Konfigurieren der ASA für die Weiterleitung von IPv6-Datenverkehr

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Adaptive Security Appliance (ASA) so konfiguriert wird, dass IPv6-Datenverkehr (Internet Protocol Version 6) in ASA 7.0(1) und höher weitergeleitet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA Version 7.0(1) und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Derzeit ist IPv6 im Hinblick auf die Marktdurchdringung noch relativ neu. Die Unterstützung bei der IPv6-Konfiguration und die Fehlerbehebung sind jedoch stetig gestiegen. Dieses Dokument soll diese Anforderungen erfüllen und Folgendes bieten:

- Ein allgemeiner Überblick über die IPv6-Nutzung
- Die grundlegenden IPv6-Konfigurationen auf der ASA
- Informationen zur Fehlerbehebung bei IPv6-Verbindungen über die ASA
- Eine Liste der häufigsten IPv6-Probleme und -Lösungen, die vom Cisco Technical Assistance

Center (TAC) identifiziert wurden

Hinweis: Da sich IPv6 noch in der Anfangsphase als globale IPv4-Ersetzung befindet, wird dieses Dokument regelmäßig aktualisiert, um Genauigkeit und Relevanz zu gewährleisten.

IPv6-Funktionsinformationen

Hier einige wichtige Informationen zur IPv6-Funktionalität:

- Das IPv6-Protokoll wurde erstmals in der ASA-Version 7.0(1) eingeführt.
- Die Unterstützung von IPv6 im transparenten Modus wurde in der ASA Version 8.2(1) eingeführt.

IPv6 - Überblick

Das IPv6-Protokoll wurde Mitte bis Ende der 1990er Jahre entwickelt, hauptsächlich aufgrund der Tatsache, dass der öffentliche IPv4-Adressbereich schnell in die Erschöpfung überging. Obwohl Network Address Translation (NAT) IPv4 erheblich unterstützte und dieses Problem verzögerte, wurde unumstritten, dass ein Ersatzprotokoll erforderlich sein würde. Das IPv6-Protokoll wurde im Dezember 1998 offiziell in RFC 2460 beschrieben. Weitere Informationen zum Protokoll finden Sie im offiziellen RFC 2460-Dokument auf der IETF-Website (Internet Engineering Task Force).

IPv6-Verbesserungen gegenüber IPv4

In diesem Abschnitt werden die Verbesserungen beschrieben, die im Vergleich zum älteren IPv4-Protokoll im IPv6-Protokoll enthalten sind.

Erweiterte Adressierungsfunktionen

Das IPv6-Protokoll erhöht die Größe der IP-Adressen von 32 Bit auf 128 Bit, um eine größere Anzahl adressierbarer Knoten und eine einfachere automatische Konfiguration der Adressen zu unterstützen. Die Skalierbarkeit des Multicast-Routings wird durch Hinzufügen eines *Bereichsfelds* zu den Multicast-Adressen verbessert. Zusätzlich wird ein neuer Adresstyp, eine *Anycast-Adresse* genannt, definiert. Dies wird verwendet, um ein Paket an einen beliebigen Knoten in einer Gruppe zu senden.

Vereinfachung des Header-Formats

Einige IPv4-Header-Felder wurden verworfen oder als optionale Option ausgewählt, um die üblichen Verarbeitungskosten für die Paketverarbeitung zu reduzieren und die Bandbreitenkosten des IPv6-Headers zu begrenzen.

Verbesserte Unterstützung für Erweiterungen und Optionen

Änderungen bei der Kodierung der IP-Header-Optionen ermöglichen eine effizientere Weiterleitung, weniger strenge Beschränkungen bei der Länge von Optionen und eine größere Flexibilität bei der Einführung neuer Optionen in der Zukunft.

Flow Label-Funktion

Es wird eine neue Funktion hinzugefügt, um die Kennzeichnung von Paketen zu ermöglichen, die zu bestimmten *Datenverkehrsflüssen* gehören, für die der Absender eine besondere Behandlung anfordert, wie z. B. eine nicht standardmäßige Quality of Service (QoS) oder einen *Echtzeit*-Service.

Authentifizierungs- und Datenschutzfunktionen

Erweiterungen, die zur Unterstützung von Authentifizierung, Datenintegrität und (optionaler) Datensicherheit verwendet werden, sind für IPv6 festgelegt.

