Configurar o ASA para passar o tráfego do IPv6

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável de Cisco (ASA) a fim passar o tráfego da versão 6 do protocolo de internet (IPv6) nas versões ASA 7.0(1) e mais atrasado.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada nas versões ASA de Cisco 7.0(1) e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Atualmente, o IPv6 é ainda relativamente novo em termos da penetração do mercado. Contudo, a assistência para a configuração do IPv6 e os pedidos do Troubleshooting aumentaram firmemente. A finalidade deste documento é endereçar aquelas necessidades e fornecê-la:

- Uma visão geral ampla do uso do IPv6
- As configurações básicas do IPv6 no ASA
- Informação sobre como pesquisar defeitos a Conectividade do IPv6 com o ASA
- Uma lista dos problemas e das soluções os mais comuns do IPv6, como identificada pelo centro de assistência técnica da Cisco (TAC)

Note: Dado que o IPv6 está ainda nos estágios iniciais como uma substituição do IPv4 globalmente, este documento será atualizado periodicamente a fim manter a precisão e a importância.

Informação da característica do IPv6

Está aqui alguma informação importante sobre a funcionalidade do IPv6:

- O protocolo do IPv6 foi introduzido primeiramente na versão ASA 7.0(1).
- O apoio para o IPv6 no modo transparente foi introduzido na versão ASA 8.2(1).

Vista geral do IPv6

O protocolo do IPv6 foi desenvolvido no meados de ao final dos anos 90, primeiramente devido ao fato de que o espaço de endereços público do IPv4 se moveu rapidamente para a prostração. Embora o Network Address Translation (NAT) dramaticamente ajudasse o IPv4 e atrasasse este problema, tornou-se incontestável que um protocolo da substituição estaria precisado eventualmente. O protocolo do IPv6 foi detalhado oficialmente no RFC 2460 em dezembro 1998. Você pode ler mais sobre o protocolo no documento oficial do RFC 2460, situado no Web site do Internet Engineering Task Force (IETF).

Melhorias do IPv6 sobre o IPv4

Esta seção descreve as melhorias que são incluídas com o protocolo do IPv6 contra o protocolo mais velho do IPv4.

Capacidades de endereçamento expandidas

O protocolo do IPv6 aumenta o tamanho do endereço IP de Um ou Mais Servidores Cisco ICM NT de 32 bit aos bit 128 a fim apoiar mais níveis da hierarquia do endereçamento, um número muito maior de Nós endereçáveis, e uma configuração automática mais simples dos endereços. A escalabilidade do roteamento de transmissão múltipla é melhorada pela adição de um campo do *espaço aos* endereços de multicast. Adicionalmente, um novo tipo de endereço, chamou um *qualquer endereço de molde*, é definido. Isto é usado a fim enviar um pacote a todo o um nó em um grupo.

Simplificação do formato de cabeçalho

Alguns campos de cabeçalho do IPv4 foram deixados cair ou feitos opcionais a fim reduzir os custos de processamento do comum-caso do pacote que seguram e a fim limitar os custos de largura de banda do encabeçamento do IPv6.

Apoio melhorado para Ramais e opções

Muda na maneira que as opções do cabeçalho IP são codificadas permitem a transmissão dos mais eficiente, limites menos estritos no comprimento das opções, e a maior flexibilidade para a introdução de opções novas no futuro.

Capacidade de rotulagem do fluxo

Uma capacidade nova é adicionada a fim permitir a rotulagem dos pacotes que pertencem aos *fluxos de* tráfego particular para que o remetente pede a manipulação especial, tal como o Qualidade de Serviço (QoS) não-padrão ou o *serviço de tempo real*.

Capacidades da autenticação e da privacidade

Os Ramais que são usados a fim apoiar a autenticação, a integridade de dados, e a confidencialidade de dados (opcional) são especificados para o IPv6.

