Configurez l'ASA pour passer le trafic d'IPv6

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
Les informations de caractéristique d'IPv6
Aperçu d'IPv6
Améliorations d'IPv6 au-dessus d'ipv4
Capacités d'adressage développées
Simplification de format d'en-tête
Soutien amélioré des extensions et des options
Capacité de écriture de labels d'écoulement
Capacités d'authentification et d'intimité
Configurer
Diagramme du réseau
Configurez les interfaces pour l'IPv6
Configurez l'acheminement d'IPv6
Configurez le routage statique pour l'IPv6
Configurez le routage dynamique pour l'IPv6 avec OSPFv3
Vérifier
Dépanner
Dépannez la Connectivité L2 (le ND)
ARP d'ipv4 contre le ND d'IPv6
Debugs ND
Captures de paquet ND
Syslog ND
Dépannez l'acheminement de base d'IPv6
Debugs de protocole de routage pour l'IPv6
Commandes show utiles pour l'IPv6
Traceurs de paquet avec l'IPv6
Liste complète de debugs IPv6-Related ASA
Problèmes communs IPv6-Related
Sous-réseaux incorrectement configurés
Codage modifié EUI 64
Les clients utilisent des adresses provisoires d'IPv6 par défaut
Foires aux questions d'IPv6
Est-ce que je peux passer le trafic pour l'ipv4 et l'IPv6 sur la même interface, en même temps ?

Est-ce que je peux m'appliquer l'IPv6 et l'ipv4 ACLs à la même interface ?
L'ASA prend en charge-elle QoS pour l'IPv6 ?
Est-ce que je devrais utiliser NAT avec l'IPv6 ?
Pourquoi est-ce que je vois les adresses d'IPv6 de lien-gens du pays dans la sortie de commande de *Basculement d'exposition* ?
Mises en garde/demandes d'amélioration connues
Informations connexes

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable Cisco (ASA) afin de passer le trafic de la version 6 d'Internet Protocol (IPv6) dans des versions 7.0(1) et ultérieures ASA.

Conditions préalables

Exigences

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions 7.0(1) et ultérieures de Cisco ASA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Actuellement, l'IPv6 est toujours relativement nouveau en termes de traversée du marché. Cependant, l'assistance à la configuration d'IPv6 et les demandes de dépannage ont solidement augmenté. Le but de ce document est de satisfaire ces besoins et de fournir :

- Une présentation générale d'utilisation d'IPv6
- Les configurations de base d'IPv6 sur l'ASA
- Informations sur la façon dépanner la Connectivité d'IPv6 par l'ASA
- Une liste des problèmes et des solutions d'IPv6 les plus communs, comme identifiée par le

centre d'assistance technique Cisco (TAC)

Note: Étant donné que l'IPv6 est toujours aux parties comme remplacement d'ipv4 globalement, ce document sera périodiquement mis à jour afin de mettre à jour la précision et la pertinence.

Les informations de caractéristique d'IPv6

Voici quelques informations importantes au sujet de la fonctionnalité d'IPv6 :

- Le protocole d'IPv6 a été introduit la première fois dans la version 7.0(1) ASA.
- Le soutien de l'IPv6 en mode transparent a été introduit dans la version 8.2(1) ASA.

Aperçu d'IPv6

Le protocole d'IPv6 a été développé pendant les seconde moitié années 1990, principalement étant donné que l'espace public d'ipv4 addres a déplacé rapidement vers l'épuisement. Bien que le Traduction d'adresses de réseau (NAT) ait excessivement aidé l'ipv4 et ait retardé ce problème, il est devenu indéniable qu'un protocole de remplacement serait par la suite nécessaire. Le protocole d'IPv6 a été officiellement détaillé dans RFC 2460 en décembre 1998. Vous pouvez avoir connaissance plus du protocole dans le document RFC 2460 de fonctionnaire, localisé sur le site Web de l'Internet Engineering Task Force (IETF).

Améliorations d'IPv6 au-dessus d'ipv4

Cette section décrit les améliorations qui sont incluses avec le protocole d'IPv6 contre le protocole plus ancien d'ipv4.