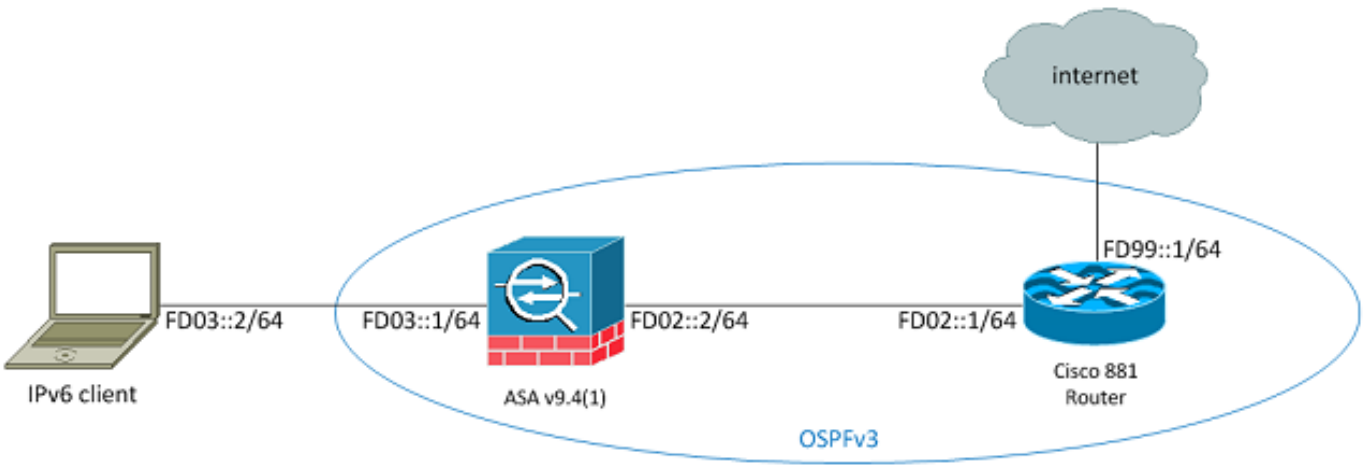
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die Cisco ASA für die Verwendung von IPv6 konfigurieren.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Dies ist die IPv6-Topologie für die in diesem Dokument verwendeten Beispiele:



Konfigurieren von Schnittstellen für IPv6

Um den IPv6-Datenverkehr über eine ASA weiterzuleiten, müssen Sie IPv6 auf mindestens zwei Schnittstellen aktivieren. In diesem Beispiel wird beschrieben, wie IPv6 aktiviert wird, um Datenverkehr von der internen Schnittstelle auf **Gi0/0** an die externe Schnittstelle auf **Gi0/1** weiterzuleiten:

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

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

Sie können nun die IPv6-Adressen auf beiden Schnittstellen konfigurieren.

> **Hinweis**: In diesem Beispiel werden die Adressen im Unique Local Addresses (ULA)-Bereich von fc00:/7 verwendet, sodass alle Adressen mit **FD** beginnen (z. B. fdxx:xxxx:xxxx:xxxx..). Wenn Sie IPv6-Adressen schreiben, können Sie auch doppelte Doppelpunkte (**::**) verwenden, um eine Zeile Nullen so darzustellen, dass **FD01::1/64** mit **FD01:0000:000:000:0000:0000000 übereinstimmt. 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
```

Sie sollten jetzt die grundlegende Layer-2- (L2)/Layer-3- (L3)-Verbindung zu einem Upstream-Router im externen VLAN unter der Adresse **fd02::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
```

Konfigurieren von IPv6-Routing

Ebenso wie bei IPv4 müssen Sie, obwohl IPv6-Verbindungen mit den Hosts im direkt verbundenen Subnetz vorhanden sind, auch über die Routen zu den externen Netzwerken verfügen, um zu wissen, wie Sie diese erreichen können. Das erste Beispiel zeigt, wie eine statische Standardroute konfiguriert wird, um alle IPv6-Netzwerke über die externe Schnittstelle mit einer Next-Hop-Adresse von **fd02::1** zu erreichen.