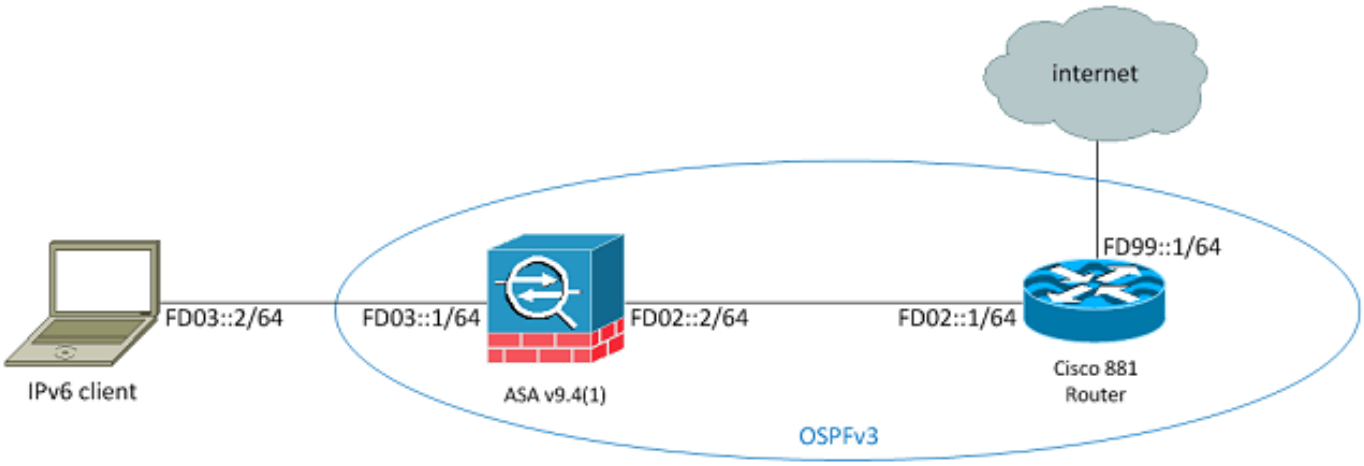
Configurar

Esta seção descreve como configurar Cisco ASA para o uso do IPv6.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Esta é a topologia do IPv6 para os exemplos que são usados durante todo este documento:



Configurar relações para o IPv6

A fim passar o tráfego do IPv6 com um ASA, você deve primeiramente permitir o IPv6 pelo menos em duas relações. Este exemplo descreve como permitir o IPv6 a fim passar o tráfego da

interface interna em **Gi0/0 à** interface externa em **Gi0/1**:

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

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

Você pode agora configurar os endereços do IPv6 em ambas as relações.

> **Note**: Neste exemplo, os endereços no espaço original dos endereços locais (ULA) de fc00::/7 são usados, assim que todos os endereços começam com o **FD** (como, fdxx: xxxx: xxxx….). Também, quando você escreve endereços do IPv6, você pode usar dois pontos dobro (**::**) a fim representar uma linha de zero de modo que **FD01::1/64** seja o mesmo que **FD01:0000:0000:0000:0000:0000:0000:00001**.

```
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
```

Você deve agora ter a camada básica 2 (Conectividade L2)/Layer 3 (L3) a um roteador fluxo acima no VLAN exterior no endereço **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
```

Configurar a distribuição do IPv6

Tal como com o IPv4, mesmo que haja uma Conectividade do IPv6 com os anfitriões na sub-rede conectado diretamente, você deve ainda ter as rotas às redes externas a fim saber alcançá-las. O primeiro exemplo mostra como configurar uma rota padrão estática a fim alcançar todas as redes do IPv6 através da interface externa com um endereço de próximo salto de **fd02::1**.

Configurar o roteamento estático para o IPv6

Use esta informação a fim configurar o roteamento estático para o IPv6:

```
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)#
```

Como mostrado, há agora uma Conectividade a um host em uma sub-rede externo:

```
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)#
```

> **Note**: Se um protocolo de roteamento dinâmico é desejado a fim segurar o roteamento para o IPv6, a seguir você pode configurar aquele também. Isto é descrito na próxima seção.

Configurar o roteamento dinâmico para o IPv6 com OSPFv3

Primeiramente, você deve examinar configuração da versão 3 do caminho mais curto aberto a primeira (OSPFv3) no roteador ascendente dos Serviços integrados do Cisco 881 Series (ISR):

```
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.
```

Está aqui a configuração da interface relevante:

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

Você pode usar capturas de pacote de informação ASA a fim verificar que os pacotes de hello de OSPF estão vistos do ISR na interface externa:

```
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)#
```

Na captação do pacote anterior, você pode ver que os pacotes OSPF (ip-proto-89) chegam do endereço local de link do IPv6, que corresponde à relação correta no ISR:

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

Você pode agora criar um processo OSPFv3 no ASA a fim estabelecer uma adjacência com o ISR:

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