Capacités d'adressage développées

Le protocole d'IPv6 augmente la taille d'adresse IP de 32 bits à 128 bits afin de prendre en charge plus de niveaux d'adresser la hiérarchie, un nombre beaucoup plus grand de Noeuds adressables, et la configuration automatique plus simple des adresses. L'évolutivité du routage de Multidiffusion est améliorée par l'ajout d'un champ de *portée aux* adresses de multidiffusion. Supplémentaire, un nouveau type d'adresse, a appelé une *adresse de diffusion anycast*, est défini. Ceci est utilisé afin d'envoyer un paquet à n'importe quel un noeud dans un groupe.

Simplification de format d'en-tête

Quelques champs d'en-tête d'ipv4 ont été abandonnés ou rendus facultatifs afin de réduire le coût de traitement de commun-dossier de traitement des paquets et afin de limiter le coût de bande passante de l'en-tête d'IPv6.

Soutien amélioré des extensions et des options

Change de la manière que les options d'en-tête IP sont encodé tient compte d'un expédition plus efficace, des limites moins rigoureuses sur la longueur d'options, et d'une meilleure flexibilité pour l'introduction de nouvelles options à l'avenir.

Capacité de écriture de labels d'écoulement

Une nouvelle capacité est ajoutée afin d'activer l'écriture de labels des paquets qui appartiennent à la *circulation* particulière pour laquelle l'expéditeur demande la manipulation spéciale, telle que le Qualité de service (QoS) de non-par défaut ou le service *en temps réel*.

Capacités d'authentification et d'intimité

Des extensions qui sont utilisées afin de prendre en charge l'authentification, l'intégrité des données, et la confidentialité des données (facultative) sont spécifiées pour l'IPv6.

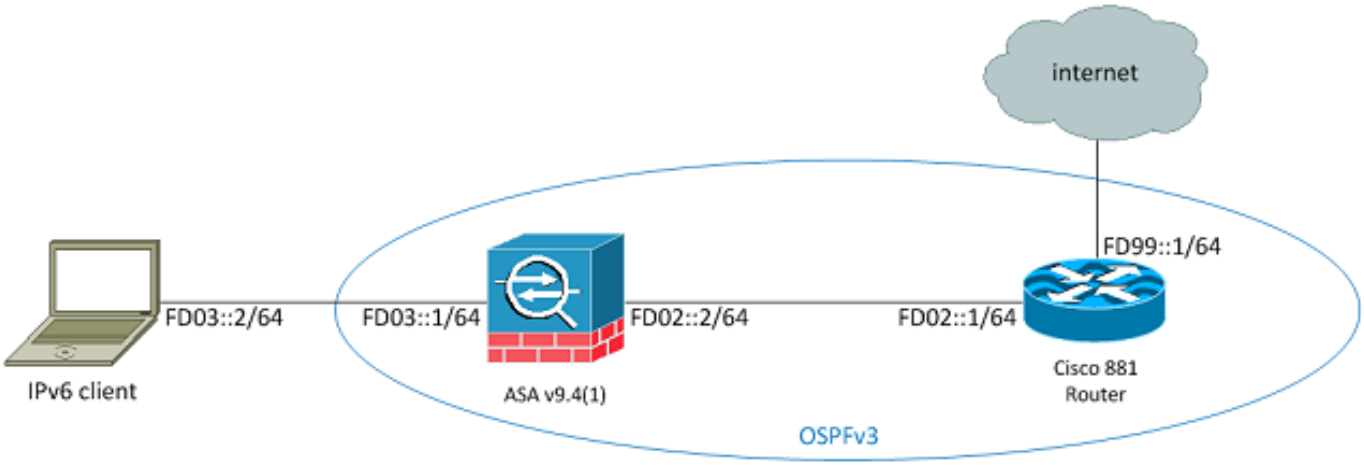
Configurer

Cette section décrit comment configurer Cisco ASA pour l'usage de l'IPv6.

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

C'est la topologie d'IPv6 pour les exemples qui sont utilisés dans tout ce document :



Configurez les interfaces pour l'IPv6

Afin de passer le trafic d'IPv6 par une ASA, vous devez d'abord activer l'IPv6 sur au moins deux interfaces. Cet exemple décrit comment permettre à l'IPv6 afin de passer le trafic de l'interface interne sur **Gi0/0 à l'**interface extérieure sur **Gi0/1** :

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

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

Vous pouvez maintenant configurer les adresses d'IPv6 sur chacun des deux interfaces.

