Configurar o ASA para Passar o Tráfego IPv6

Contents

Introduction

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) para transmitir o tráfego do Internet Protocol versão 6 (IPv6) no ASA versão 7.0(1) e posterior.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA versões 7.0(1) e posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

Atualmente, o IPv6 ainda é relativamente novo em termos de penetração no mercado. No entanto, a assistência à configuração do IPv6 e as solicitações de solução de problemas aumentaram constantemente. O objetivo deste documento é atender a essas necessidades e fornecer:

- Uma visão geral do uso do IPv6
- As configurações básicas do IPv6 no ASA
- Informações sobre como solucionar problemas de conectividade IPv6 através do ASA
- Uma lista dos problemas e soluções mais comuns do IPv6, conforme identificado pelo Cisco Technical Assistance Center (TAC)

Note: Como o IPv6 ainda está nos estágios iniciais como um substituto do IPv4

globalmente, este documento será atualizado periodicamente para manter a precisão e a relevância.

Informações sobre o recurso IPv6

Aqui estão algumas informações importantes sobre a funcionalidade IPv6:

- O protocolo IPv6 foi introduzido pela primeira vez no ASA versão 7.0(1).
- O suporte para IPv6 no modo transparente foi apresentado no ASA versão 8.2(1).

Visão geral do IPv6

O protocolo IPv6 foi desenvolvido em meados dos anos 90, principalmente devido ao fato de o espaço de endereço IPv4 público ter se movido rapidamente para a depleção. Embora a Network Address Translation (NAT) tenha ajudado drasticamente o IPv4 e atrasado esse problema, tornou-se inegável que um protocolo substituto seria necessário. O protocolo IPv6 foi oficialmente detalhado no RFC 2460 em dezembro de 1998. Você pode ler mais sobre o protocolo no documento RFC 2460 oficial, localizado no site Internet Engineering Task Force (IETF).

Melhorias de IPv6 sobre IPv4

Esta seção descreve as melhorias incluídas no protocolo IPv6 em relação ao protocolo IPv4 mais antigo.

Recursos de endereçamento expandidos

O protocolo IPv6 aumenta o tamanho do endereço IP de 32 bits para 128 bits para suportar mais níveis de hierarquia de endereçamento, um número muito maior de nós endereçáveis e configuração automática mais simples de endereços. A escalabilidade do roteamento multicast é melhorada pela adição de um campo *de escopo* aos endereços multicast. Além disso, um novo tipo de endereço, chamado de *endereço anycast*, é definido. Isso é usado para enviar um pacote a qualquer nó em um grupo.

Simplificação de formato de cabeçalho

Alguns campos de cabeçalho IPv4 foram descartados ou tornados opcionais para reduzir o custo de processamento de caso comum do manuseio de pacotes e para limitar o custo de largura de banda do cabeçalho IPv6.

Suporte aprimorado para extensões e opções

As mudanças na forma como as opções de cabeçalho IP são codificadas permitem um encaminhamento mais eficiente, limites menos rigorosos no comprimento das opções e maior flexibilidade para a introdução de novas opções no futuro.

Recurso de identificação de fluxo

Um novo recurso é adicionado para permitir a rotulagem de pacotes que pertencem a *fluxos* de tráfego específicos para os quais o remetente solicita tratamento especial, como Qualidade de Serviço (QoS) não padrão ou serviço *em tempo real*.

Recursos de autenticação e privacidade

As extensões usadas para suportar autenticação, integridade de dados e confidencialidade de dados (opcional) são especificadas para IPv6.

