ASA configureren om IPv6-verkeer door te geven

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[IPv6-functieinformatie](#)
[IPv6-Overzicht](#)
[IPv6-verbeteringen via IPv4](#)
[Uitgebreide adresseringsmogelijkheden](#)
[Vereenvoudiging van headerformaat](#)
[Verbeterde ondersteuning voor uitbreidingen en opties](#)
[Capaciteit van stroometikettering](#)
[Verificatie en Privacyfuncties](#)
[Configureren](#)
[Netwerkdiagram](#)
[Interfaces configureren voor IPv6](#)
[IPv6-routing configureren](#)
[Configureer statische routing voor IPv6](#)
[Configuratie van Dynamische routing voor IPv6 met OSPFv3](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Probleemoplossing L2-connectiviteit (ND)](#)
[IPv4 ARP versus IPv6 ND](#)
[ND-debugs](#)
[ND-pakketvastlegging](#)
[ND-systemen](#)
[Probleemoplossing voor fundamentele IPv6-routing](#)
[Routing Protocol-knooppunten voor IPv6](#)
[Handige tonen opdrachten voor IPv6](#)
[Packet Tracers met IPv6](#)
[Volledige lijst met IPv6-gerelateerde ASA-debugs](#)
[Standaard IPv6-gerelateerde problemen](#)
[Onjuist geconfigureerd subnetten](#)
[Gewijzigde EUI 64-codering](#)
[Clients gebruiken tijdelijke IPv6-adressen per standaard](#)
[IPv6-FAQ's](#)

[Kan ik verkeer voor zowel IPv4 als IPv6 op dezelfde interface tegelijkertijd doorgeven?](#)
[Kan ik zowel IPv6 als IPv4 ACL's op dezelfde interface toepassen?](#)
[Ondersteunt de ASA QoS voor IPv6?](#)
[Moet ik NAT met IPv6 gebruiken?](#)
[Waarom zie ik de link-lokale IPv6 adressen in de uitvoer van ***de*** showfailover?](#)
[Bekende voorzorgsmaatregelen/verbeteringsaanvragen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) dient te configureren om internetprotocol versie 6 (IPv6) aan verkeer te onderwerpen in ASA versie 7.0(1) en hoger.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA versies 7.0(1) en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Momenteel is IPv6 wat marktpenetratie betreft nog relatief nieuw. IPv6-configuratieassistentie en het indienen van problemen zijn echter gestaag toegenomen. Dit document heeft tot doel aan deze behoeften tegemoet te komen en te voorzien in:

- Een algemeen overzicht van het gebruik van IPv6
- De basisconfiguratie van IPv6 op de ASA
- Informatie over hoe u IPv6-connectiviteit met de ASA kunt oplossen
- Een lijst van de meest voorkomende IPv6-problemen en oplossingen, zoals geïdentificeerd door het Cisco Technical Assistance Center (TAC)

Opmerking: Gezien het feit dat IPv6 nog in de beginfase is als wereldwijde IPv4-vervanging, zal dit document regelmatig worden bijgewerkt om de nauwkeurigheid en relevantie ervan te behouden.

IPv6-functieinformatie

Hier is een paar belangrijke informatie over de IPv6-functionaliteit:

- Het IPv6-protocol werd voor het eerst geïntroduceerd in ASA versie 7.0(1).
- Ondersteuning voor IPv6 in transparante modus is geïntroduceerd in ASA versie 8.2(1).

IPv6-Overzicht

Het IPv6-protocol werd in het midden tot eind jaren negentig ontwikkeld, voornamelijk door het feit dat de openbare IPv4-adresruimte snel naar uitputting toe is gegaan. Hoewel NAT (Network Address Translation) IPv4 drastisch heeft geholpen en dit probleem heeft uitgesteld, kon niet worden ontkend dat er uiteindelijk een vervangingsprotocol nodig zou zijn. Het IPv6-protocol werd in december 1998 officieel gedetailleerd in RFC 2460. U kunt meer over het protocol lezen in het officiële RFC 2460-document, dat zich bevindt op de website van Internet Engineering Task Force (IETF).

IPv6-verbeteringen via IPv4

In dit gedeelte worden de verbeteringen beschreven die worden meegeleverd met het IPv6-protocol in vergelijking met het oudere IPv4-protocol.

Uitgebreide adresseringsmogelijkheden

Het IPv6-protocol verhoogt de IP-adresgrootte van 32 bits naar 128 bits om meer niveaus van adressering, een veel groter aantal adresseerbare knooppunten en een eenvoudiger automatische configuratie van adressen te ondersteunen. De schaalbaarheid van multicast routing wordt verbeterd door de toevoeging van een scope-veld aan de multicast-adressen. Bovendien wordt een nieuw type adres, een *elk cast adres* genoemd, gedefinieerd. Dit wordt gebruikt om een pakje naar een willekeurig knooppunt in een groep te verzenden.

Vereenvoudiging van headerformaat

Sommige IPv4-veldnamenvelden zijn gevallen of optioneel gemaakt om de gewone verwerkingskosten van pakkethantering te verlagen en om de bandbreedte-kosten van de IPv6-header te beperken.