> **Note**: Dans cet exemple, les adresses dans le seul espace des adresses locales (ULA) de fc00::/7 sont utilisées, ainsi toutes les adresses commencent par **FD** (comme, fdxx : xxxx : xxxx….. En outre, quand vous écrivez des adresses d'IPv6, vous pouvez employer de doubles deux points (**: :**) afin de représenter une ligne des zéros de sorte que **FD01::1/64** soit identique 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
```

Vous devriez maintenant avoir la couche de base 2 Connectivité (L2)/Layer 3 (L3) à un routeur en amont sur le VLAN extérieur à 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
```

Configurez l'acheminement d'IPv6

Tout comme avec l'ipv4, quoiqu'il y ait de Connectivité d'IPv6 avec les hôtes sur le sous-réseau direct-connecté, vous devez encore avoir les artères aux réseaux externes afin de savoir les atteindre. Le premier exemple affiche comment configurer une route statique par défaut afin d'atteindre tous les réseaux d'IPv6 par l'intermédiaire de l'interface extérieure avec une adresse du prochain saut de **fd02::1**.

Configurez le routage statique pour l'IPv6

Employez ces informations afin de configurer le routage statique pour l'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)#
```

Comme affiché, il y a maintenant de Connectivité à un hôte sur un sous-réseau externe :

```
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**: Si un protocole de routage dynamique est désiré afin de manipuler le routage pour l'IPv6, alors vous pouvez configurer cela aussi bien. Ceci est décrit dans la section suivante.

Configurez le routage dynamique pour l'IPv6 avec OSPFv3

D'abord, vous devriez examiner la configuration ouverte de la version 3 de Shortest Path First (OSPFv3) sur l'Integrated Services Router ascendant de gamme Cisco 881 (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.
```

Voici la configuration d'interface appropriée :

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

Vous pouvez utiliser des captures de paquet ASA afin de vérifier que les paquets HELLO OSPF sont vus de l'ISR sur l'interface extérieure :

```
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)#
```

Dans la capture précédente de paquet, vous pouvez voir que les paquets OSPF (**ip-proto-89**) arrivent de l'adresse locale à la liaison d'IPv6, qui correspond à l'interface appropriée sur l'ISR :

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

Vous pouvez maintenant créer un processus OSPFv3 sur l'ASA afin d'établir une contiguïté avec l'ISR :

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

Appliquez-vous la configuration OSPF à l'ASA en dehors de l'interface :

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

Ceci devrait faire envoyer l'ASA les paquets HELLO OSPF d'émission sur le sous-réseau d'IPv6. Sélectionnez la commande de **show ipv6 ospf neighbor** afin de vérifier la contiguïté avec le routeur :

```
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
```

Vous pouvez également confirmer l'ID de voisin sur l'ISR, car il utilise l'ipv4 addres configuré le plus élevé pour l'ID par défaut :

```
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#
```

L'ASA devrait maintenant avoir appris l'ipv6 route par défaut de l'ISR. Afin de confirmer ceci, sélectionnez la commande de **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#
```

La configuration de base des paramètres d'interface et des caractéristiques de routage pour l'IPv6 sur l'ASA est maintenant complète.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépanner

Les procédures de dépannage pour la Connectivité d'IPv6 suit la majeure partie de la même méthodologie qui est utilisée afin de dépanner la Connectivité d'ipv4, avec quelques différences. D'un point de vue de dépannage, une des différences les plus importantes entre l'ipv4 et l'IPv6 est que le Protocole ARP (Address Resolution Protocol) n'existe plus dans l'IPv6. Au lieu de l'utilisation de l'ARP afin de résoudre des adresses IP sur le segment de réseau local, l'IPv6 utilise un protocole appelé Neighbor Discovery (ND).

Il est également important de comprendre que le ND accroît la version 6 (ICMPv6) d'Internet Control Message Protocol pour l'address resolution de Contrôle d'accès au support (MAC). Plus d'informations sur le ND d'IPv6 peuvent être trouvées dans le guide de configuration d'IPv6 ASA dans la section de détection d'ipv6 neighbor de l'*ouvrage 1 CLI : Guide de configuration général CLI d'exécutions de gamme de Cisco ASA, 9.4* ou dans RFC 4861.

