar een ander poortnummer binnen dat bereik. Een PAT-omzetting voor een poortnummer buiten dit bereik leidt niet tot omzetting naar een nummer binnen het betreffende bereik.

V. Wat is Session Initiation Protocol (SIP) en kunnen SIP-pakketten via NAT worden verwerkt?

A. Session Initiation Protocol (SIP) is een op ASCII gebaseerd controleprotocol op de toepassingslaag dat kan worden gebruikt om oproepen tussen twee of meer endpoints tot stand te brengen, te behouden en te beëindigen. SIP is een alternatief protocol dat door de Internet Engineering Task Force (IETF) is ontwikkeld voor multimedia conferencing via IP. Met Cisco's SIP-implementatie kunnen ondersteunde Cisco-platforms de opzet van spraak- en multimedia-oproepen via IP-netwerken signaleren.

SIP-pakketten kunnen via NAT worden verwerkt.

V. Wat houdt ondersteuning van Hosted NAT Traversal voor Session Border Controller (SBC) in?

A. Met de Cisco IOS-functie Hosted NAT Traversal voor SBC kan een Cisco IOS NAT SIP ALG-router (Application Layer Gateway) fungeren als SBC op een Cisco Multiservice IP-to-IP gateway. Hierdoor bent u verzekerd van optimale levering van VoIP-services (Voice-over-IP).

Raadpleeg Cisco IOS Hosted NAT Traversal configureren voor Session Border Controller voor meer informatie.

V. Hoeveel SIP-, Skinny- en H323-oproepen kunnen via het geheugen en de CPU van een router met NAT worden verwerkt?

A. Het aantal oproepen dat door een NAT-router wordt verwerkt, is afhankelijk van de hoeveelheid geheugen die op het apparaat beschikbaar is en de verwerkingskracht van de CPU.

V. Ondersteunt een NAT-router TCP-segmentatie van Skinny- en H323-pakketten?

A. IOS-NAT ondersteunt TCP-segmentatie voor H323 in 12.4 Mainline en TCP-segmentatie voor SKINNY vanaf release 12.4(6)T.

V. Zijn er voorbehouden ten aanzien van de configuratie van NAT-overloading bij spraakimplementatie?

A. Ja. Wanneer u NAT-overloading en spraakimplementatie configureert, moet het registratiebericht via NAT verlopen en moet een koppeling worden gemaakt voor extern -> intern om het interne apparaat te bereiken. Het interne apparaat verzendt deze registratie periodiek en NAT werkt deze pin-hole/koppeling bij op basis van de informatie in het signaalbericht.

V. Zijn er bekende problemen die worden veroorzaakt door de opdracht clear ip nat trans * of clear ip nat trans forced in spraakimplementaties?

A. Als u in spraakimplementaties de opdracht **clear ip nat trans *** of **clear ip nat trans forced** opgeeft en er sprake is van dynamische NAT, wordt de pin-hole/koppeling verwijdert en moet u wachten tot de volgende registratiecyclus van het interne apparaat om deze weer te creëren. Cisco raadt u aan deze 'clear'-opdrachten niet in spraakimplementaties te gebruiken.

V. Ondersteunt NAT spraak op basis van colocatie?

A. Nee. Dit wordt momenteel niet ondersteund. De volgende implementatie met NAT (op hetzelfde apparaat) wordt beschouwd als een colocatie-oplossing: CME/DSP-Farm/SCCP/H323.

V. Ondersteunt NVI Skinny ALG, H323 ALG en TCP SIP ALG?

A. Nee. UDP SIP ALG (gebruikt door de meeste implementaties) wordt overigens niet beïnvloed.

NAT met VRF/MPLS

V. Zal een NAT-router ooit verwerking via NAT van dezelfde adresruimte in een VRF ondersteunen als via NAT wordt verwerkt in een algemene adresruimte? Momenteel krijg ik de volgende melding: *"% similar static entry (1.1.1.1 ---> 22.2.2.2) already exists"* (% gelijksoortige statische vermelding (1.1.1.1 —> 22.2.2) bestaat al) wanneer ik probeer het volgende te configureren:

```
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. Verouderde NAT ondersteunt de configuratie van overlappende adressen via verschillende VRF's. U moet overlapping als een regel definiëren met de optie **match-in-vrf en ip nat inside/outside instellen in dezelfde VRF voor verkeer via die specifieke VRF.** Ondersteuning voor overlapping omvat niet de algemene routingtabel.

U moet het trefwoord **match-in-vrf toevoegen voor de overlappende statische NAT-vermeldingen voor VRF voor verschillende VRF's.** Het is echter niet mogelijk om algemene adressen en NAT-adressen voor VRF te overlappen.