Verbeterde ondersteuning voor uitbreidingen en opties

Veranderingen in de manier waarop de IP-headeropties worden gecodeerd maken het efficiënter

verzenden mogelijk, minder strenge limieten aan de lengte van opties en meer flexibiliteit voor de introductie van nieuwe opties in de toekomst.

Capaciteit van stroometikettering

Er wordt een nieuwe mogelijkheid toegevoegd om de etikettering mogelijk te maken van pakketten die behoren tot specifieke *verkeersstromen* waarvoor de afzender speciale behandeling vraagt, zoals non-default Quality of Service (QoS) of *real-time* service.

Verificatie en Privacyfuncties

Uitbreidingen die worden gebruikt ter ondersteuning van authenticatie, gegevensintegriteit en (optionele) gegevensvertrouwelijkheid worden gespecificeerd voor IPv6.

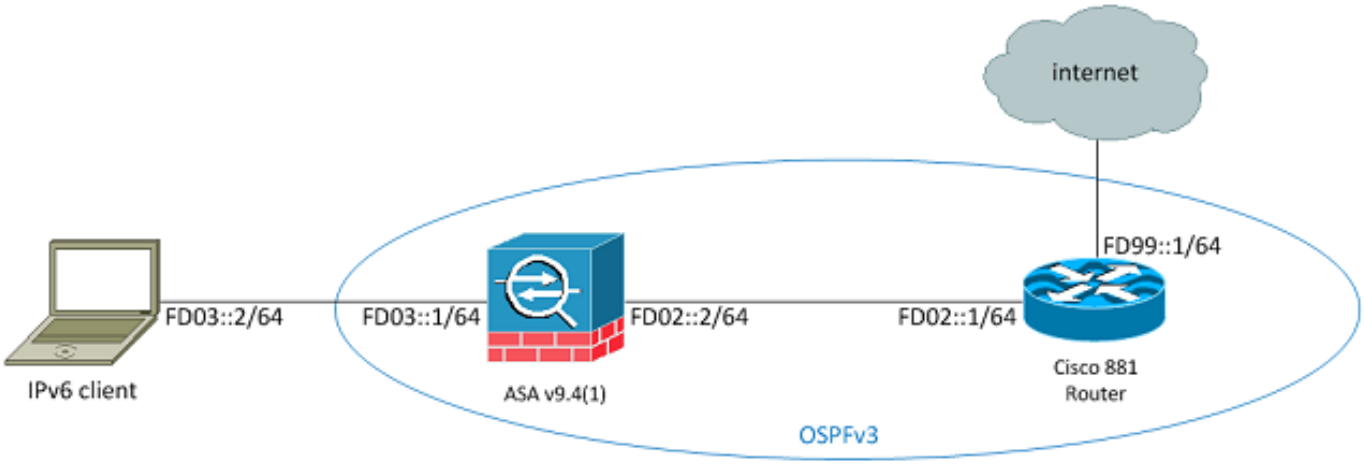
Configureren

In dit gedeelte wordt beschreven hoe u Cisco ASA kunt configureren voor het gebruik van IPv6.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit is de IPv6 topologie voor de voorbeelden die door dit document worden gebruikt:



Interfaces configureren voor IPv6

Om het IPv6-verkeer door een ASA te laten passeren moet u eerst IPv6 op minstens twee interfaces inschakelen. Dit voorbeeld beschrijft hoe IPv6 kan worden ingeschakeld om verkeer van de binneninterface op **Gi0/0** naar de buiteninterface op **Gi0/1** over te **brengen**:

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 enable

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 enable
```

U kunt nu de IPv6-adressen op beide interfaces configureren.

> Opmerking: In dit voorbeeld worden de adressen in de Unieke Local Address (ULA) space van fc00::/7 gebruikt, zodat alle adressen beginnen met **FD** (zoals, fdxx:xxxx:xxxx....). Wanneer u IPv6-adressen schrijft, kunt u ook dubbele kleuren (**:**) gebruiken om een regel van nullen te vertegenwoordigen, zodat **FD01:1/64** hetzelfde is als **FD01:0000:0000:0000:000 000:000:00001**.

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 address fd03::1/64
ASAv(config-if)# nameif inside
ASAv(config-if)# security-level 100

ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 address fd02::2/64
ASAv(config-if)# nameif outside
ASAv(config-if)# security-level 0
```

U zou nu de basisverbinding van Layer 2 (L2)/Layer 3 (L3) aan een upstream router op het buitenVLAN op adres **krw02** moeten hebben**:1**:

```
ASAv(config-if)# ping fd02::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd02::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

IPv6-routing configureren

Net zoals met IPv4, zelfs al is er IPv6 connectiviteit met de hosts op direct aangesloten netwerk, moet u nog de routes naar de externe netwerken hebben om te weten hoe u hen kunt bereiken. Het eerste voorbeeld toont hoe te om een statische standaardroute te vormen om alle IPv6 netwerken via de buiteninterface met een volgende hopadres van **krw02** te bereiken**:1**.

Configureer statische routing voor IPv6

Gebruik deze informatie om de statische routing voor IPv6 te configureren:

```
ASAv(config)# ipv6 route outside 0::0/0 fd02::1
ASAv(config)# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
L fd02::2/128 [0/0]
via ::, outside
```

```
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
S   ::/0 [1/0]
via fd02::1, outsideASAv(config)#
```

Zoals getoond, is er nu connectiviteit aan een gastheer op externe Subnet:

```
ASAv(config)# ping fd99::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd99::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASAv(config)#
```

> Opmerking: Als een dynamisch routingprotocol wordt gewenst om de routing voor IPv6 aan te pakken, kunt u dat ook configureren. Dit wordt beschreven in de volgende paragraaf.

Configuratie van Dynamische routing voor IPv6 met OSPFv3

Eerst moet u de configuratie van het Open Kortste Pad Eerste Versie 3 (OSPFv3) op de upstream Cisco 881 Series geïntegreerde services router (ISR) onderzoeken:

```
C881#show run | sec ipv6
ipv6 unicast-routing

!--- This enables IPv6 routing in the Cisco IOS®.

.....
ipv6 ospf 1 area 0
address-family ipv6 unicast
passive-interface default
no passive-interface Vlan302

!--- This is the interface to send OSPF Hellos to the ASA.

default-information originate always

!--- Always distribute the default route.

redistribute static
ipv6 route ::/0 FD99::2

!--- Creates a static default route for IPv6 to the internet.
```

Hier is de relevante interfaceconfiguratie:

```
C881#show run int Vlan302
```

```
interface Vlan302
....
ipv6 address FD02::1/64
ipv6 ospf 1 area 0
C881#
```

U kunt ASA-pakketvastlegging gebruiken om te controleren of de OSPF-*Hallo*-pakketten gezien worden van ISR op de externe interface:

```
ASAv(config)# show run access-list test_ipv6
access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# show cap
capture capout type raw-data access-list test_ipv6 interface outside
[Capturing - 37976 bytes]
ASAv(config)# show cap capout

367 packets captured

1: 11:12:04.949474 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
2: 11:12:06.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
   3: 11:12:07.854768       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
4: 11:12:07.946545 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
5: 11:12:08.949459 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
6: 11:12:09.542772 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
....
  13: 11:12:16.983011       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
14: 11:12:18.947170 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
15: 11:12:19.394831 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
16: 11:12:19.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
  21: 11:12:26.107477       fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
ASAv(config)#
```

In de vorige pakketvastlegging kunt u zien dat de OSPF-pakketten (ip-proto-89) van het IPv6 link-plaatselijk adres komen, dat overeenkomt met de juiste interface op ISR:

```
C881#show ipv6 interface brief
......
Vlan302 [up/up]
    FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

U kunt nu een OSPFv3 proces op de ASA om een nabijheid met ISR te maken:

```
ASAv(config)# ipv6 router ospf 1
ASAv(config-rtr)# passive-interface default
ASAv(config-rtr)# no passive-interface outside
ASAv(config-rtr)# log-adjacency-changes
ASAv(config-rtr)# redistribute connected
ASAv(config-rtr)# exit
```

Pas de OSPF-configuratie op de ASA-externe interface toe:

```
ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 ospf 1 area 0
ASAv(config-if)# end
```

Dit zou de ASA moeten veroorzaken om de pakketten van de uitzendingOSPF Hallo op IPv6 te verzenden. Voer de opdracht **Show ipv6 ospf-buur in** om nabijheid met de router te verifiëren:

```
ASAv# show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface
    14.38.104.1 1     FULL/BDR        0:00:33     14              outside
```

U kunt de buurID op ISR ook bevestigen, aangezien het het hoogste geconfigureerde IPv4-adres voor de ID standaard gebruikt:

```
C881#show ipv6 ospf 1
 Routing Process "ospfv3 1" with ID 14.38.104.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
static
 Originate Default Route with always

!--- Notice the other OSPF settings that were configured.

Router is not originating router-LSAs with maximum metric
....

C881#
```

De ASA had nu de standaard IPv6 route van de ISR moeten leren. Om dit te bevestigen, voer de **show ipv6 route** opdracht in:

```
ASAv# show ipv6 route

IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
O 2001:aaaa:aaaa:aaaa::/64 [110/10]
via ::, outside
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
OE2  ::/0 [110/1], tag 1

!--- Here is the learned default route.
```

```
    via fe80::c671:feff:fe93:b516, outside
ASAv#
```

De basisconfiguratie van de interface-instellingen en de routingfuncties voor IPv6 in de ASA is nu voltooid.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

De procedures voor het opsporen en verhelpen van IPv6-connectiviteit volgen het grootste deel van de zelfde methodologie die wordt gebruikt om IPv4-connectiviteit op te lossen, met een paar verschillen. Vanuit het perspectief van probleemoplossing is een van de belangrijkste verschillen tussen IPv4 en IPv6 dat het Protocol voor adresoplossing (ARP) niet langer in IPv6 bestaat. In plaats van het gebruik van ARP om IP-adressen op het lokale LAN-segment op te lossen, gebruikt IPv6 een protocol dat ND (Nabbor Discovery) wordt genoemd.