Actuellement, la plupart de dépannage IPv6-related implique le ND, le routage, ou les problèmes de configuration de sous-réseau. C'est vraisemblablement dû au fait que ce sont également les différences principales entre l'ipv4 et l'IPv6. Les travaux ND différemment que l'ARP, et l'adressage de réseau interne est également très différent, car l'utilisation de NAT est fortement découragée dans l'IPv6 et l'adressage privé n'est plus accru la manière dont il était dans l'ipv4 (après RFC 1918). Une fois que ces différences sont comprises et/ou les problèmes L2/L3 sont résolus, le processus de dépannage à la couche 4 (L4) et est en haut essentiellement identique que cela utilisé pour l'ipv4 parce que les TCP/UDP et les protocoles de couche plus élevée fonctionnent essentiellement le même (indépendamment de la version d'IP qui est utilisé).

Dépannez la Connectivité L2 (le ND)

La commande la plus fondamentale qui est utilisée afin de dépanner la Connectivité L2 avec l'IPv6

est la commande de **show ipv6 neighbor [nameif]**, qui est l'équivalent du **show arp** pour l'ipv4.

Voici un exemple de sortie :

```
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)#
```

Dans cette sortie, vous pouvez voir la résolution réussie pour l'ipv6 addres de **fd02::1**, qui appartient au périphérique avec une adresse MAC de **c471.fe93.b516**.

> **Note**: Vous pourriez noter que la même adresse MAC d'interface de routeur apparaît deux fois dans la sortie précédente parce que le routeur a également une adresse locale à la liaison avec auto-assignation pour cette interface. L'adresse locale à la liaison est une adresse de périphérique-particularité qui peut seulement être utilisée pour la transmission sur le réseau directement connecté. Les Routeurs n'expédient pas des paquets par l'intermédiaire des adresses locales à la liaison, mais plutôt ils sont seulement pour la transmission sur le segment de réseau directement connecté. Beaucoup de protocoles de routage d'IPv6 (tels qu'OSPFv3) utilisent des adresses locales à la liaison afin de partager les informations de protocole de routage sur le segment L2.

Afin d'effacer le cache ND, sélectionnez la commande de **clear ipv6 neighbors**. Si le ND échoue pour un hôte spécifique, vous pouvez sélectionner la commande de **debug ipv6 nd**, aussi bien qu'effectuez des captures de paquet et vérifiez les Syslog, afin de déterminer cela qui se produit au niveau L2. Souvenez-vous que le ND d'IPv6 emploie des messages d'ICMPv6 afin de résoudre les adresses MAC pour des adresses d'IPv6.

ARP d'ipv4 contre le ND d'IPv6

Considérez cette table de comparaison d'ARP pour l'ipv4 et de ND pour l'IPv6 :

ARP d'ipv4	ND d'IPv6
DEMANDE d'ARP (qui a 10.10.10.1 ?)	Sollicitation voisine
RÉPONSE d'ARP (10.10.10.1 est à dead.dead.dead)	Publicité voisine

Dans le prochain scénario, le ND ne résout pas l'adresse MAC de l'hôte *fd02::1* qui se trouve sur l'interface extérieure.

Debugs ND

Voici la sortie de la commande de **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
```

Dans cette sortie de débogage, il *s'avère* que les annonces voisines de **fd02::2** ne sont jamais reçues. Vous pouvez vérifier les captures de paquet afin de confirmer si c'est réellement le cas.

Captures de paquet ND

> **Note**: En date de l'ASA libérez 9.4(1), des Listes d'accès sont toujours exigés pour des captures de paquet d'IPv6. Une demande d'amélioration a été classée afin de dépister ceci avec l'ID de bogue Cisco CSCtn09836.

Configurez les captures de liste de contrôle d'accès (ACL) et de paquet :

```
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
```

Initiez un ping à **fd02::1 de l'**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]
```

Suivant les indications des captures de paquet, les annonces voisines de **fd02::1** sont reçues. Cependant, les annonces ne sont pas traitées pour quelque raison, suivant les indications des sorties de débogage. Pour davantage d'examen, vous pouvez visualiser les Syslog.