```
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
```

V. Ondersteunt verouderde NAT VRF-Lite (verwerking via NAT van een VRF naar een andere VRF)?

A. Nee. U moet NVI gebruiken voor verwerking via NAT tussen verschillende VRF's. U kunt verouderde NAT gebruiken voor verwerking van VRF naar algemeen of voor verwerking binnen dezelfde VRF.

NAT NVI

V. Wat is NAT NVI?

A. NVI staat voor NAT Virtual Interface. Hiermee kan NAT omzetting uitvoeren tussen twee verschillende VRF's. Deze oplossing moet worden gebruikt in plaats van netwerkadresomzetting via één fysieke interface van een router.

V. Moet NAT NVI worden gebruikt bij verwerking via NAT tussen een interface in een algemene adresruimte en een interface in een adresruimte in VRF?

A. Cisco raadt aan verouderde NAT te gebruiken voor VRF naar algemene NAT (ip nat inside/out) en tussen interfaces in dezelfde VRF. NVI wordt gebruikt voor NAT tussen verschillende VRF's.

V. Wordt TCP-segmentatie voor NAT-NVI ondersteund?

A. Er is geen ondersteuning voor TCP-segmentatie voor NAT-NVI.

V. Ondersteunt NVI Skinny ALG, H323 ALG en TCP SIP ALG?

A. Nee. UDP SIP ALG (gebruikt door de meeste implementaties) wordt overigens niet beïnvloed.

V. Wordt TCP-segmentatie ondersteund met SNAT?

A. SNAT ondersteunt geen TCP-ALG's (zoals SIP, SKINNY, H323 of DNS). TCP-segmentatie wordt dan ook niet ondersteund. UDP SIP en DNS worden echter wel ondersteund.

SNAT

V. Wat is Stateful NAT (SNAT)?

A. Met SNAT kunnen twee of meer netwerkadresomzetters fungeren als omzettingsgroep. Eén lid van de omzettingsgroep verwerkt verkeer dat omzetting van IP-adresinformatie vereist. Daarnaast wordt de back-upomzetter op de hoogte gesteld van eventuele actieve stromen. De back-upomzetter kan vervolgens informatie van de actieve omzetter gebruiken om dubbele vermeldingen in de omzettingstabel voor te bereiden. Als de actieve omzetter wordt gehinderd door een kritische storing, kan het verkeer snel naar de back-upomzetter worden overgeschakeld. De verkeersstroom blijft doorgaan, aangezien dezelfde netwerkadresomzettingen worden gebruikt en de status van die omzettingen eerder is gedefinieerd.

V. Wordt TCP-segmentatie ondersteund door SNAT?

A. SNAT ondersteunt geen TCP-ALG's (zoals SIP, SKINNY, H323 of DNS). TCP-segmentatie wordt dan ook niet ondersteund. UDP SIP en DNS worden echter wel ondersteund.

V. Ondersteunt SNAT asymmetrische routing?

A. Asymmetrische routing ondersteunt NAT door het gebruik van asymmetrische wachtrijen. Asymmetrische wachtrijen zijn standaard ingeschakeld. Vanaf release 12.4(24)T wordt het gebruik van wachtrijen niet langer ondersteund. Klanten moeten ervoor zorgen dat pakketten correct worden gerouteerd en de juiste vertraging wordt toegevoegd om asymmetrische routing goed te laten verlopen.

NAT-PT (v6 naar v4)

V. Wat is NAT-PT?

A. NAT-PT is omzetting voor NAT van v4 naar v6. Protocolomzetting (NAT-PT) is een IPv6-IPv4-vertaalmechanisme, zoals gedefinieerd in RFC 2765 en RFC 2766 , waardoor apparaten die alleen IPv6 bevatten kunnen communiceren met apparaten die alleen IPv4 bevatten, en vice versa.

V. Wordt NAT-PT ondersteund in het CEF-pad (Cisco Express Forwarding)?

A. NAT-PT wordt niet ondersteund in het CEF-pad.

V. Welke ALG's worden in NAT-PT ondersteund?

A. NAT-PT ondersteunt TFTP/FTP en DNS. Er is geen ondersteuning voor spraak en SNAT in NAT-PT.

V. Wordt NAT-PT ondersteund door ASR 1004?

A. Aggregation services routers (ASR) gebruiken NAT64.

Platformafhankelijke Cisco 7300/7600/6k

V. Is Stateful NAT (SNAT) beschikbaar op Catalyst 6500 in de SX-softwarereeks?

A. SNAT is niet beschikbaar op Catalyst 6500 in de SX-softwarereeks.

V. Wordt VRF-bewuste NAT ondersteund in hardware op de 6k?

A. VRF-bewuste NAT wordt niet ondersteund in hardware op dit platform.

V. Ondersteunen 7600 en Cat6000 VRF-bewuste NAT?

A. Op het 65xx/76xx-platform wordt VRF-bewuste NAT niet ondersteund en de CLI's worden geblokkeerd.

Opmerking: U kunt een ontwerp implementeren door gebruik te maken van een FWSM dat in virtuele contexttransparante modus draait.

Platformafhankelijke Cisco 850

V. Wordt Skinny NAT ALG ondersteund door Cisco 850 in release 12.4T?

A. Nee. Er is geen ondersteuning voor Skinny NAT ALG in release 12.4T voor de 850 Series.

Implementatie van NAT

V. Hoe implementeer ik NAT?

A. Met NAT kunnen private IP-internetwerken niet-geregistreerde IP-adressen gebruiken om verbinding te maken met het internet. NAT zet het private (RFC1918) adres in het interne netwerk om in wettelijke routeerbare adressen voordat pakketten naar een ander netwerk worden doorgestuurd.

V. Hoe implementeer ik NAT met spraak?