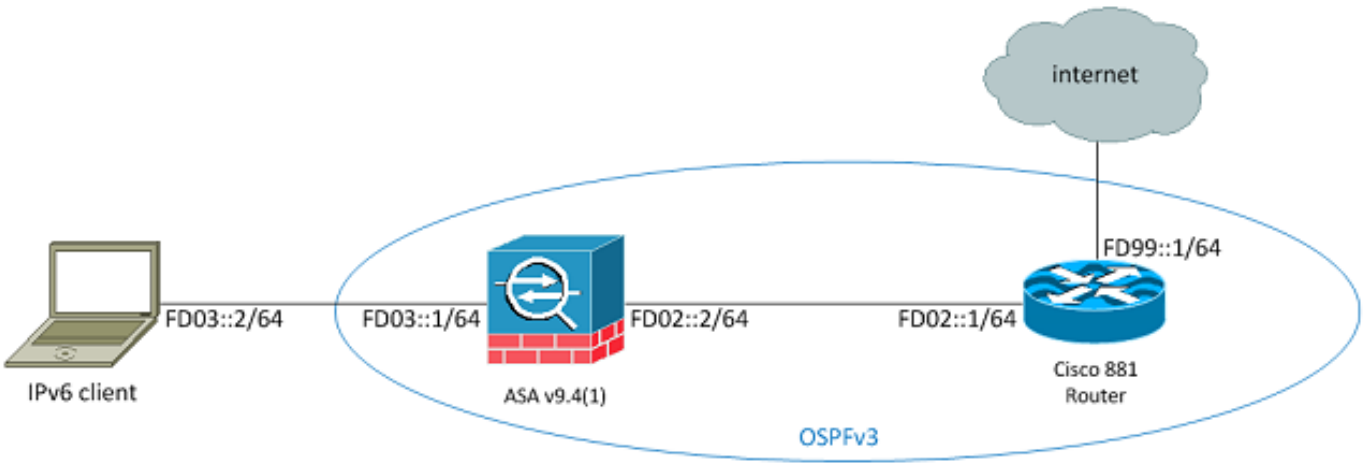
Configurar

Esta seção descreve como configurar o 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 IPv6 para os exemplos usados neste documento:



Configurar interfaces para IPv6

Para passar o tráfego IPv6 por um ASA, você deve primeiro ativar o IPv6 em pelo menos duas interfaces. Este exemplo descreve como habilitar o IPv6 para passar o tráfego da interface interna em **Gi0/0** para a 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
```

Agora você pode configurar os endereços IPv6 em ambas as interfaces.

> **Note**: Neste exemplo, os endereços no espaço ULA (unique local Addresses, endereços unique local) de fc00::/7 são usados, portanto todos os endereços começam com **FD** (como fdxx:xxxx:xxxx...).). Além disso, ao escrever endereços IPv6, pode utilizar dois pontos duplos (**::**) para representar uma linha de zeros de modo que **FD01::1/64** seja igual ao **FD01:0000:0000:0000:0000:00 00:0000:00001**.

```
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
```

Agora você deve ter a conectividade básica da camada 2 (L2)/camada 3 (L3) para um roteador upstream na VLAN externa 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 o roteamento IPv6

Assim como no IPv4, mesmo que haja conectividade IPv6 com os hosts na sub-rede conectada diretamente, você ainda deve ter as rotas para as redes externas para saber como alcançá-las. O primeiro exemplo mostra como configurar uma rota padrão estática para acessar todas as redes IPv6 através da interface externa com um endereço de próximo salto de **fd02::1**.

Configurar o roteamento estático para IPv6

Use estas informações para configurar o roteamento estático para 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, agora há conectividade com um host em uma sub-rede externa:

```
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 for desejado para lidar com o roteamento para IPv6, você também poderá configurá-lo. Isso é descrito na próxima seção.

Configurar o roteamento dinâmico para IPv6 com OSPFv3

Primeiro, você deve examinar a configuração do Open Shortest Path First Version 3 (OSPFv3) no roteador de serviços integrados Cisco 881 Series (ISR) de upstream:

```
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.
```

Esta é a configuração de interface relevante:

```
C881#show run int Vlan302
interface Vlan302
....
```

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

Você pode usar as capturas de pacotes ASA para verificar se os pacotes *Hello* do OSPF são 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 captura de pacotes anterior, você pode ver que os pacotes OSPF (ip-proto-89) chegam do endereço link local IPv6, que corresponde à interface correta no ISR:

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

Agora você pode criar um processo OSPFv3 no ASA para estabelecer uma adjacência com o ISR:

```
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
```

Aplique a configuração do OSPF à interface externa do ASA:

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

Isso deve fazer com que o ASA envie os pacotes Hello do OSPF de broadcast na sub-rede IPv6. Insira o comando **show ipv6 ospf neighbor** para 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 também pode confirmar o ID do vizinho no ISR, pois ele usa o maior endereço IPv4 configurado para o ID por padrão:

```
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 ter aprendido a rota IPv6 padrão do ISR. Para confirmar isso, insira 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 das configurações da interface e dos recursos de roteamento para IPv6 no ASA está agora concluída.

Verificar

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

Troubleshoot

Os procedimentos de identificação e solução de problemas de conectividade IPv6 seguem a maior parte da mesma metodologia usada para solucionar problemas de conectividade IPv4, com algumas diferenças. Do ponto de vista da solução de problemas, uma das diferenças mais importantes entre IPv4 e IPv6 é que o Address Resolution Protocol (ARP) não existe mais no IPv6. Em vez do uso do ARP para resolver endereços IP no segmento de LAN local, o IPv6 usa um protocolo chamado Neighbor Discovery (ND).

Também é importante entender que o ND aproveita o Internet Control Message Protocol Version 6 (ICMPv6) para a resolução de endereços de Media Access Control (MAC). Mais informações sobre a ND do IPv6 podem ser encontradas no guia de configuração do ASA IPv6 na seção Descoberta de vizinhos do IPv6 do *CLI Book 1: Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9.4* ou no RFC 4861.

Atualmente, a maioria da solução de problemas relacionados ao IPv6 envolve problemas de configuração de ND, roteamento ou sub-rede. Isso provavelmente se deve ao fato de que essas também são as principais diferenças entre IPv4 e IPv6. O ND funciona de forma diferente do ARP, e o endereçamento de rede interna também é bem diferente, já que o uso do NAT é altamente desencorajado no IPv6 e o endereçamento privado não é mais aproveitado da forma como era no IPv4 (após RFC 1918). Depois que essas diferenças são compreendidas e/ou os problemas de L2/L3 são resolvidos, o processo de solução de problemas na Camada 4 (L4) e superiores é essencialmente o mesmo usado para IPv4 porque o TCP/UDP e os protocolos de camada superior funcionam essencialmente da mesma forma (independentemente da versão IP que é usada).

Identificar e Solucionar Problemas de Conectividade L2 (ND)

O comando mais básico usado para solucionar problemas de conectividade L2 com IPv6 é o **comando show ipv6 neighbor [nameif]**, que é o equivalente ao **show arp** para IPv4.

Aqui está um exemplo de saída:

```
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 resolução bem-sucedida para o endereço IPv6 de **fd02::1**, que pertence ao dispositivo com um endereço MAC de **c471.fe93.b516**.

> **Note**: Você pode observar que o mesmo endereço MAC da interface do roteador aparece duas vezes na saída anterior porque o roteador também tem um endereço link local atribuído automaticamente para essa interface. O endereço de link local é um endereço específico do dispositivo que só pode ser usado para comunicação na rede diretamente conectada. Os roteadores não encaminham pacotes através de endereços de link local, mas são apenas para comunicação no segmento de rede conectado diretamente. Muitos protocolos de roteamento IPv6 (como OSPFv3) utilizam endereços de link local para compartilhar informações do protocolo de roteamento no segmento L2.

Para limpar o cache ND, insira o comando **clear ipv6 neighbors**. Se o ND falhar para um host específico, você pode inserir o comando **debug ipv6 nd**, bem como executar capturas de pacotes e verificar os syslogs, para determinar o que ocorre no nível L2. Lembre-se de que o ND IPv6 usa mensagens ICMPv6 para resolver os endereços MAC para endereços IPv6.