```
FD02::1
C881#
```

Aplique a configuração de OSPF à interface externa ASA:

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

Isto deve fazer com que o ASA envie os pacotes de hello de OSPF da transmissão na sub-rede do IPv6. Inscreva o **comando neighbor OSPF do IPv6 da mostra** a fim verificar a adjacência com o roteador:

```
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
```

Você pode igualmente confirmar o ID de vizinho no ISR, porque usa o endereço configurado o mais alto do IPv4 para o ID à revelia:

```
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#
```

O ASA deve agora ter aprendido a rota do IPv6 do padrão do ISR. A fim confirmar isto, inscreva o **comando show ipv6 route**:

```
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#
```

A configuração básica dos ajustes e dos recursos de roteamento da relação para o IPv6 no ASA está agora completa.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Os procedimentos de Troubleshooting para a Conectividade do IPv6 seguem a maioria da mesma metodologia que é usada a fim pesquisar defeitos a Conectividade do IPv4, com algumas diferenças. De uma perspectiva do Troubleshooting, uma das diferenças as mais importantes entre o IPv4 e o IPv6 é que o Address Resolution Protocol (ARP) já não existe no IPv6. Em vez do uso do ARP a fim resolver endereços IP de Um ou Mais Servidores Cisco ICM NT no segmento de LAN local, o IPv6 usa um protocolo chamado a descoberta vizinha (ND).

Éigualmente importante compreender essa versão 6 do protocolo Protocolo de control de mensajes de Internet (ICMP) das forças de alavanca ND (ICMPv6) para o address resolution do Media Access Control (MAC). Mais informação sobre o IPv6 ND pode ser encontrada no manual de configuração do IPv6 ASA na seção da descoberta vizinha do IPv6 do *livro 1 CLI: Guia de configuração de CLI das operações gerais da série de Cisco ASA, 9.4* ou no RFC 4861.

Atualmente, a maioria de Troubleshooting IPv6-related envolve o ND, o roteamento, ou os problemas da configuração da sub-rede. Isto é provavelmente devido a ao fato de que estas são igualmente as diferenças chave entre o IPv4 e o IPv6. Os trabalhos ND diferentemente do que o ARP, e o endereçamento de rede interna são igualmente bastante diferentes, porque o uso do NAT está desanimado altamente no IPv6 e o endereçamento privado já não leveraged a maneira que era no IPv4 (após o RFC 1918). Uma vez que estas diferenças são compreendidas e/ou os problemas L2/L3 são resolved, o processo de Troubleshooting na camada 4 (L4) e é acima essencialmente o mesmo que aquele usado para o IPv4 porque o TCP/UDP e os protocolos de camada mais elevada funcionam essencialmente o mesmos (apesar da versão IP que é usada).

Pesquise defeitos a Conectividade L2 (o ND)

A maioria de comando básico que é usado a fim pesquisar defeitos a Conectividade L2 com IPv6 é o comando **vizinho do [nameif] do IPv6 da mostra**, que é o equivalente da **mostra arp** para o IPv4.

Estão aqui umas saídas de exemplo:

```
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)#
```

Nesta saída, você pode ver a definição bem sucedida para o endereço do IPv6 de **fd02::1**, que pertence ao dispositivo com um MAC address de **c471.fe93.b516**.

> **Note**: Você pôde observar que o endereço MAC de interface do mesmo roteador aparece duas vezes na saída precedente porque o roteador igualmente tem um endereço local de link auto-atribuído para esta relação. O endereço local de link é um endereço dispositivo-específico que possa somente ser usado para uma comunicação na rede conectada diretamente. O Roteadores não envia pacotes através dos endereços locais de link, mas um pouco é somente para uma comunicação no segmento da rede conectada diretamente. Muitos protocolos de roteamento do IPv6 (tais como OSPFv3) utilizam endereços locais de link a fim compartilhar da informação do protocolo de roteamento no segmento L2.

A fim cancelar o esconderijo ND, inscreva o **comando neighbors claro do IPv6**. Se o ND falha para um host particular, você pode incorporar o comando **nd do IPv6 debugar**, assim como executa capturas de pacote de informação e verifica os Syslog, a fim determinar aquele que ocorre a nível L2. Recorde que o IPv6 ND usa as mensagens ICMPv6 a fim resolver os endereços MAC para endereços do IPv6.

IPv4 ARP contra o IPv6 ND

Considere esta tabela de comparação do ARP para o IPv4 e do ND para o IPv6:

IPv4 ARP	IPv6 ND
ARP REQUEST (quem tem 10.10.10.1?)	Solicitação vizinha
RESPOSTA ARP (10.10.10.1 está em dead.dead.dead)	Anúncio de vizinho

Na encenação seguinte, o ND não resolve o MAC address do host *fd02::1* que é ficado situado na interface externa.

O ND debuga

Está aqui a saída de **debuga o** comando **nd do IPv6**:

```
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
```

Neste resultado do debug, *parece* que os anúncios de vizinho de **fd02::2** estão recebidos nunca. Você pode verificar as capturas de pacote de informação a fim confirmar se este é realmente o caso.

Capturas de pacote de informação ND

> **Note**: Até à data do ASA libere 9.4(1), listas de acesso são exigidos ainda para capturas de pacote de informação do IPv6. Uma requisição de aprimoramento foi arquivada a fim seguir esta com identificação de bug Cisco CSCtn09836.

Configurar o Access Control List (ACL) e capturas de pacote de informação:

```
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
```

Inicie um sibilo a **fd02::1 do** 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]
```

Segundo as indicações das capturas de pacote de informação, os anúncios de vizinho de **fd02::1** são recebidos. Contudo, as propagandas não são processadas por qualquer motivo, segundo as indicações dos resultados do debug. Para um exame mais adicional, você pode ver os Syslog.

Syslog ND

Estão aqui alguns Syslog do exemplo ND:

```
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
```

Dentro destes Syslog, você pode ver que os pacotes do anúncio de vizinho ND do ISR em **fd02::1** são deixado cair devido ao identificador exclusivo prolongado alterado falhado (EUI) 64 (EUI-64 alterado) verificações do formato.

Tip: Refira a seção *alterada da codificação do endereço EUI-64 d*este documento para obter mais informações sobre deste problema específico. Esta lógica do Troubleshooting pode ser aplicada a todos os tipos de razões da gota também, como quando os ACL não permitem o ICMPv6 em uma relação específica ou quando as falhas da verificação do Unicast Reverse Path Forwarding (uRPF) ocorrem, ambo podem causar os problemas de conectividade L2 com IPv6.

Pesquise defeitos a distribuição básica do IPv6

Os procedimentos de Troubleshooting para protocolos de roteamento quando o IPv6 é usado são essencialmente os mesmos como aqueles quando o IPv4 é usado. O uso dos **comandos debug and show**, assim como das capturas de pacote de informação, é útil com tentativas de verificar a razão que um protocolo de roteamento não se comporta como esperado.

O protocolo de roteamento debuga para o IPv6

Esta seção fornece os comandos debug úteis para o IPv6.

A distribuição global do IPv6 debuga

Você pode usar a **distribuição do IPv6 debugar** debuga a fim pesquisar defeitos todas as alterações de tabela de roteamento do IPv6:

```
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 debuga

Você pode usar o **comando ospf do IPv6 debugar** a fim pesquisar defeitos as edições OSPFv3:

```
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
```

Estão aqui umas saídas de exemplo para os todos os debugam que são permitidos depois que o processo OSPFv3 é reiniciado:

```
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)

O EIGRP no ASA não apoia o uso do IPv6. Refira as diretrizes para a seção EIGRP do *livro 1 CLI: Guia de configuração de CLI das operações gerais da série de Cisco ASA, 9.4* para mais informação.

Border Gateway Protocol (BGP)

Este **comando debug** pode ser usado a fim pesquisar defeitos o BGP quando o IPv6 é usado:

```
ASAv# debug ip bgp ipv6 unicast  ?

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

Comandos de exibição úteis para o IPv6

Você pode usar estes **comandos show** a fim pesquisar defeitos edições do IPv6:

- **show ipv6 route**
- **show ipv6 interface brief**
- **mostre o <process ID> OSPF do IPv6**
- **mostre o tráfego do IPv6**
- **mostre o vizinho do IPv6**
- **mostre o ICMP do IPv6**

Projétis luminosos do pacote com IPv6

Você pode usar a funcionalidade incorporado do projétil luminoso do pacote com o IPv6 no ASA da mesma forma como com IPv4. Está aqui um exemplo onde a funcionalidade do pacote-projétil luminoso seja usada a fim simular o host interno em **fd03::2**, que tenta conectar a um servidor de Web em **5555::1** que é ficado situado no Internet com a rota padrão que é instruída da relação **881** através do 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#
```

Observe que o MAC address da saída é o endereço local de link da relação 881. Como mencionado previamente, para muitos protocolos de roteamento dinâmico, o Roteadores use endereços do IPv6 do link local a fim estabelecer adjacências.