Syslog ND

Voici quelques Syslog ND d'exemple :

```
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
```

Dans ces Syslog, vous pouvez voir que les paquets voisins de publicité ND de l'ISR à **fd02::1** sont

dus lâché à l'identifiant unique étendu modifié défectueux (EUI) 64 (EUI-64 modifié) contrôles du format.

> **Conseil** : Référez-vous à la section *modifiée de codage de l'adresse EUI-64 de* ce document pour plus d'informations sur ce problème spécifique. Cette logique de dépannage peut être aussi bien appliquée à toutes sortes de raisons de baisse, comme quand l'ACLs ne permettent pas l'ICMPv6 sur une interface spécifique ou quand les pannes de contrôle de Fonction Unicast Reverse Path Forwarding (uRPF) se produisent, qui peuvent entraîner les problèmes de connectivité L2 avec l'IPv6.

Dépannez l'acheminement de base d'IPv6

Les procédures de dépannage pour des protocoles de routage quand l'IPv6 est utilisé sont essentiellement identiques comme ceux quand l'ipv4 est utilisé. L'utilisation de **mettent au point** et des **commandes show**, aussi bien que le paquet le capture, est utile avec des tentatives de s'assurer la raison pour laquelle un protocole de routage ne se comporte pas comme prévu.

Debugs de protocole de routage pour l'IPv6

Cette section fournit les commandes de débogage utiles pour l'IPv6.

IPv6 global conduisant des debugs

Vous pouvez utiliser le **debug ipv6 routing** mettez au point afin de dépanner toutes les modifications de table de routage d'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
```

Debugs OSPFv3

Vous pouvez employer la commande de **debug ipv6 ospf** afin de dépanner les questions 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
```

Voici un exemple de sortie pour les tous les met au point qui sont activés après que le processus OSPFv3 soit redémarré :

```
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)

L'EIGRP sur l'ASA ne prend en charge pas l'utilisation de l'IPv6. Référez-vous aux instructions pour la section EIGRP de l'*ouvrage 1 CLI : Guide de configuration général CLI d'exécutions de gamme de Cisco ASA, 9.4* pour en savoir plus.

Protocole BGP (Border Gateway Protocol)

Cette commande de **débogage** peut être utilisée afin de dépanner le BGP quand l'IPv6 est utilisé :

```
ASAv# debug ip bgp ipv6 unicast  ?

X:X:X:X::X IPv6 BGP neighbor address
```

```
keepalives BGP keepalives
updates BGP updates
<cr>
```

Commandes show utiles pour l'IPv6

Vous pouvez employer ces **commandes show** afin de dépanner des questions d'IPv6 :

- **show ipv6 route**
- **brief de show ipv6 interface**
- **<process ID> de show ipv6 ospf**
- **show ipv6 traffic**
- **show ipv6 neighbor**
- **affichez l'ICMP d'IPv6**

Traceurs de paquet avec l'IPv6

Vous pouvez utiliser la fonctionnalité intégrée de traceur de paquet avec l'IPv6 sur l'ASA de la même manière qu'avec l'ipv4. Voici un exemple où la fonctionnalité de traceur de paquets est utilisée afin de simuler l'hôte interne à **fd03::2**, qui tente de connecter à un web server à **5555::1** qui se trouve sur l'Internet avec le default route qui est appris de l'interface **881** par l'intermédiaire de l'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#
```

Notez que l'adresse MAC de sortie est l'adresse locale à la liaison de l'interface 881. Comme mentionné précédemment, pour beaucoup de protocoles de routage dynamique, l'IPv6 de lien-gens du pays d'utilisation de Routeurs adresse afin d'établir des contiguïtés.