IPv4 ARP versus IPv6 ND

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

ARP IPv4	IPv6 ND
SOLICITAÇÃO ARP (quem tem 10.10.10.1?)	Solicitação de vizinho
RESPOSTA ARP (10.10.10.1 está morto.morto.morto)	Anúncio de vizinho

No próximo cenário, o ND não consegue resolver o endereço MAC do host *fd02::1* localizado na interface externa.

Depurações de ND

Aqui está a saída do comando **debug ipv6 nd**:

```
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
```

Nesta saída de depuração, *parece* que os anúncios de vizinhos de **fd02::2** nunca são recebidos. Você pode verificar as capturas de pacote para confirmar se esse é realmente o caso.

Capturas de pacote ND

> **Note**: A partir do ASA versão 9.4(1), as listas de acesso ainda são necessárias para capturas de pacotes IPv6. Uma solicitação de aprimoramento foi inserida para rastrear isso com o bug da Cisco ID CSCtn09836.

Configure a ACL (Access Control List, lista de controle de acesso) e as capturas de pacotes:

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

Inicie um ping para **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]
```

Como mostrado nas capturas de pacote, os anúncios de vizinhos de **fd02::1** são recebidos. No entanto, os anúncios não são processados por algum motivo, como mostrado nas saídas de depuração. Para uma análise mais detalhada, você pode ver os syslogs.

Syslogs ND

Aqui estão alguns exemplos de syslogs 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
```

Nesses syslogs, você pode ver que os pacotes de anúncio de vizinhos ND do ISR em **fd02::1** são descartados devido a falhas nas verificações de formato EUI (Modified Extended Unique Identifier) 64 (Modificado EUI-64).

> **Tip**: Consulte a seção *Codificação de Endereço EUI-64 Modificada* deste documento para obter mais informações sobre este problema específico. Essa lógica de solução de problemas também pode ser aplicada a todos os tipos de motivos de queda, como quando as ACLs não permitem o ICMPv6 em uma interface específica ou quando ocorrem falhas de verificação do Unicast Reverse Path Forwarding (uRPF), que podem causar problemas de conectividade de L2 com IPv6.

Solucionar problemas de roteamento IPv6 básico

Os procedimentos de identificação e solução de problemas para protocolos de roteamento quando o IPv6 é usado são essencialmente os mesmos quando o IPv4 é usado. O uso de comandos **debug** e **show**, bem como capturas de pacotes, são úteis para tentar determinar o motivo pelo qual um protocolo de roteamento não se comporta como esperado.

Depurações do protocolo de roteamento para IPv6

Esta seção fornece os comandos debug úteis para IPv6.

Depurações globais de roteamento IPv6

Você pode usar a depuração **debug ipv6 routing** para solucionar problemas de todas as alterações na tabela de roteamento 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
```

Depurações de OSPFv3

Você pode usar o comando **debug ipv6 ospf** para solucionar problemas do 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
```

Aqui está um exemplo de saída para todas as depurações ativadas após o processo OSPFv3 ser 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
```

Protocolo de Roteamento IGRP Melhorado (EIGRP)

O EIGRP no ASA não suporta o uso de IPv6. Consulte a seção Diretrizes para o EIGRP do *CLI Book 1: Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9.4* para obter mais informações.

BGP (Border Gateway Protocol)

Este comando **debug** pode ser usado para solucionar problemas do 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 show úteis para IPv6

Você pode usar estes comandos **show** para solucionar problemas de IPv6:

- **show ipv6 route**
- **show ipv6 interface brief**
- **show ipv6 ospf <process ID>**
- **show ipv6 traffic**
- **show ipv6 neighbor**
- **show ipv6 icmp**

Packet Tracers com IPv6

Você pode usar a funcionalidade do packet tracer integrada com IPv6 no ASA da mesma forma que com IPv4. Aqui está um exemplo onde a funcionalidade packet-tracer é usada para simular o host interno em **fd03::2**, que tenta se conectar a um servidor web em **5555::1** localizado na Internet com a rota padrão aprendida da interface **881** 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#
```

Observe que o endereço MAC de saída é o endereço de link local da interface 881. Como mencionado anteriormente, para muitos protocolos de roteamento dinâmico, os roteadores usam endereços IPv6 de link local para estabelecer adjacências.