A lista completa de IPv6-Related ASA debuga

Seja aqui debuga que pode ser usado a fim pesquisar defeitos edições do IPv6:

```
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
```

Problemas comuns IPv6-Related

Esta seção descreve como pesquisar defeitos as edições as mais comuns IPv6-related.

Sub-redes impropriamente configuradas

Muitos casos de TAC do IPv6 são gerado devido a uma falta geral do conhecimento sobre como o IPv6 funciona, ou devido ao administrador tenta executar o IPv6 com o uso de processos IPv4-specific.

Por exemplo, o TAC viu os casos onde um administrador foi atribuído um bloco \56 de endereços do IPv6 por um provedor de serviço do Internet (ISP). O administrador então atribui um endereço e a sub-rede \56 completa à interface externa ASA e escolhe algum intervalo interno usar-se para os server internos. Contudo, com IPv6, todos os host internos devem igualmente usar endereços do IPv6 do roteável, e o bloco de endereço do IPv6 deve ser dividido em sub-redes menores como necessário. Nesta encenação, você pode criar muitas sub-redes \64 enquanto parte do bloco \56 que esteve atribuído.

Tip: Refira o RFC 4291 para a informação adicional.

Codificação alterada EUI 64

O ASA pode ser configurado a fim exigir endereços alterados do IPv6 EUI-64-encoded. O EUI, conforme o RFC 4291, permite que um host atribua-se um identificador 64-bit original da relação do IPv6 (EUI-64). Esta característica é uma vantagem sobre o IPv4, porque remove a exigência utilizar o DHCP para a atribuição de endereço do IPv6.

Se o ASA é configurado a fim exigir este realce através do **comando nameif do IPv6 enforce-eui64**, a seguir deixará cair provavelmente muitas solicitações e propagandas da descoberta vizinha de outros anfitriões na sub-rede local.

Tip: Para mais informação, refira compreendendo o documento da comunidade do apoio de Cisco do endereço de bit do IPv6 EUI-64.

Os clientes usam endereços provisórios do IPv6 à revelia

Àrevelia, muitos sistemas operacionais do cliente (OS), como versões 7 e 8 de Microsoft Windows, Macintosh OS-X, e sistemas Linux-baseados, uso auto-atribuíram endereços *provisórios do* IPv6 para privacidade prolongada através da configuração automática de endereço apátrida do IPv6 (SLAAC).

O tac Cisco viu alguns casos onde este causou problemas inesperados nos ambientes porque os anfitriões gerenciem o tráfego do endereço provisório e não do endereço estático-atribuído. Em consequência, os ACL e as rotas host-baseadas puderam causar o tráfego ao tornado deixados cair ou distribuídos impropriamente, que faz com que a comunicação do host falhe.

Há dois métodos que são usados a fim endereçar esta situação. O comportamento pode ser desabilitado individualmente nos sistemas de cliente, ou você pode desabilitar este comportamento no Roteadores do ® ASA e de Cisco IOS. No ASA ou no lado do roteador, você deve alterar a bandeira da mensagem do anúncio de roteador (RA) que provoca este comportamento.

Refira as próximas seções a fim desabilitar este comportamento nos sistemas individuais dos clientes.

Microsoft Windows

Termine estas etapas a fim desabilitar este comportamento em sistemas de Microsoft Windows:

1. Em Microsoft Windows, abra um comando prompt elevado (corrida como o administrador).
2. Incorpore este comando a fim desabilitar a característica aleatória da geração do endereço IP de Um ou Mais Servidores Cisco ICM NT, e pressione-o então **entram**:

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

3. Incorpore este comando a fim forçar Microsoft Windows para usar o padrão EUI-64:

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

4. Recarregue a máquina a fim aplicar as mudanças.

Macintosh OS-X

Em um terminal, incorpore este comando a fim desabilitar o IPv6 SLAAC no host até a repartição seguinte:

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

A fim fazer o permanent da configuração, incorpore este comando:

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

Linux

Em um shell terminal, incorpore este comando:

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

Desabilite SLAAC globalmente do ASA

O segundo método que é usado a fim endereçar este comportamento é alterar a mensagem RA que é enviada do ASA aos clientes, que provoca o uso de SLAAC. A fim alterar a mensagem RA, incorpore este comando do *modo de configuração da interface*:

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

Este comando altera a mensagem RA que é enviada pelo ASA de modo que a bandeira do Bit A não seja ajustada, e os clientes não gerenciem um endereço provisório do IPv6.

