Conformité IPV6 d’un switch Cisco L3

Le switch Cisco ne doit pas être configuré pour utiliser des adresses locales IPv6 Unicast.

Telles que définies actuellement, les adresses locales sont ambiguës et peuvent être présentes sur plusieurs sites. L'adresse elle-même ne contient aucune indication du site auquel elle appartient. L'utilisation d'adresses locales peut nuire à la sécurité du réseau et provoquer des erreurs de routage, comme indiqué dans la section 2 de la RFC3879.

La RFC3879 désapprouve formellement le préfixe Unicast IPv6 FEC0::/10 défini dans la RFC3513.

Vérification

Vérifiez la configuration du switch pour vous assurer qu'aucune adresse IPv6 FEC0::/10 n'est définie.

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les annonces sur toutes les interfaces externes compatibles IPv6.

De nombreuses attaques ARP ont déjà été documentées en IPV4.

Afin d’atténuer ces vulnérabilités, les connexions sur lesquelles il n’y aucune machine doivent être configurées pour supprimer les annonces. C’est le cas notamment des réseaux d’interconnexion.

Sur le switch, vérifier que toutes les annonces sont supprimées sur les interfaces IPV6 des réseaux d’interconnexion.

La configuration devrait ressembler à l'exemple ci-dessous :

```
interface gigabitethernet1/0
ipv6 address 2001::1:0:22/64
ipv6 nd ra suppress
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPV6 indéterminés.

L'une des faiblesses de la fragmentation IPV6 est le paquet de transport non déterminé. Ce paquet peut contenir un protocole non déterminé provoqué par la fragmentation. En fonction de la longueur de la chaîne d'en-têtes d'extension IPv6, le fragment initial peut ne pas contenir les informations de port de la couche quatre du paquet.

Vérifiez la configuration du switch pour déterminer s’il est configuré pour rejeter les paquets de transport IPV6 indéterminés.

Vérifier qu’une ACL IPV6 entrante a été configurée sur l’interface externe.

Vérifier que l’ACL rejette les paquets de transport indéterminés comme indiqué ci-dessous :

```
SW1(config)# ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny ipv6 any any undetermined-
transport log
SW1(config-ipv6-acl)#permit ipv6 … … … …
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config-ipv6-acl)#exit
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6 in
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPV6 avec un type d’en-tête de routage 0, 1 ou 3-255.

L'en-tête de routage peut être utilisé de manière malveillante pour envoyer un paquet via un chemin moins sécurisé que celui qui est supposé être légitime par les protocoles de routage. L’utilisation de l’en-tête d’extension de routage a peu d’utilité, hormis son implémentation par Mobile IPV6.

L’en-tête de routage de type 0 (RFC 5095) est dangereux car il permet aux attaquants d’usurper des adresses sources.

L’en-tête de routage de type 1 est défini par une spécification appelée « Nimrod Routing », un projet abandonné de la DARPA. La plupart des implémentation ne reconnaisse pas cet en-tête.

Les en-têtes de routage de type 3 à 255 sont actuellement indéfinies et doivent être supprimées en entrée et en sortie.

Vérifier que le switch rejette les paquets IPV6 avec des en-têtes de routage de type 0, 1 ou 3 à 255. Dans l’exemple ci-dessous, seul le type 2 est autorisé vers la machine 2001:DB8::0:1:1:1234 :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#permit ipv6 any host
2001:DB8::0:1:1:1234 routing-type 2
SW1(config-ipv6-acl)#deny ipv6 any any routing log
SW1(config-ipv6-acl)#permit … … … …
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config)#int g1/0 SW1(config-if)#ipv6 traffic-filter
FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPv6 contenant un en-tête Hop-by-Hop avec des valeurs de type d'option non valides.

Ces options sont réservées à l'en-tête « Options de destination ». Le caractère facultatif et extensible des en-têtes d'extension IPv6 nécessite une attention particulière, car de nombreuses implémentations ne rejettent pas systématiquement les paquets dont les en-têtes sont illisibles, ce qui peut entraîner un déni de service sur l'appareil cible. De plus, le formatage TLV (type, longueur, valeur) permet d'utiliser des en-têtes très volumineux.

Examinez la configuration du switch Cisco pour vérifier qu'elle rejette correctement les paquets IPV6 contenant un en-tête avec un type d’option invalide :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny hbh any any dest-option-type
4 log
SW1(config-ipv6-acl)#deny hbh any any dest-option-type
195 log
SW1(config-ipv6-acl)#deny hbh any any dest-option-type
home-address log
SW1(config-ipv6-acl)# permit ipv6 … … … …
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPv6 contenant un en-tête d’option de destination avec des valeurs de type d'option non valides.

Ces options sont réservées à l'en-tête « Hop-by-hop ». Le caractère facultatif et extensible des en-têtes d'extension IPv6 nécessite une attention particulière, car de nombreuses implémentations ne rejettent pas systématiquement les paquets dont les en-têtes sont illisibles, ce qui peut entraîner un déni de service sur l'appareil cible. De plus, le formatage TLV (type, longueur, valeur) permet d'utiliser des en-têtes très volumineux.