Lista completa de depurações ASA relacionadas ao IPv6

Aqui estão as depurações que podem ser usadas para solucionar problemas de 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 relacionados ao IPv6

Esta seção descreve como solucionar os problemas mais comuns relacionados ao IPv6.

Sub-redes configuradas incorretamente

Muitos casos de TAC IPv6 são gerados devido a uma falta geral de conhecimento sobre como o IPv6 funciona ou devido a tentativas do administrador de implementar o IPv6 com o uso de processos específicos do IPv4.

Por exemplo, o TAC observou casos em que um administrador recebeu um bloco \56 de endereços IPv6 por um ISP (Provedor de serviços de Internet). Em seguida, o administrador atribui um endereço e a sub-rede completa \56 à interface externa do ASA e escolhe algum intervalo interno para usar para os servidores internos. No entanto, com o IPv6, todos os hosts internos também devem usar endereços IPv6 roteáveis, e o bloco de endereços IPv6 deve ser dividido em sub-redes menores conforme necessário. Neste cenário, você pode criar muitas \64 sub-redes como parte do bloco \56 que foi alocado.

> **Tip**: Consulte o RFC 4291 para obter informações adicionais.

Codificação EUI 64 modificada

O ASA pode ser configurado para exigir endereços IPv6 codificados EUI-64 modificados. O EUI, de acordo com o RFC 4291, permite que um host atribua a si mesmo um identificador de interface IPv6 (EUI-64) de 64 bits exclusivo. Esse recurso é uma vantagem sobre o IPv4, pois remove a necessidade de utilizar o DHCP para a atribuição de endereços IPv6.

Se o ASA estiver configurado para exigir essa melhoria por meio do comando **ipv6 apply-eui64 nameif**, ele provavelmente descartará muitas solicitações de descoberta de vizinhos e anúncios de outros hosts na sub-rede local.

> **Tip**: Para obter mais informações, consulte o documento Understanding IPv6 EUI-64 Bit Address Cisco Support Community .

Os clientes usam endereços IPv6 temporários por padrão

Por padrão, muitos sistemas operacionais (OSs) clientes, como Microsoft Windows versões 7 e 8, Macintosh OS-X e sistemas baseados em Linux, usam endereços *temporários* IPv6 atribuídos automaticamente para uma privacidade estendida via Configuração automática de endereço IPv6

stateless (SLAAC).

O Cisco TAC observou alguns casos em que isso causou problemas inesperados em ambientes porque os hosts geram tráfego do endereço temporário e não do endereço atribuído estaticamente. Como resultado, as ACLs e as rotas baseadas em host podem fazer com que o tráfego seja descartado ou roteado incorretamente, o que faz com que a comunicação do host falhe.

Há dois métodos que são usados para lidar com essa situação. O comportamento pode ser desabilitado individualmente nos sistemas cliente ou você pode desabilitar esse comportamento nos roteadores ASA e Cisco IOS®. No lado do ASA ou do roteador, você deve modificar o sinalizador de mensagem do anúncio do roteador (RA) que dispara esse comportamento.

Consulte as próximas seções para desabilitar esse comportamento nos sistemas de clientes individuais.

Microsoft Windows

Conclua estes passos para desabilitar esse comportamento em sistemas Microsoft Windows:

1. No Microsoft Windows, abra um prompt de comando elevado (executado como administrador).

2. Digite este comando para desabilitar o recurso aleatório de geração de endereço IP e pressione **Enter**:

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

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

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

4. Reinicie a máquina para aplicar as alterações.

Macintosh OS-X

Em um terminal, insira este comando para desabilitar o IPv6 SLAAC no host até a próxima reinicialização:

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

Para tornar a configuração permanente, insira este comando:

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

Linux

Em um shell de terminal, digite este comando:

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

Desabilite globalmente o SLAAC do ASA

O segundo método usado para endereçar esse comportamento é modificar a mensagem do RA enviada do ASA para os clientes, o que aciona o uso do SLAAC. Para modificar a mensagem do

RA, insira este comando no modo *Interface Configuration*:

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

Esse comando modifica a mensagem do RA enviada pelo ASA para que o flag de bit A não esteja definido e os clientes não gerem um endereço IPv6 temporário.