Statisches Routing für IPv6 konfigurieren

Verwenden Sie diese Informationen, um statisches Routing für IPv6 zu konfigurieren:

```
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)#
```

Wie gezeigt, besteht jetzt eine Verbindung zu einem Host in einem externen Subnetz:

```
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)#
```

> **Hinweis**: Wenn ein dynamisches Routing-Protokoll zur Verarbeitung des Routing für IPv6 gewünscht wird, können Sie dies ebenfalls konfigurieren. Dies wird im nächsten Abschnitt beschrieben.

Dynamisches Routing für IPv6 mit OSPFv3 konfigurieren

Zunächst sollten Sie die Konfiguration für Open Shortest Path First Version 3 (OSPFv3) auf dem Cisco Integrated Services Router (ISR) der Serie 881 überprüfen:

```
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.
```

Die relevante Schnittstellenkonfiguration ist wie folgt:

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

Sie können ASA-Paketerfassungen verwenden, um zu überprüfen, ob die OSPF *Hello*-Pakete vom ISR auf der externen Schnittstelle erkannt werden:

```
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 der vorherigen Paketerfassung sehen Sie, dass die OSPF-Pakete (**ip-proto-89**) von der IPv6-Link-Local-Adresse eingehen, die der richtigen Schnittstelle auf dem ISR entspricht:

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

Sie können jetzt auf der ASA einen OSPFv3-Prozess erstellen, um eine Adjacency mit dem ISR einzurichten:

```
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
```

Wenden Sie die OSPF-Konfiguration auf die externe ASA-Schnittstelle an:

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

Dies sollte dazu führen, dass die ASA die Broadcast-OSPF Hello-Pakete im IPv6-Subnetz sendet. Geben Sie den Befehl **show ipv6 ospf neighbor** ein, um die Adjazenz zum Router zu überprüfen:

```
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
```

Sie können auch die Nachbar-ID auf dem ISR bestätigen, da dieser standardmäßig die am höchsten konfigurierte IPv4-Adresse für die ID verwendet:

```
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#
```

Die ASA sollte jetzt die Standard-IPv6-Route vom ISR gelernt haben. Um dies zu bestätigen, geben Sie den Befehl **show ipv6 route** ein:

```
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#
```

Die grundlegende Konfiguration der Schnittstelleneinstellungen und der Routing-Funktionen für IPv6 auf der ASA ist nun abgeschlossen.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Die Fehlerbehebungsverfahren für IPv6-Verbindungen folgen weitgehend derselben Methode, die zur Fehlerbehebung bei IPv4-Verbindungen verwendet wird, mit einigen Abweichungen. Was die Fehlerbehebung angeht, so ist einer der wichtigsten Unterschiede zwischen IPv4 und IPv6, dass das Address Resolution Protocol (ARP) in IPv6 nicht mehr existiert. Anstelle von ARP zur Auflösung von IP-Adressen im lokalen LAN-Segment verwendet IPv6 ein Protokoll namens Neighbor Discovery (ND).

Es ist auch wichtig zu verstehen, dass ND Internet Control Message Protocol Version 6 (ICMPv6) für die Auflösung von MAC-Adressen (Media Access Control) nutzt. Weitere Informationen zu IPv6 ND finden Sie im ASA IPv6 Configuration Guide im Abschnitt IPv6 Neighbor Discovery im *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4* oder in RFC 4861.

Die meisten Probleme im Zusammenhang mit IPv6 betreffen derzeit ND-, Routing- oder Subnetz-Konfigurationsprobleme. Dies ist wahrscheinlich darauf zurückzuführen, dass es sich dabei auch um die wichtigsten Unterschiede zwischen IPv4 und IPv6 handelt. Die ND arbeitet anders als ARP, und die interne Netzwerkadressierung ist ebenfalls ganz anders, da die Verwendung von NAT bei IPv6 stark abgeschreckt wird und die private Adressierung nicht mehr so genutzt wird wie bei IPv4 (nach RFC 1918). Wenn diese Unterschiede verstanden und/oder die L2/L3-Probleme behoben wurden, entspricht der Fehlerbehebungsprozess auf Layer 4 (L4) und höher im Wesentlichen dem für IPv4, da die TCP/UDP- und die Protokolle höherer Schichten im Wesentlichen dieselbe Funktion haben (unabhängig von der verwendeten IP-Version).

Fehlerbehebung bei L2-Verbindungen (ND)

Der einfachste Befehl, der zur Fehlerbehebung bei L2-Verbindungen mit IPv6 verwendet wird, ist der Befehl **show ipv6 neighbor [nameif]**, der dem Befehl **show arp** für IPv4 entspricht.

Hier ein Beispiel für die Ausgabe:

```
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 dieser Ausgabe sehen Sie die erfolgreiche Auflösung für die IPv6-Adresse **fd02::1**, die zum Gerät mit der MAC-Adresse **c471.fe93.b516** gehört.