Het is ook belangrijk om te begrijpen dat ND gebruik maakt van Internet Control Message Protocol, versie 6 (ICMPv6), voor de adresresolutie van Media Access Control (MAC). Meer informatie over IPv6-ND is te vinden in de ASA IPv6 Configuration-handleiding in het gedeelte IPv6-buurtdetectie van het *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4* of in RFC 4861.

Op dit moment impliceert de meeste IPv6-gerelateerde problemen met betrekking tot het oplossen van problemen of ND, routing of SUBNET-configuratieproblemen. Dit is waarschijnlijk te wijten aan het feit dat deze ook de belangrijkste verschillen zijn tussen IPv4 en IPv6. De ND werkt anders dan ARP en de interne netwerkadressering is ook heel anders, omdat het gebruik van NAT in IPv6 sterk wordt ontmoedigd en privé-adressering niet langer zo heftig is als in IPv4 (na RFC 1918). Zodra deze verschillen worden begrepen en/of de L2/L3 problemen worden opgelost, is het proces van het opsporen en verhelpen bij Layer 4 (L4) en hoger in wezen hetzelfde als het proces dat voor IPv4 wordt gebruikt omdat de TCP/UDP- en hoger-laagprotocollen in wezen hetzelfde functioneren (ongeacht de IP-versie die wordt gebruikt).

Probleemoplossing L2-connectiviteit (ND)

De meest fundamentele opdracht die wordt gebruikt om L2-connectiviteit met IPv6 in een probleemoplossing te brengen, is de opdracht **Show ipv6 buurman [name if]**, die het equivalent van de **show arp** voor IPv4 is.

Hier wordt een voorbeeld uitgevoerd:

```
ASAv(config)# show ipv6 neighbor outside
IPv6 Address Age Link-layer Addr State Interface
fd02::1                                   0 c471.fe93.b516  REACH   outside
fe80::c671:feff:fe93:b516                32 c471.fe93.b516  DELAY   outside
fe80::e25f:b9ff:fe3f:1bbf 101 e05f.b93f.1bbf STALE outside
fe80::b2aa:77ff:fe7c:8412 101 b0aa.777c.8412 STALE outside
```

```
fe80::213:c4ff:fe80:5f53 101 0013.c480.5f53 STALE outside
fe80::a64c:11ff:fe2a:60f4 101 a44c.112a.60f4 STALE outside
fe80::217:fff:fe17:af80 99 0017.0f17.af80 STALE outside
ASAv(config)#
```

In deze uitvoer kunt u de succesvolle resolutie zien voor het IPv6-adres van **krw02:1**, dat aan het apparaat toebehoort met een MAC-adres van **c471.fe93.b516**.

> Opmerking: U kunt opmerken dat het zelfde adres van de router interface MAC tweemaal in de vorige uitvoer verschijnt omdat de router ook een zelf-toegewezen verbinding-lokaal adres voor deze interface heeft. Het link-lokale adres is een apparaat-specifiek adres dat slechts voor communicatie op het direct aangesloten netwerk kan worden gebruikt. De routers sturen geen pakketten door via link-lokale adressen, maar zijn eerder slechts voor communicatie op het direct aangesloten netwerksegment. Veel IPv6-routingprotocollen (zoals OSPFv3) gebruiken link-lokale adressen om routing-protocolinformatie op het L2-segment te delen.

Om het ND cache te ontruimen, dient u de **duidelijke ipv6 buren** opdracht in. Als ND voor een bepaalde host mislukt, kunt u de **debug ipv6 en** opdracht invoeren, evenals pakketvastlegging uitvoeren en de syslogs controleren om te bepalen wat op L2 niveau optreedt. Onthoud dat IPv6 ND ICMPv6-berichten gebruikt om de MAC-adressen voor IPv6-adressen op te lossen.

IPv4 ARP versus IPv6 ND

Denk aan deze vergelijkingstabel van ARP voor IPv4 en ND voor IPv6:

IPv4 ARP	IPv6-netwerkmodule
ARP-VERZOEK (Wie heeft 10.10.10.1?)	buurtaanvraag
ARP REPLY (10.10.10.1 is bij dood.dood)	buurtadvertenties

In het volgende scenario lost de ND het MAC-adres van de *fd02:1* host niet op die zich op de externe interface bevindt.

ND-debugs

Dit is de uitvoer van **debug ipv6 en** opdracht:

```
ICMPv6-ND: Sending NS for fd02::1 on outside

!--- "Who has fd02::1"

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
ICMPv6-ND: DELETE -> INCMP: fd02::1
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NA for fd02::2 on outside

!--- "fd02::2 is at dead.dead.dead"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: INCMP deleted: fd02::1
ICMPv6-ND: INCMP -> DELETE: fd02::1
ICMPv6-ND: DELETE -> INCMP: fd02::1

!--- Here is where the ND times out.

ICMPv6-ND: Sending NS for fd02::1 on outside
ICMPv6-ND: Sending NS for fd02::1 on outside
```

In deze debug uitvoer *lijkt* het alsof de buurtadvertenties van **fd02:2** nooit ontvangen zijn. U kunt de pakketvastlegging controleren om te bevestigen of dit daadwerkelijk het geval is.