> **Tip**: Consulte o RFC 4941 para obter informações adicionais.

Perguntas frequentes sobre IPv6

Esta seção descreve algumas perguntas frequentes relacionadas ao uso do IPv6.

Posso transmitir tráfego para IPv4 e IPv6 na mesma interface, ao mesmo tempo?

Yes. Você deve simplesmente ativar o IPv6 na interface e atribuir um endereço IPv4 e IPv6 à interface, e ele lida com ambos os tipos de tráfego simultaneamente.

Posso aplicar ACLs IPv6 e IPv4 à mesma interface?

Você pode fazer isso em versões do ASA anteriores à versão 9.0(1). A partir do ASA versão 9.0(1), todas as ACLs no ASA são *unificadas*, o que significa que uma ACL suporta uma combinação de entradas IPv4 e IPv6 na mesma ACL.

Nas versões 9.0(1) e posteriores do ASA, as ACLs são simplesmente mescladas e a ACL única e unificada é aplicada à interface através do comando **access-group**.

O ASA é compatível com QoS para IPv6?

Yes. O ASA suporta política e enfileiramento de prioridade para IPv6 da mesma forma que suporta com IPv4.

A partir do ASA versão 9.0(1), todas as ACLs no ASA são *unificadas*, o que significa que uma ACL suporta uma combinação de entradas IPv4 e IPv6 na mesma ACL. Como resultado, todos os comandos de QoS que são ativados em um mapa de classe que corresponde a uma ACL tomam medidas no tráfego IPv4 e IPv6.

Devo usar NAT com IPv6?

Embora o NAT possa ser configurado para IPv6 no ASA, o uso do NAT no IPv6 é altamente desencorajado e desnecessário, considerando a quantidade quase infinita de endereços IPv6 disponíveis e roteáveis globalmente.

Se o NAT for necessário em um cenário IPv6, você poderá encontrar mais informações sobre

como configurá-lo na seção Diretrizes de NAT IPv6 do *CLI Book 2: Guia de configuração da CLI do firewall Cisco ASA Series, 9.4*.

> **Note**: Há algumas diretrizes e limitações que devem ser consideradas ao implementar o NAT com IPv6.

Por que vejo os endereços IPv6 de link local na saída do comando *show failover*?

No IPv6, o ND usa endereços de link local para executar a resolução de endereços L2. Por esse motivo, os endereços IPv6 das interfaces monitoradas na saída do comando **show failover** mostram o endereço de link local e não o endereço IPv6 global configurado na interface. Este é um comportamento esperado.

Avisos conhecidos/solicitações de aprimoramento

Aqui estão algumas advertências conhecidas sobre o uso do IPv6:

- ID de bug da Cisco CSCtn09836 âÂ Â *cláusula de "correspondência" de captura ASA 8.x não captura o tráfego IPv6*
- ID de bug da Cisco CSCuq85949 â Â *ENH: Suporte ASA IPv6 para WCCP*
- ID de bug da Cisco CSCut78380 Â Â *O roteamento ECMP do ASA IPv6 não equilibra a carga do tráfego*

Informações Relacionadas

- RFC 2460 âÂ Â Protocolo Internet, Versão 6 (IPv6) Especificação
- RFC 4291 âÂ Â Arquitetura de endereçamento IP versão 6
- RFC 4861 âÂ Â Neighbor Discovery para IP versão 6 (IPv6)
- Livro 1 da CLI: Guia de configuração da CLI de operações gerais do Cisco ASA Series, 9,4 Â IPv6
- Configuração do AnyConnect SSL sobre IPv4+IPv6 para ASA
- Suporte técnico e documentação Â Cisco Systems