> **Hinweis**: Möglicherweise ist festzustellen, dass dieselbe MAC-Adresse der Router-Schnittstelle in der vorherigen Ausgabe zweimal angezeigt wird, da dem Router auch eine selbst zugewiesene lokale Adresse für diese Schnittstelle zugewiesen ist. Die Link-Local-Adresse ist eine gerätespezifische Adresse, die nur für die Kommunikation im direkt verbundenen Netzwerk verwendet werden kann. Router leiten Pakete nicht über Link-Local-Adressen weiter, sondern nur für die Kommunikation im direkt verbundenen Netzwerksegment. Viele IPv6-Routing-Protokolle (z. B. OSPFv3) verwenden Link-Local-Adressen, um Routing-Protokollinformationen für das L2-Segment freizugeben.

Um den ND-Cache zu löschen, geben Sie den Befehl **clear ipv6 neighbors** ein. Wenn die ND für einen bestimmten Host fehlschlägt, können Sie den Befehl **debug ipv6 nd** eingeben sowie Paketerfassungen durchführen und die Syslogs überprüfen, um festzustellen, was auf der L2-Ebene geschieht. Denken Sie daran, dass die IPv6 ND ICMPv6-Nachrichten verwendet, um die MAC-Adressen für IPv6-Adressen aufzulösen.

IPv4 ARP und IPv6 ND im Vergleich

Betrachten Sie die Vergleichstabelle von ARP für IPv4 und ND für IPv6:

IPv4-ARP	IPv6 ND
ARP-ANFRAGE (Wer hat 10.10.10.1?)	Nachbar-Solication
ARP-ANTWORT (10.10.10.1 ist tot.tot.tot)	Nachbarwerbung

Im nächsten Szenario kann die ND die MAC-Adresse des Hosts *fd02:1*, der sich auf der externen Schnittstelle befindet, nicht auflösen.

ND-Debugger

Hier ist die Ausgabe von **debug ipv6 nd** Befehl:

```
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 dieser Debug-Ausgabe *scheint* es, dass die Nachbarwerbung von **fd02::2** nie empfangen werden. Sie können die Paketerfassungen überprüfen, um zu überprüfen, ob dies tatsächlich der Fall ist.

ND-Paketerfassung

> **Hinweis**: Ab ASA Version 9.4(1) sind für die IPv6-Paketerfassung noch Zugriffslisten erforderlich. Es wurde ein Verbesserungsantrag eingereicht, um dies mit der Cisco Bug-ID CSCtn09836 nachzuverfolgen.

Konfigurieren Sie die Zugriffskontrollliste (ACL) und die Paketerfassung:

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

Initiieren Sie einen Ping an **fd02::1** von der 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]
```

Wie in den Paketerfassungen gezeigt, werden die Nachbarwerbung von **fd02:1** empfangen. Die Werbung wird jedoch aus irgendeinem Grund nicht verarbeitet, wie in den Debug-Ausgaben gezeigt. Für weitere Untersuchungen können Sie sich die Syslogs ansehen.

ND-Syslogs

Hier einige Beispiele für ND-Syslogs:

```
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
```

In diesen Syslogs sehen Sie, dass die NAD Neighbor Advertisement Packets vom ISR bei **fd02::1** aufgrund fehlgeschlagener Modified Extended Unique Identifier (EUI) 64-Formatprüfungen (Modified EUI-64) verloren gehen.

> **Tipp**: Weitere Informationen zu diesem Problem finden Sie im Abschnitt *Modified EUI-64 Address Encoding* dieses Dokuments. Diese Fehlerbehebungslogik kann auch auf alle Arten von Drop-Gründen angewendet werden, z. B. wenn die ACLs ICMPv6 auf einer bestimmten Schnittstelle nicht zulassen oder wenn Fehler bei der Prüfung der Unicast Reverse Path Forwarding (uRPF) auftreten, die beide L2-Verbindungsprobleme bei IPv6 verursachen können.