Examinez la configuration du switch Cisco pour vérifier qu'elle rejette correctement les paquets IPV6 contenant un en-tête d’option de destination avec des valeurs de type 0x05 (alerte de switch) ou 0xC2 (Charge utile Jumbo) :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny 60 any any dest-option-type 5
log
SW1(config-ipv6-acl)#deny 60 any any dest-option-type
194 log
SW1(config-ipv6-acl)#permit … … … …
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPv6 contenant un en-tête d’extension avec l’option d’identification du point de terminaison.

Le caractère facultatif et extensible des en-têtes d'extension IPv6 nécessite une attention particulière, car de nombreuses implémentations ne rejettent pas systématiquement les paquets dont les en-têtes sont illisibles, ce qui peut entraîner un déni de service sur l'équipement cible. De plus, le formatage TLV (type, longueur, valeur) permet d'utiliser des en-têtes très volumineux. Ce type d'option est associé au système de routage Nimrod et ne fait l'objet d'aucune RFC.

Examinez la configuration du switch Cisco pour vérifier qu'elle rejette correctement les paquets IPV6 contenant des valeurs de type 0x8A (identification du point de terminaison), et ce qu’elles apparaissent dans un en-tête d’option Hop-by-Hop ou Destination :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny any any dest-option-type 138
log
SW1(config-ipv6-acl)#permit ipv6 … … … …
SW1(config-ipv6-acl)# deny ipv6 any any log
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPv6 contenant l’option d’adresse NSAP dans l’en-tête d’option de destination.

Le caractère facultatif et extensible des en-têtes d'extension IPv6 nécessite une attention particulière, car de nombreuses implémentations ne rejettent pas systématiquement les paquets dont les en-têtes sont illisibles, ce qui peut entraîner un déni de service sur l'équipement cible. De plus, le formatage TLV (type, longueur, valeur) permet d'utiliser des en-têtes très volumineux. Ce type d'option, issu de la RFC 1888 (NSAP OSI et IPV6), a été abandonné par la RFC 4048.

Configurez le switch pour supprimer les paquets IPV6 contenant l’option d’adresse NSAP dans l’en-tête d’option de destination comme indiqué dans l’exemple ci-dessous :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny 60 any any dest-option-type
195 log
SW1(config-ipv6-acl)#permit … … … …
SW1(config-ipv6-acl)# deny ipv6 any any log
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour supprimer les paquets IPv6 contenant un en-tête d’extension Hop-By-Hop ou Destination Option avec un type d’option non défini.

Le caractère facultatif et extensible des en-têtes d'extension IPv6 nécessite une attention particulière, car de nombreuses implémentations ne rejettent pas systématiquement les paquets dont les en-têtes sont illisibles, ce qui peut entraîner un déni de service sur l'équipement cible. De plus, le formatage TLV (type, longueur, valeur) permet d'utiliser des en-têtes très volumineux.

Configurez le switch pour supprimer tous les paquets IPV6 entrant contenant une valeur de type d’option non définie, qu’ils apparaissent dans un en-tête Hop-by-Hp ou Destination Option, comme illustré dans l’exemple ci-dessous :

```
SW1(config)#ipv6 access-list FILTER_IPV6
SW1(config-ipv6-acl)#deny any any dest-option-type 2
SW1(config-ipv6-acl)#deny any any dest-option-type 3
SW1(config-ipv6-acl)#deny any any dest-option-type 6
SW1(config-ipv6-acl)#deny any any dest-option-type 9
SW1(config-ipv6-acl)#deny any any dest-option-type 10
SW1(config-ipv6-acl)#deny any any dest-option-type 11
SW1(config-ipv6-acl)#deny any any dest-option-type 12
SW1(config-ipv6-acl)#deny any any dest-option-type 13
SW1(config-ipv6-acl)#deny any any dest-option-type 14
SW1(config-ipv6-acl)#deny any any dest-option-type 16
SW1(config-ipv6-acl)#deny any any dest-option-type 34
SW1(config-ipv6-acl)#deny any any dest-option-type 36
SW1(config-ipv6-acl)#deny any any dest-option-type 37
SW1(config-ipv6-acl)#deny any any dest-option-type 39
SW1(config-ipv6-acl)#deny any any dest-option-type 47
SW1(config-ipv6-acl)#deny any any dest-option-type 49
```

```
SW1(config-ipv6-acl)#deny any any dest-option-type 255
SW1(config-ipv6-acl)#permit … … … …
SW1(config-ipv6-acl)#deny ipv6 any any log
SW1(config)#int g1/0
SW1(config-if)#ipv6 traffic-filter FILTER_IPV6
```

Conformité IPV6 d’un switch Cisco L3

Le switch Cisco doit être configuré pour annoncer une limite de saut d’au moins 32 dans les messages d’annonce pour les déploiements de configuration automatique.

Le protocole Neighbor Discovery permet aux routeurs d'annoncer une valeur limite de sauts dans un message d'annonce de routeur utilisé par les hôtes, au lieu de la valeur par défaut standardisée. Si une valeur très faible était configurée et annoncée aux hôtes du segment LAN, les communications échoueraient car la limite de sauts atteindrait zéro avant que les paquets envoyés par un hôte n'atteignent leur destination.

Configurez le switch pour annoncer une limite de saut d’au moins 32 :

```
SW1(config)#ipv6 hop-limit 128
```