Liste complète de debugs IPv6-Related ASA

Voici met au point qui peut être utilisé afin de dépanner des questions d'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
```

Problèmes communs IPv6-Related

Cette section décrit comment dépanner les questions IPv6-related les plus communes.

Sous-réseaux incorrectement configurés

Beaucoup de cas de l'IPv6 TAC sont dus généré à un manque général de la connaissance au sujet de la façon dont l'IPv6 fonctionne, ou d'en raison des tentatives d'administrateur d'implémenter l'IPv6 avec l'utilisation des processus IPv4-specific.

Par exemple, le TAC a vu des cas où un administrateur a été assigné un bloc \56 d'adresses

d'IPv6 par un fournisseur de services Internet (ISP). L'administrateur alors assigne une adresse et le plein sous-réseau \56 à l'ASA en dehors de l'interface et choisit une certaine plage interne pour l'utiliser pour les serveurs intérieurs. Cependant, avec l'IPv6, tous les hôtes internes devraient également utiliser des adresses routable d'IPv6, et le bloc d'ipv6 addres devrait être décomposé en sous-réseaux plus petits comme nécessaire. Dans ce scénario, vous pouvez créer beaucoup de sous-réseaux \64 pendant qu'une partie du bloc \56 qui a été alloué.

> **Conseil** : Référez-vous à RFC 4291 pour information les informations complémentaires.

Codage modifié EUI 64

L'ASA peut être configurée afin d'exiger des adresses modifiées d'IPv6 EUI-64-encoded. L'EUI, selon RFC 4291, permet à un hôte pour s'assigner un seul identifiant d'interface 64-bit d'IPv6 (EUI-64). Cette caractéristique est un avantage par rapport à l'ipv4, car elle retire la condition requise d'utiliser le DHCP pour l'affectation d'ipv6 addres.

Si l'ASA est configurée afin d'exiger cette amélioration par l'intermédiaire de la commande de **nameif de l'IPv6 enforce-eui64**, alors elle relâchera vraisemblablement beaucoup de sollicitations et d'annonces voisines de détection d'autres hôtes sur le sous-réseau local.

> **Conseil** : Le pour en savoir plus, se rapportent compréhension derrière le document de la Communauté de support de Cisco d'adresse de bit de l'IPv6 EUI-64.

Les clients utilisent des adresses provisoires d'IPv6 par défaut

Par défaut, beaucoup de systèmes d'exploitation de client (OSs), comme des versions 7 et 8 de Microsoft Windows, Macintosh OS-X, et systèmes basés sur Linux, utilisent des adresses *provisoires* avec auto-assignation d'IPv6 pour l'intimité étendue par l'intermédiaire de l'autoconfiguration sans état d'adresse d'IPv6 (SLAAC).

Cisco TAC a vu quelques cas où ceci a posé des problèmes inattendus dans les environnements parce que les hôtes génèrent le trafic de l'adresse provisoire et pas de l'adresse statique-assignée. En conséquence, l'ACLs et les artères gérées par le système central pourraient entraîner le trafic à devenu relâchés ou incorrectement conduits, qui fait échouer la transmission d'hôte.

Il y a deux méthodes qui sont utilisées afin d'adresser cette situation. Le comportement peut être désactivé individuellement sur les systèmes client, ou vous pouvez désactiver ce comportement sur les Routeurs ASA et de Cisco IOS®. De l'ASA ou du côté routeur, vous devez modifier l'indicateur de message de publicité de routeur (RA) qui déclenche ce comportement.

Référez-vous aux sections suivantes afin de désactiver ce comportement sur les différents systèmes de clients.

Microsoft Windows

Terminez-vous ces étapes afin de désactiver ce comportement sur des systèmes de Microsoft

Windows :

1. Dans Microsoft Windows, ouvrez une invite de commande élevée (passage comme administrateur).

2. Sélectionnez cette commande afin de désactiver la configuration aléatoire de génération d'adresse IP, et puis l'appuyez sur **entrent** :

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

3. Sélectionnez cette commande afin de forcer Microsoft Windows pour utiliser la norme EUI-64 :

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

4. Redémarrez l'ordinateur afin d'appliquer les modifications.

Macintosh OS-X

Dans un terminal, sélectionnez cette commande afin de désactiver l'IPv6 SLAAC sur l'hôte jusqu'à la prochaine réinitialisation :

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

Afin de faire la constante de configuration, sélectionnez cette commande :