A. Dankzij NAT-ondersteuning voor spraakfuncties kunnen SIP-ingesloten berichten die via een router lopen die is geconfigureerd met Network Address Translation (NAT) worden omgezet naar het pakket. Een Application Layer Gateway (ALG) wordt met NAT gebruikt om de spraakpakketten om te zetten.

V. Hoe integreer ik NAT met MPLS VPN's?

A. Dankzij NAT-integratie met MPLS VPN's kunnen meerdere MPLS VPN's op één apparaat worden geconfigureerd om samen te werken. NAT kan bepalen van welke MPLS VPN IP-verkeer wordt ontvangen, zelfs als de MPLS VPN's allemaal hetzelfde IP-adresseringsschema gebruiken. Dankzij deze verbetering kunnen meerdere MPLS VPN-klanten services delen terwijl ze er zeker van zijn dat elke MPLS VPN volledig gescheiden is van de andere.

V. Wordt HSRP voor hoge beschikbaarheid ondersteund door statische toewijzing via NAT?

A. Wanneer een ARP-query (Address Resolution Protocol) wordt geactiveerd voor een adres dat met statische toewijzing via Network Address Translation (NAT) is geconfigureerd en door de router wordt geregeld, reageert NAT met het BIA MAC-adres op de interface waarnaar het ARP verwijst. Twee routers fungeren als actieve en stand-by HSRP. De NAT-binneninterfaces moeten zijn ingeschakeld en geconfigureerd om bij een groep te behoren.

V. Hoe implementeer ik NAT NVI?

A. NAT NVI maakt een einde aan de noodzaak om een interface te configureren als interne of externe NAT.

V. Hoe implementeer ik taakverdeling met NAT?

A. Er zijn twee typen taakverdeling mogelijk met NAT: u kunt inkomende taken verdelen over een reeks servers en u kunt taken voor gebruikersverkeer verdelen via twee of meer ISP's voor verwerking via het internet.

Raadpleeg IOS NAT-taakverdeling via twee ISP-verbindingen voor meer informatie over de verdeling van uitgaande taken.

V. Hoe implementeer ik NAT in combinatie met IPsec?

A. IP Security (IPsec) Encapsulating Security Payload (ESP) wordt ondersteund via NAT en IPSec NAT Transparency.

Dankzij de functie IPsec ESP via NAT kunt u meerdere gelijktijdige IPsec ESP-tunnels of -verbindingen ondersteunen via een Cisco IOS NAT-apparaat dat is geconfigureerd voor overloading of PAT-modus (Port Address Translation).

Met IPSec NAT Transparency kan IPSec-verkeer via NAT- of PAT-punten in het netwerk worden verzonden doordat veel bekende incompatibiliteiten tussen NAT en IPsec zijn aangepakt.

V. Hoe implementeer ik NAT-PT?

A. NAT-PT (Network Address Translation-Protocol Translation) is een IPv6-IPv4-vertaalmechanisme, zoals gedefinieerd in RFC 2765 en RFC 2766 , dat IPv6-apparaten toestaat om te communiceren met apparaten die alleen IPv4 bevatten, en vice versa.

V. Hoe implementeer ik multicast NAT?

A. Het is mogelijk om de bron-IP voor een multicast stream via NAT te verwerken. Er kan geen routekaart worden gebruikt bij dynamische NAT-verwerking voor multicast, alleen een toegangslijst.

Raadpleeg Multicast NAT op Cisco-routers voor meer informatie. De multicast bestemmingsgroep wordt via NAT verwerkt met behulp van een Multicast Service Reflection-oplossing.

V. Hoe implementeer ik stateful NAT (SNAT)?

A. SNAT maakt doorlopende service mogelijk voor dynamisch toegewezen NAT-sessies. Sessies die statistisch worden gedefinieerd hebben het voordeel van redundantie zonder de inzet van SNAT. Bij afwezigheid van SNAT zouden sessies die dynamische NAT-toewijzingen gebruiken tijdens een kritieke storing worden verbroken en opnieuw tot stand moeten worden gebracht. Alleen de minimale SNAT-configuratie wordt ondersteund. Toekomstige implementaties moeten alleen worden uitgevoerd nadat u met het Cisco-accountteam heeft overlegd om het ontwerp te valideren op basis van de huidige beperkingen.

SNAT wordt aanbevolen voor de volgende scenario's:

- Primair/back-up is geen aanbevolen modus, omdat er bepaalde functies ontbreken in vergelijking met HSRP.
- Voor failover-scenario's en voor een configuratie met 2 routers. Als de ene router crasht, neemt de andere router de verwerking naadloos over. (De SNAT-architectuur is niet ontworpen voor het ondervangen van interfacefluctuaties.)
- Scenario voor niet-asymmetrische routing wordt ondersteund. Asymmetrische routing is alleen mogelijk als de latentie in het antwoordpakket hoger is dan die tussen 2 SNAT-routers om de SNAT-berichten uit te wisselen.

SNAT-architectuur is momenteel niet ontworpen voor robuustheid; de volgende handelingen zullen dan ook waarschijnlijk niet slagen:

- Wissen van NAT-vermeldingen terwijl er verkeer is.
- Wijzigen van interfaceparameters (zoals wijzigen van IP-adres, shut/no-shut, enzovoort)

terwijl er verkeer is.

- SNAT-specifieke **clear**- of **show**-opdrachten zullen waarschijnlijk niet goed worden uitgevoerd en worden niet aanbevolen.Enkele SNAT-gerelateerde **clear**- en **show**-opdrachten zijn:

```
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>
```

- Als u vermeldingen wilt wissen, kan de opdracht **clear ip nat trans forced** of **clear ip nat trans *** worden gebruikt.Als u vermeldingen wilt bekijken, kunnen de opdrachten **show ip nat translation**, **show ip nat translations verbose** en **show ip nat stats** worden gebruikt. Als *service internal* is geconfigureerd, zal ook SNAT-specifieke informatie worden getoond.
- Het wissen van NAT-omzettingen op de back-uprouter wordt niet aanbevolen. Wis de NAT-vermeldingen altijd op de primaire SNAT-router.
- SNAT is geen HA; daarom moeten de configuraties op beide routers hetzelfde zijn. Beide routers moeten dezelfde image gebruiken. Zorg ook dat het onderliggende platform dat voor beide SNAT-routers wordt gebruikt hetzelfde is.

Best practices voor NAT

V. Zijn er best practices voor NAT?

A. Ja. Dit zijn best practices voor NAT:

1. Wanneer u zowel dynamische als statische NAT gebruikt, moet de ACL die de regel voor dynamisch NAT instelt de statische lokale hosts uitsluiten zodat er geen overlap is.
2. Wees voorzichtig met het gebruik van ACL voor NAT met **permit ip any any** omdat dit onvoorspelbare resultaten kan opleveren. Na release 12.4(20)T zal NAT lokaal gegenereerde HSRP- en routingprotocolpakketten omzetten als deze naar de buteninterface worden verzonden, evenals lokaal versleutelde pakketten die voldoen aan de NAT-regel.
3. Wanneer u overlappende netwerken voor NAT heeft, moet u het trefwoord **match-in-vrf** gebruiken.U moet het trefwoord **match-in-vrf** toevoegen voor de overlappende statische NAT-vermeldingen voor verschillende VRF's. Het is echter niet mogelijk om algemene adressen en NAT-adressen voor VRF te laten overlappen.

```
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-groepen met hetzelfde adresbereik kunnen niet in verschillende VRF's worden gebruikt, tenzij het trefwoord **match-in-vrf** wordt gebruikt.Voorbeeld:

```
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
```

Opmerking: Ook al is de CLI-configuratie geldig, zonder het trefwoord **match-in-vrf** wordt de configuratie niet ondersteund.

5. Wanneer u taakverdeling van ISP's implementeert met overloading van de NAT-interface, is het raadzaam om route-map met interface-matching te gebruiken in plaats van ACL-matching.
6. Wanneer u groepstoewijzing gebruikt, moet u niet twee verschillende toewijzingen (ACL of routekaart) gebruiken om hetzelfde NAT-groepsadres te delen.
7. Wanneer u dezelfde NAT-regels implementeert op twee verschillende routers in het failover-scenario, moet u HSRP-redundantie gebruiken.
8. Definieer niet hetzelfde interne algemene adres voor statische NAT en een dynamische groep. Dat kan tot ongewenste resultaten leiden.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.