ND-pakketvastlegging

> Opmerking: Vanaf ASA release 9.4(1) zijn er nog steeds toegangslijsten vereist voor IPv6-pakketvastlegging. Er is een verbeteringsverzoek ingediend om dit bij Cisco bug-ID CSCtn09836 te volgen.

Configureer de toegangscontrolelijst (ACL) en pakketvastlegging:

```
ASAv(config)# access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# cap capout interface outside access-list test_ipv6
```

Initiate a ping to **fd2:1** uit de ASA:

```
ASAv(config)# show cap capout
....
23: 10:55:10.275284 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
24: 10:55:10.277588 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
26: 10:55:11.287735 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
27: 10:55:11.289642 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
28: 10:55:12.293365 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
29: 10:55:12.298538 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
32: 10:55:14.283341 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
33: 10:55:14.285690 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
35: 10:55:15.287872 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
36: 10:55:15.289825 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
```

Zoals te zien is in de pakketvastlegging worden de buurtadvertenties van **fd2:1** ontvangen. De advertenties worden echter om de een of andere reden niet verwerkt, zoals wordt getoond in de debug-uitgangen. Voor nader onderzoek kunt u de systemen bekijken.

ND-systemen

Hier zijn een paar voorbeelden van ND-blogs:

```
May 13 2015 10:55:10: %ASA-7-609001: Built local-host identity:fd02::2
May 13 2015 10:55:10: %ASA-6-302020: Built outbound ICMP connection for faddr
ff02::1:ff00:1/0 gaddr fd02::2/0 laddr fd02::2/0(any)
May 13 2015 10:55:10: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:10: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:11: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:11: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:12: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:12: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:14: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:14: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:15: %ASA-3-325003: EUI-64 source address check failed.  Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:15: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
```

Binnen deze systemen kunt u zien dat de ND buurtadvertenties van de ISR bij **kringen02:1** worden ingetrokken omdat er geen wijzigingen zijn aangebracht in het uitgebreide unieke identificatienummer (EUI) 64 (Gewijzigde EUI-64).

> **Tip**: Raadpleeg het gedeelte *Gewijzigde EUI-64 adrescodering* van dit document voor meer informatie over dit specifieke probleem. Deze logica voor het oplossen van problemen kan ook worden toegepast op alle soorten dalingsredenen, zoals wanneer de ACLs ICMPv6 op een specifieke interface niet toelaat of wanneer de optie Unicast Reverse Path Forwarding (uRPF) fouten voor de controles voorkomen, die beiden L2 aansluitingskwesties met IPv6 kunnen veroorzaken.

Probleemoplossing voor fundamentele IPv6-routing

De procedures voor het oplossen van problemen bij het routeren van protocollen wanneer IPv6 wordt gebruikt zijn in wezen hetzelfde als de procedures wanneer IPv4 wordt gebruikt. Het gebruik van **debug** en **show** opdrachten, zowel als pakketvastlegging, is handig met pogingen om de reden vast te stellen dat een routingprotocol zich niet gedraagt zoals verwacht.

Routing Protocol-knooppunten voor IPv6

Deze sectie verschaft de nuttige debug-opdrachten voor IPv6.

Wereldwijde IPv6-routingknooppunten

U kunt de **debug ipv6-routing** debug gebruiken om alle wijzigingen in de IPv6-routingtabel op te lossen:

```
ASAv# clear ipv6 ospf 1 proc

Reset OSPF process? [no]: yes
ASAv# IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, Delete 2001:aaaa:aaaa:aaaa::/64 from table
IPv6RT0: ospfv3 1, Delete backup for fd02::/64
IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ospfv3 1, Delete ::/0 from table
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Add 2001:aaaa:aaaa:aaaa::/64 to table
IPv6RT0: ospfv3 1, Added next-hop :: over outside for 2001:aaaa:aaaa:aaaa::/64,
[110/10]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516
nh_source fe80::c671:feff:fe93:b516 via interface outside route-type 16
IPv6RT0: ospfv3 1, Add ::/0 to table
IPv6RT0: ospfv3 1, Added next-hop fe80::c671:feff:fe93:b516 over outside for ::/0,
[110/1]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Route add 2001:aaaa:aaaa:aaaa::/64 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Reuse backup for fd02::/64, distance 110
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516 nh_source fe80::c671:feff:fe93:b516 via interface outside
route-type 16
IPv6RT0: ospfv3 1, Route add ::/0 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
```

OSPFv3-apparaten

U kunt de opdracht **debug ipv6 ospf** gebruiken om problemen met OSPFv3 op te lossen:

```
ASAv# debug ipv6 ospf ?

adj OSPF adjacency events
database-timer OSPF database timer
events OSPF events
flood OSPF flooding
graceful-restart OSPF Graceful Restart processing
hello OSPF hello events
ipsec OSPF ipsec events
lsa-generation OSPF lsa generation
```

```
lsdb OSPF database modifications
packet OSPF packets
retransmission OSPF retransmission events
spf OSPF spf
```