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

Linux

Dans un shell terminal, sélectionnez cette commande :

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

Débronchement SLAAC globalement de l'ASA

La deuxième méthode qui est utilisée afin d'adresser ce comportement est de modifier le message de RA qui est envoyé de l'ASA aux clients, qui déclenche l'utilisation de SLAAC. Afin de modifier le message de RA, sélectionnez cette commande de *mode de configuration d'interface* :

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

Cette commande modifie le message de RA qui est envoyé par l'ASA de sorte qu'A - indicateur de bit n'est pas placé, et les clients ne génèrent pas un ipv6 addres provisoire.

> **Conseil** : Référez-vous à RFC 4941 pour information les informations complémentaires.

Foires aux questions d'IPv6

Cette section décrit quelques forums aux questions en vue de l'utilisation de l'IPv6.

Est-ce que je peux passer le trafic pour l'ipv4 et l'IPv6 sur la même interface, en même temps ?

Oui. Vous devez simplement activer l'IPv6 sur l'interface et assigner un ipv4 et un ipv6 addres à l'interface, et elle manipule les deux types de trafic simultanément.

Est-ce que je peux m'appliquer l'IPv6 et l'ipv4 ACLs à la même interface ?

Vous pouvez faire ceci dans des versions ASA plus tôt que la version 9.0(1). En date de la version 9.0(1) ASA, tout l'ACLs sur l'ASA *sont unifiés*, ainsi il signifie qu'un ACL prend en charge un mélange d'entrées d'ipv4 et d'IPv6 dans le même ACL.

Dans des versions 9.0(1) et ultérieures ASA, l'ACLs sont simplement fusionnés ensemble et l'ACL simple et unifié est appliqué à l'interface par l'intermédiaire de l'ordre d'**access-group**.

L'ASA prend en charge-elle QoS pour l'IPv6 ?

Oui. L'ASA prend en charge le maintien de l'ordre et la file d'attente à priorité déterminée pour l'IPv6 de la même manière qu'elle fait avec l'ipv4.

En date de la version 9.0(1) ASA, tout l'ACLs sur l'ASA *sont unifiés*, ainsi il signifie qu'un ACL prend en charge un mélange d'entrées d'ipv4 et d'IPv6 dans le même ACL. En conséquence, toutes les commandes de QoS qui sont décrétées sur un class-map qui apparie un ACL agissent sur le trafic d'ipv4 et d'IPv6.

Est-ce que je devrais utiliser NAT avec l'IPv6 ?

Bien que NAT peut être configurée pour l'IPv6 sur l'ASA, l'utilisation de NAT dans l'IPv6 est fortement découragée et inutile, donné la quantité infinie proche d'adresses disponibles et globally-routable d'IPv6.

Si NAT est exigé dans un scénario d'IPv6, vous peut trouver plus d'informations sur la façon les configurer dans la section d'instructions d'ipv6 nat de l'*ouvrage 2 CLI : Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, 9.4*.

> **Note**: Il y a quelques instructions et limites qui devraient être considérées quand vous implémentez NAT avec l'IPv6.

Pourquoi est-ce que je vois les adresses d'IPv6 de lien-gens du pays dans la sortie de commande de *Basculement d'exposition* ?

Dans l'IPv6, le ND emploie des adresses locales à la liaison afin d'exécuter l'address resolution L2. Pour cette raison, les adresses d'IPv6 pour les interfaces surveillées dans la sortie de commande de **Basculement d'exposition** affichent l'adresse locale à la liaison et pas l'ipv6 addres global qui est configurée sur l'interface. C'est comportement prévu.

Mises en garde/demandes d'amélioration connues

Voici quelques mises en garde connues en vue de l'utilisation de l'IPv6 :

- *La clause de « correspondance » de capture du ASA 8.x du* Â d'âÂ de l'ID de bogue Cisco CSCtn09836 *n'attrape pas le trafic d'IPv6*
- *ENH du* Â d'âÂ de l'ID de bogue Cisco CSCuq85949 *: Soutien d'IPv6 ASA de WCCP*
- *Le routage de l'IPv6 ECMP du ASA du* Â d'âÂ de l'ID de bogue Cisco CSCut78380 *n'équilibre pas la charge le trafic*

Informations connexes

- Internet Protocol de du Â d'âÂ RFC 2460, spécification de la version 6 (IPv6)
- Architecture d'adressage d'IP version 6 de du Â d'âÂ RFC 4291
- Détection voisine de du Â d'âÂ RFC 4861 pour l'IP version 6 (IPv6)
- Ouvrage 1 CLI : Guide de configuration général CLI d'exécutions de gamme de Cisco ASA, 9.4 IPv6 de du Â d'âÂ
- SSL d'AnyConnect au-dessus d'IPv4+IPv6 à la configuration ASA
- Cisco Systems du Â d'âÂ de Soutien technique et de documentation