> **Tip**: Refira o RFC 4941 para a informação adicional.

IPv6 FAQ

Esta seção descreve algumas perguntas mais frequentes com respeito ao uso do IPv6.

Posso eu passar o tráfego para o IPv4 e o IPv6 na mesma relação, ao mesmo tempo?

Sim. Você deve simplesmente permitir o IPv6 na relação e atribuir um IPv4 e um endereço do IPv6 à relação, e segura ambos os tipos de tráfego simultaneamente.

Posso eu aplicar o IPv6 e o IPv4 ACL à mesma relação?

Você pode fazer este nas versões ASA mais cedo do que a versão 9.0(1). Até à data da versão

ASA 9.0(1), todos os ACL no ASA *são unificados*, assim que significa que um ACL apoia uma mistura de entradas do IPv4 e do IPv6 no mesmo ACL.

Nas versões ASA 9.0(1) e mais atrasado, os ACL são fundidos simplesmente junto e o único, ACL unificado é aplicado à relação através do **comando access-group**.

O ASA apoia QoS para o IPv6?

Sim. O ASA apoia o policiamento e as filas de prioridade para o IPv6 da mesma forma que faz com IPv4.

Até à data da versão ASA 9.0(1), todos os ACL no ASA *são unificados*, assim que significa que um ACL apoia uma mistura de entradas do IPv4 e do IPv6 no mesmo ACL. Em consequência, todos os comandos qos que forem decretados em um mapa de classe que combina um ACL tomam a ação no tráfego do IPv4 e do IPv6.

Devo eu usar o NAT com IPv6?

Embora o NAT possa ser configurado para o IPv6 no ASA, o uso do NAT no IPv6 é desanimado altamente e desnecessário, dado a quantidade infinita próxima de disponível, endereços do IPv6 do globalmente-roteável.

Se o NAT é exigido em uma encenação do IPv6, você pode encontrar mais informação sobre como configurar-la na seção das diretrizes do IPv6 NAT do *livro 2 CLI: Guia de configuração de CLI do Series Firewall de Cisco ASA, 9.4*.

> **Note**: Há algumas diretrizes e limitações que devem ser consideradas quando você executa o NAT com IPv6.

Por que eu ver os endereços do IPv6 do link local na saída do *comando show failover*?

No IPv6, o ND usa endereços locais de link a fim executar o address resolution L2. Por este motivo, os endereços do IPv6 para as relações monitoradas na saída do **comando show failover** mostram o endereço local de link e não o endereço global do IPv6 que é configurado na relação. Este é um comportamento esperado.

Advertências conhecidas/requisições de aprimoramento

Estão aqui algumas advertências conhecidas com respeito ao uso do IPv6:

- *A cláusula do "fósforo" da captação do ASA 8.x do* Â do âÂ da identificação de bug Cisco CSCtn09836 *não trava o tráfego do IPv6*
- *ENH do* Â do âÂ da identificação de bug Cisco CSCuq85949*: Apoio do IPv6 ASA para o*

WCCP

- *O roteamento do IPv6 ECMP do ASA do* Â do âÂ da identificação de bug Cisco CSCut78380 *não carrega o tráfego do equilíbrio*

Informações Relacionadas

- Protocolo de internet do do Â do âÂ do RFC 2460, especificação da versão 6 (IPv6)
- Arquitetura de endereçamento do IP versão 6 do do Â do âÂ do RFC 4291
- Descoberta vizinha do do Â do âÂ do RFC 4861 para o IP Versão 6 (IPv6)
- Livro 1 CLI: Guia de configuração de CLI das operações gerais da série de Cisco ASA, 9.4 IPv6s do do Â do âÂ
- AnyConnect SSL sobre IPv4+IPv6 à configuração ASA
- Cisco Systems do do Â do âÂ do Suporte técnico & da documentação