Fehlerbehebung bei grundlegendem IPv6-Routing

Die Fehlerbehebungsverfahren für Routing-Protokolle bei Verwendung von IPv6 sind im Wesentlichen dieselben wie bei Verwendung von IPv4. Die Verwendung von **Debug**- und **Show**-Befehlen sowie Paketerfassungen ist nützlich, wenn versucht wird, den Grund zu ermitteln, warum sich ein Routing-Protokoll nicht wie erwartet verhält.

Routing-Protokoll-Debugger für IPv6

Dieser Abschnitt enthält die nützlichen Debugbefehle für IPv6.

Globale Debugger für IPv6-Routing

Sie können das **Debug-**Debuggen für **IPv6-Routing** verwenden, um alle Änderungen an der IPv6-Routing-Tabelle zu beheben:

```
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-Debugger

Sie können den Befehl **debug ipv6 ospf** verwenden, um OSPFv3-Probleme zu beheben:

```
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
```

Im Folgenden finden Sie eine Beispielausgabe für alle Debuggen, die nach dem Neustart des OSPFv3-Prozesses aktiviert werden:

```
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 (EIGRP)

Das EIGRP auf der ASA unterstützt die Verwendung von IPv6 nicht. Weitere Informationen finden Sie im Abschnitt Guidelines for EIGRP in *CLI Book 1: Konfigurationsleitfaden für die CLI der Cisco ASA-Serie, 9.4* für weitere Informationen.

Border Gateway Protocol (BGP)

Dieser **Debug-**Befehl kann zur Fehlerbehebung bei BGP verwendet werden, wenn IPv6 verwendet wird:

```
ASAv# debug ip bgp ipv6 unicast  ?

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

Nützliche Show-Befehle für IPv6

Sie können die folgenden **show**-Befehle verwenden, um IPv6-Probleme zu beheben:

- **show ipv6 route**
- **show ipv6 interface brief**
- **show ipv6 ospf <Prozess-ID>**
- **show ipv6-Datenverkehr**
- **show ipv6 neighbor**
- **show ipv6 icmp**

Packet Tracer mit IPv6

Sie können die integrierte Packet-Tracer-Funktion mit IPv6 auf der ASA auf die gleiche Weise verwenden wie mit IPv4. Im folgenden Beispiel wird die Packet-Tracer-Funktion verwendet, um den internen Host bei **fd03::2** zu simulieren, der versucht, eine Verbindung zu einem Webserver unter **555:1 herzustellen, der sich** im Internet befindet und die Standardroute enthält, die von der **881**-Schnittstelle über OSPF gelernt wird:

```
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#
```

Beachten Sie, dass die Ausgangs-MAC-Adresse die lokale Adresse der 881-Schnittstelle ist. Wie bereits erwähnt, verwenden Router bei vielen dynamischen Routing-Protokollen Link-Local-IPv6-Adressen, um Adjacencies einzurichten.

Vollständige Liste der IPv6-bezogenen ASA-Debugs

Im Folgenden finden Sie die Debugger, die zur Behebung von IPv6-Problemen verwendet werden können:

```
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
```

Häufige IPv6-bezogene Probleme

In diesem Abschnitt wird beschrieben, wie Sie die häufigsten Probleme im Zusammenhang mit IPv6 beheben können.

Falsch konfigurierte Subnetze

Viele IPv6-TAC-Tickets werden aufgrund eines allgemeinen Mangels an Wissen über die IPv6-Funktionen oder aufgrund von Administratorversuchen erstellt, IPv6 mithilfe von IPv4-spezifischen Prozessen zu implementieren.

Das TAC hat beispielsweise Fälle gesehen, in denen einem Administrator ein \56-IPv6-Adressblock von einem Internetdienstanbieter (Internet Service Provider, ISP) zugewiesen wurde. Der Administrator weist der externen ASA-Schnittstelle dann eine Adresse und das vollständige \56-Subnetz zu und wählt einen internen Bereich für die internen Server aus. Bei IPv6 sollten jedoch alle internen Hosts auch routingfähige IPv6-Adressen verwenden, und der IPv6-Adressblock sollte bei Bedarf in kleinere Subnetze unterteilt werden. In diesem Szenario können Sie viele \64-Subnetze als Teil des reservierten Blocks \56 erstellen.

> **Tipp**: Weitere Informationen finden Sie unter RFC 4291.

Modifizierte EUI 64-Codierung

Die ASA kann so konfiguriert werden, dass modifizierte EUI-64-codierte IPv6-Adressen erforderlich sind. Die EUI ermöglicht es einem Host gemäß RFC 4291, sich selbst eine eindeutige 64-Bit-IPv6-Schnittstellenkennung (EUI-64) zuzuweisen. Diese Funktion ist gegenüber IPv4 von Vorteil, da DHCP für die IPv6-Adresszuweisung nicht mehr verwendet werden muss.

Wenn die ASA so konfiguriert ist, dass diese Erweiterung über den Befehl **ipv6 enforsiche-eui64 nameif** erforderlich ist, werden wahrscheinlich viele Aufforderungen zur Ermittlung von Netznachbarn und Anzeigen von anderen Hosts im lokalen Subnetz gelöscht.

Tipp: Weitere Informationen finden Sie im Dokument Understanding IPv6 EUI-64 Bit Address Cisco Support Community.

Clients verwenden standardmäßig temporäre IPv6-Adressen.

Standardmäßig verwenden viele Client-Betriebssysteme (OS), wie Microsoft Windows Versionen 7 und 8, Macintosh OS-X und Linux-basierte Systeme, selbst zugewiesene *temporäre* IPv6-Adressen für erweiterten Datenschutz über IPv6 Stateless Address Autoconfiguration (SLAAC).

Das Cisco TAC hat in einigen Fällen unerwartete Probleme in Umgebungen verursacht, da die Hosts Datenverkehr von der temporären Adresse und nicht von der statisch zugewiesenen Adresse generieren. Aus diesem Grund können die ACLs und die Host-basierten Routen dazu führen, dass der Datenverkehr entweder verworfen oder unsachgemäß weitergeleitet wird, wodurch die Host-Kommunikation fehlschlägt.

Es gibt zwei Methoden, um dieser Situation zu begegnen. Das Verhalten kann auf den Client-Systemen einzeln deaktiviert werden, oder Sie können dieses Verhalten auf den ASA- und Cisco IOS®-Routern deaktivieren. Auf der ASA- oder Router-Seite müssen Sie das Router Advertisement (RA) Message Flag ändern, das dieses Verhalten auslöst.

Lesen Sie die folgenden Abschnitte, um dieses Verhalten auf den einzelnen Clientsystemen zu deaktivieren.

Microsoft Windows

Gehen Sie wie folgt vor, um dieses Verhalten auf Microsoft Windows-Systemen zu deaktivieren:

1. Öffnen Sie in Microsoft Windows eine erweiterte Eingabeaufforderung (als Administrator ausführen).

2. Geben Sie diesen Befehl ein, um die Funktion zur Generierung zufälliger IP-Adressen zu deaktivieren, und drücken Sie dann die **Eingabetaste**:

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

3. Geben Sie diesen Befehl ein, um Microsoft Windows zur Verwendung des EUI-64-Standards zu zwingen:

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

4. Starten Sie den Computer neu, um die Änderungen anzuwenden.

Macintosh OS-X

Geben Sie in einem Terminal diesen Befehl ein, um IPv6 SLAAC auf dem Host bis zum nächsten Neustart zu deaktivieren:

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

Geben Sie den folgenden Befehl ein, um die Konfiguration dauerhaft zu machen:

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