Hier is een voorbeeldoutput voor alle apparaten die worden toegelaten nadat het OSPFv3 proces opnieuw is begonnen:

```
ASAv# clear ipv6 ospf 1
OSPFv3: rcv. v:3 t:1 l:44 rid:192.168.128.115
aid:0.0.0.0 chk:a9ac inst:0 from outside
OSPFv3: Rcv hello from 192.168.128.115 area 0 from outside fe80::217:fff:fe17:af80
interface ID 142
OSPFv3: End of hello processingpr
OSPFv3: rcv. v:3 t:1 l:44 rid:14.38.104.1
aid:0.0.0.0 chk:bbf3 inst:0 from outside
OSPFv3: Rcv hello from 14.38.104.1 area 0 from outside fe80::c671:feff:fe93:b516
interface ID 14
OSPFv3: End of hello processingo
ASAv# clear ipv6 ospf 1 process

Reset OSPF process? [no]: yes
ASAv#
OSPFv3: Flushing External Links
Insert LSA 0 adv_rtr 172.16.118.1, type 0x4005 in maxage
OSPFv3: Add Type 0x4005 LSA ID 0.0.0.0 Adv rtr 172.16.118.1 Seq 80000029 to outside
14.38.104.1 retransmission list
....

!--- The neighbor goes down:

OSPFv3: Neighbor change Event on interface outside
OSPFv3: DR/BDR election on outside
OSPFv3: Elect BDR 14.38.104.1
OSPFv3: Elect DR 192.168.128.115
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Prefix DR LSA intf outside
OSPFv3: Schedule Prefix Stub LSA area 0
OSPFv3: 14.38.104.1 address fe80::c671:feff:fe93:b516 on outside is dead, state DOWN
....

!--- The neighbor resumes the exchange:

OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0xd09 opt 0x0013 flag 0x7 len 28
 mtu 1500 state EXSTART
OSPFv3: First DBD and we are not SLAVE
OSPFv3: rcv. v:3 t:2 l:168 rid:14.38.104.1
     aid:0.0.0.0 chk:5aa3 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x914 opt 0x0013 flag 0x2 len 168
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the MASTER
OSPFv3: outside Nbr 14.38.104.1: Summary list built, size 0
OSPFv3: Send DBD to 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x1 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:192.168.128.115
     aid:0.0.0.0 chk:295c inst:0 from outside
OSPFv3: Rcv DBD from 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x7 len 28
 mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the SLAVE
OSPFv3: outside Nbr 192.168.128.115: Summary list built, size 0
OSPFv3: Send DBD to 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x0 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:14.38.104.1
     aid:0.0.0.0 chk:8d74 inst:0 from outside
```

```
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x0 len 28
 mtu 1500 state EXCHANGE
....

!--- The routing is re-added to the OSPFv3 neighbor list:

OSPFv3: Add Router 14.38.104.1 via fe80::c671:feff:fe93:b516, metric: 10
 Router LSA 14.38.104.1/0, 1 links
   Link 0, int 14, nbr 192.168.128.115, nbr int 142, type 2, cost 1
     Ignore newdist 11 olddist 10
```

Enhanced Interior Gateway Routing Protocol (NGEW)

Ecu op de ASA steunt het gebruik van IPv6 niet. Verwijs naar de Richtsnoeren voor sectie Ecu van het *CLI Boek 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4* voor meer informatie.

Border Gateway Protocol (BGP)

Deze **debug** opdracht kan worden gebruikt om BGP problemen op te lossen wanneer IPv6 wordt gebruikt:

```
ASAv# debug ip bgp ipv6 unicast  ?

X:X:X:X::X IPv6 BGP neighbor address
keepalives BGP keepalives
updates BGP updates
<cr>
```

Handige tonen opdrachten voor IPv6

U kunt deze opdrachten **tonen** gebruiken om IPv6-problemen op te lossen:

- **tonen ipv6-route**
- **samenvatting van ipv6-interface**
- **ipv6 ospf <proces-ID> tonen**
- **IPv6-verkeer tonen**
- **tonen ipv6-buurman**
- **toon ipv6 icmp**

Packet Tracers met IPv6

U kunt de ingebouwde pakkettracer-functionaliteit met IPv6 op de ASA op dezelfde manier gebruiken als met IPv4. Hier is een voorbeeld waar de pakkettracer-functionaliteit wordt gebruikt om de binnenhost op **krw03** te simuleren**:2**, die probeert verbinding te maken met een webserver op **555:1** die op het internet met de standaardroute is gevestigd dat geleerd wordt van de **881** interface via OSPF:

```
ASAv# packet-tracer input inside tcp fd03::2 10000 5555::1 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd59ca0f0, priority=1, domain=permit, deny=false
       hits=2734, user_data=0x0, cs_id=0x0, l3_type=0xdd86
       src mac=0000.0000.0000, mask=0000.0000.0000
       dst mac=0000.0000.0000, mask=0100.0000.0000
       input_ifc=inside, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop fe80::c671:feff:fe93:b516 using egress ifc  outside

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7fffd589cc30, priority=1, domain=nat-per-session, deny=true
       hits=1166, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=6
       src ip/id=::/0, port=0, tag=any
       dst ip/id=::/0, port=0, tag=any
       input_ifc=any, output_ifc=any

<<truncated output>>

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

ASAv#
```

Merk op dat het IP-adres het link-lokale adres van de 881-interface is. Zoals eerder vermeld, gebruiken routers voor vele dynamische routingprotocollen link-lokale IPv6-adressen om nabijheid te maken.