Linux

Geben Sie in einer Terminal-Shell den folgenden Befehl ein:

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

Globale Deaktivierung von SLAAC von der ASA

Die zweite Methode, die zur Behebung dieses Verhaltens verwendet wird, besteht in der Änderung der RA-Nachricht, die von der ASA an die Clients gesendet wird, was die Verwendung von SLAAC auslöst. Um die RA-Meldung zu ändern, geben Sie den folgenden Befehl aus dem *Schnittstellenkonfigurationsmodus ein*:

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

Mit diesem Befehl wird die RA-Nachricht, die von der ASA gesendet wird, so geändert, dass das A-Bit-Flag nicht gesetzt ist und die Clients keine temporäre IPv6-Adresse generieren.

> **Tipp**: Weitere Informationen finden Sie unter RFC 4941.

Häufig gestellte Fragen zu IPv6

In diesem Abschnitt werden einige häufig gestellte Fragen zur Verwendung von IPv6 beschrieben.

Kann ich den Datenverkehr für IPv4 und IPv6 gleichzeitig an dieselbe Schnittstelle weiterleiten?

Ja. Sie müssen einfach IPv6 auf der Schnittstelle aktivieren und der Schnittstelle sowohl eine IPv4- als auch eine IPv6-Adresse zuweisen. Beide Arten von Datenverkehr werden gleichzeitig verarbeitet.

Kann ich IPv6- und IPv4-ACLs auf dieselbe Schnittstelle anwenden?

Sie können dies in ASA-Versionen vor Version 9.0(1) tun. Ab ASA Version 9.0(1) sind alle ACLs auf der ASA *vereinheitlicht*, d. h. eine ACL unterstützt eine Mischung aus IPv4- und IPv6-Einträgen in derselben ACL.

In ASA Version 9.0(1) und höher werden die ACLs einfach zusammengeführt, und die einzige, einheitliche ACL wird über den Befehl **access-group** auf die Schnittstelle angewendet.

Unterstützt die ASA QoS für IPv6?

Ja. Die ASA unterstützt Richtlinienvergabe und Prioritätswarteschlangen für IPv6 genauso wie IPv4.

Ab ASA Version 9.0(1) sind alle ACLs auf der ASA *vereinheitlicht*, d. h. eine ACL unterstützt eine Mischung aus IPv4- und IPv6-Einträgen in derselben ACL. Aus diesem Grund werden alle QoS-Befehle, die in einer Klassenzuordnung festgelegt werden, die mit einer ACL übereinstimmt, sowohl für den IPv4- als auch den IPv6-Datenverkehr aktiv.

Soll ich NAT mit IPv6 verwenden?

Obwohl NAT für IPv6 auf der ASA konfiguriert werden kann, wird die Verwendung von NAT in IPv6 angesichts der nahezu unbegrenzten Anzahl an verfügbaren, global routbaren IPv6-Adressen dringend empfohlen und überflüssig.

Wenn NAT in einem IPv6-Szenario erforderlich ist, finden Sie weitere Informationen zur Konfiguration im Abschnitt IPv6 NAT Guidelines im *CLI Book 2: Konfigurationsleitfaden für die CLI-Konfiguration der Cisco ASA-Serie, 9.4*.

> **Hinweis**: Bei der Implementierung von NAT mit IPv6 sollten einige Richtlinien und Einschränkungen beachtet werden.

Warum werden die links-lokalen IPv6-Adressen in der Ausgabe des Befehls *show failover angezeigt*?

In IPv6 verwendet ND zur Durchführung der L2-Adressauflösung lokale Adressen. Aus diesem Grund zeigen die IPv6-Adressen für die überwachten Schnittstellen in der Ausgabe des Befehls **show failover** die lokale Adresse und nicht die globale IPv6-Adresse an, die auf der Schnittstelle konfiguriert ist. Dieses Verhalten wird erwartet.

Bekannte Probleme/Verbesserungsanfragen

Im Folgenden sind einige bekannte Vorbehalte hinsichtlich der Verwendung von IPv6 aufgeführt:

- Cisco Bug ID CSCtn09836 âÂ Â *ASA 8.x capture "match"-Klausel fängt keinen IPv6-Datenverkehr ab*
- Cisco Bug ID CSCuq85949 âÂ Â *ENH: ASA IPv6-Unterstützung für WCCP*
- Cisco Bug ID CSCut78380 âÂ Â *ASA IPv6 ECMP Routing nicht Load Balancing Verkehr*

Zugehörige Informationen

- RFC 2460 âÂ Â Internet Protocol, Version 6 (IPv6)-Spezifikation
- RFC 4291 âÂ Â IP-Adressarchitektur 6
- RFC 4861 âÂ Â Neighbor Discovery für IP Version 6 (IPv6)

- CLI-Buch 1: CLI-Konfigurationsleitfaden für allgemeine Betriebsabläufe der Cisco ASA-Serie, 9,4 â Â IPv6
- Konfiguration von AnyConnect SSL over IPv4+IPv6 auf ASA
- Technischer Support und Dokumentation - Â Â Cisco Systems