Volledige lijst met IPv6-gerelateerde ASA-debugs

Hier zijn de knoppen die kunnen worden gebruikt om IPv6-problemen op te lossen:

```
ASAv# debug ipv6 ?

dhcp IPv6 generic dhcp protocol debugging
dhcprelay IPv6 dhcp relay debugging
icmp ICMPv6 debugging
interface IPv6 interface debugging
mld IPv6 Multicast Listener Discovery debugging
nd IPv6 Neighbor Discovery debugging
ospf OSPF information
packet IPv6 packet debugging
routing IPv6 routing table debugging
```

Standaard IPv6-gerelateerde problemen

In dit gedeelte wordt beschreven hoe u de meest voorkomende IPv6-gerelateerde problemen kunt oplossen.

Onjuist geconfigureerd subnetten

Veel IPv6-TAC-gevallen worden gegenereerd door een algemeen gebrek aan kennis over de manier waarop IPv6 functioneert, of door pogingen van een beheerder om IPv6 te implementeren met behulp van IPv4-specifieke processen.

Bijvoorbeeld, heeft de TAC cases gezien waar een beheerder een \56 blok IPv6-adressen heeft toegewezen door een Internet Service Provider (ISP). De beheerder wijst dan een adres en het volledige \56 subtype toe aan de ASA externe interface en verkiest wat intern bereik om voor de binnenservers te gebruiken. Echter, met IPv6, zouden alle interne hosts ook routeerbare IPv6-adressen moeten gebruiken, en zou het IPv6-adresblok indien nodig moeten worden afgebroken in kleinere subnetten. In dit scenario kunt u vele \64 subnetten maken als deel van het \56 blok dat is toegewezen.

> **Tip**: Raadpleeg RFC 4291 voor aanvullende informatie.

Gewijzigde EUI 64-codering

De ASA kan zo worden geconfigureerd dat er aangepaste EUI-64-gecodeerde IPv6-adressen nodig zijn. Overeenkomstig RFC 4291 staat de EUI een host toe zichzelf een unieke 64-bits IPv6-interface-identificator (EUI-64) toe te wijzen. Deze optie is een voordeel in vergelijking met IPv4 aangezien het de vereiste om DHCP te gebruiken voor de IPv6 adrestoewijzing verwijdert.

Als de ASA zo is geconfigureerd dat deze versterking nodig is via de **ipv6-code64-naam indien** opdracht, dan zal deze waarschijnlijk veel zoekopdrachten en advertenties voor buurtzoekers op het lokale net laten vallen.

> **Tip**: Raadpleeg voor meer informatie het begrijpende IPv6 EUI-64-bits Cisco Support Community-document.

Clients gebruiken tijdelijke IPv6-adressen per standaard

Standaard gebruiken veel client-besturingssystemen (OS's), zoals Microsoft Windows versies 7 en 8, Macintosh OS-X en Linux-gebaseerde systemen, zelf-toegewezen *tijdelijke* IPv6-adressen voor uitgebreide privacy via IPv6 Stateless adresconfiguratie (SLAAC).

De Cisco TAC heeft sommige gevallen gezien waar dit onverwachte problemen in omgevingen veroorzaakte omdat de hosts verkeer van het tijdelijke adres en niet het statistisch toegewezen adres genereren. Als resultaat hiervan kunnen ACLs en de host-gebaseerde routes het verkeer veroorzaken om of laten vallen of onjuist routeren, wat de host-communicatie doet mislukken.

Er zijn twee methoden om deze situatie aan te pakken. Het gedrag kan afzonderlijk worden uitgeschakeld op de clientsystemen, of u kunt dit gedrag uitschakelen op de ASA- en Cisco IOS® routers. Op de ASA of router kant, moet u de berichtvlag van de RV van de Router Advertisement (RA) wijzigen die dit gedrag veroorzaakt.

Raadpleeg de volgende secties om dit gedrag op de systemen van de individuele klanten uit te schakelen.

Microsoft Windows

Voltooi deze stappen om dit gedrag uit te schakelen op Microsoft Windows-systemen:

1. Open in Microsoft Windows een versnelde opdracht (uitvoeren als beheerder).

2. Typ deze opdracht om de optie voor willekeurige IP-adresproductie uit te schakelen en druk vervolgens op **ENTER**:

   ```
   netsh interface ipv6 set global randomizeidentifiers=disabled
   ```

3. Typ deze opdracht om Microsoft Windows te dwingen de EUI-64-standaard te gebruiken:

   ```
   netsh interface ipv6 set privacy state=disabled
   ```

4. Herstart de machine om de wijzigingen toe te passen.

Macintosh OS-X

Voer in een terminal deze opdracht in om IPv6 SLAAC op de host uit te schakelen tot de volgende herstart:

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=0
```

Om de configuratie permanent te maken, voert u deze opdracht in:

```
sudo sh -c 'echo net.inet6.ip6.use_tempaddr=0 >> /etc/sysctl.conf'
```

Linux

Voer in een terminalshell deze opdracht in:

```
sysctl -w net.ipv6.conf.all.use_tempaddr=0
```

SLAAC vanuit de ASA wereldwijd uitschakelen

De tweede methode die wordt gebruikt om dit gedrag aan te pakken is het RA-bericht aan te passen dat van de ASA naar de klanten wordt gestuurd, waardoor het gebruik van de SLAAC in

gang wordt gezet. U kunt het RA-bericht als volgt wijzigen: voer deze opdracht in de modus *Interface Configuration*:

```
ASAv(config)# interface gigabitEthernet 1/1
ASAv(config-if)# ipv6 nd prefix 2001::db8/32 300 300 no-autoconfig
```

Deze opdracht wijzigt het RA-bericht dat door de ASA wordt verzonden zodat de A-bit-vlag niet wordt ingesteld en de klanten geen tijdelijk IPv6-adres genereren.

> **Tip**: Raadpleeg RFC 4941 voor aanvullende informatie.

IPv6-FAQ's

In dit deel worden een aantal vaak gestelde vragen over het gebruik van IPv6 beschreven.

Kan ik verkeer voor zowel IPv4 als IPv6 op dezelfde interface tegelijkertijd doorgeven?

Ja. U moet IPv6 op de interface eenvoudig inschakelen en zowel een IPv4- als een IPv6-adres aan de interface toewijzen en deze beide typen verkeer tegelijkertijd behandelen.

Kan ik zowel IPv6 als IPv4 ACL's op dezelfde interface toepassen?

U kunt dit in ASA-versies eerder doen dan versie 9.0(1). Vanaf ASA versie 9.0(1), worden alle ACL's op de ASA *verenigd*, wat betekent dat een ACL een mix ondersteunt van zowel IPv4- als IPv6-ingangen in dezelfde ACL.

In ASA versies 9.0(1) en later worden de ACL's eenvoudigweg samengevoegd en wordt de enkele, verenigde ACL's op de interface toegepast via de **access-group** opdracht.

Ondersteunt de ASA QoS voor IPv6?

Ja. ASA ondersteunt politie en prioriteitswachtrij voor IPv6 op dezelfde manier als bij IPv4.

Vanaf ASA versie 9.0(1), worden alle ACL's op de ASA *verenigd*, wat betekent dat een ACL een mix ondersteunt van zowel IPv4- als IPv6-ingangen in dezelfde ACL. Als resultaat hiervan, om het even welke opdrachten QoS die op een klasse-kaart worden uitgevoerd die een ACL aanpast actie op zowel het IPv4 als IPv6 verkeer uitvoeren.

Moet ik NAT met IPv6 gebruiken?

Hoewel NAT voor IPv6 op de ASA kan worden geconfigureerd, is het gebruik van NAT in IPv6 sterk ontmoedigd en onnodig, gezien de bijna oneindige hoeveelheid beschikbare, mondiaal routeerbare IPv6-adressen.

Als NAT in een IPv6-scenario vereist is, kunt u meer informatie vinden over de manier waarop u het kunt configureren in het gedeelte IPv6 NAT-richtlijnen van het *CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.4*.

> Opmerking: Er zijn enkele richtlijnen en beperkingen die in overweging moeten worden genomen wanneer u NAT met IPv6 implementeert.

Waarom zie ik de link-lokale IPv6 adressen in de uitvoer van *de* showfailover?

In IPv6 gebruikt ND link-lokale adressen om L2 adresresolutie uit te voeren. Om deze reden, tonen de IPv6 adressen voor de gecontroleerde interfaces in de opdrachtoutput van de **show** failover het link-lokale adres en niet het globale IPv6 adres dat op de interface wordt gevormd. Dit wordt verwacht.

Bekende voorzorgsmaatregelen/verbeteringsaanvragen

Hier zijn een aantal bekende voorbehouden ten aanzien van het gebruik van IPv6:

- Cisco bug-ID CSCtn09836, *-ASA 8.x-opnameclausule niet bij IPv6-verkeer past*
- Cisco bug-ID CSCuq85949-ß--Hiermee kan *ENH: ASA IPv6-ondersteuning voor WCCP*
- Cisco bug-ID CSCut78380, *-ASA IPv6-routing niet-taakverdeling voor verkeer*

Gerelateerde informatie

- RFC 2460---Internet-protocol, versie 6 (IPv6)-specificaties
- RFC 4291, -IP, versie 6, adresseringsarchitectuur
- RFC 4861, -buurman -ontdekking voor IP, versie 6 (IPv6)
- CLI-boek 1: Cisco ASA Series General Operations CLI-configuratiegids, 9.4 -Cv IPv6
- AnyConnect SSL via IPv4+IPv6 naar ASA-configuratie
- Technische ondersteuning en documentatie uHE-systemen