

Échec du trafic XPN MACSec entre Catalyst 9500 et Nexus 9000 avec augmentation des paquets non valides et des erreurs FCS

Table des matières

Problème

Lorsque MACSec XPN est activé entre un Catalyst 9500-28C8D et un Nexus N9K-C93180YC-FX, la session MKA s'établit correctement mais aucun trafic de données ne passe par la liaison. Le Catalyst 9500 signale une augmentation des « paquets non valides » sous les statistiques SA et les erreurs d'entrée FCS sur l'interface physique. Plus précisément, ces symptômes ont été observés :

- Aucune connectivité une fois MACSec activé
- La session MKA s'affiche comme établie, mais le côté Catalyst 9500 affiche les statistiques SA avec "Pkts non valides 118" croissant et "Pkts valides : 0"
- Les erreurs d'entrée FCS augmentent sur l'interface physique du Catalyst 9500
- La suppression de la configuration MACSec restaure immédiatement la connectivité et arrête les erreurs FCS

Les sessions MKA ont été établies sur les deux périphériques et ont réussi à négocier le chiffrement GCM-AES-XPN-256. Le côté Nexus a indiqué que le chiffrement était actif, mais le Catalyst 9500 a reçu des paquets chiffrés et les a rejetés en raison d'une non-concordance de validation, ce qui a entraîné l'acceptation de zéro paquet valide.

Environnement

- Catalyst 9500-28C8D exécutant Cisco IOS®
- Nexus N9K-C93180YC-FX

- Configuration MACSec XPN à l'aide de la suite de chiffrement GCM-AES-XPN-256
- Interface 400 Gigabit Ethernet (FourHundredGigE1/0/15 sur Catalyst, Ethernet1/52 sur Nexus)
- Catalyst 9500 configuré en tant que priorité de serveur clé 1, Nexus configuré en tant que priorité de serveur clé 100
- Algorithme cryptographique AES-256-CMAC pour clés pré-partagées

Résolution

Le problème a été résolu par la mise en oeuvre d'une solution de contournement qui modifie l'attribution du rôle clé-serveur entre les périphériques. La résolution recommandée comprend les étapes suivantes :

Étape 1: Identifier le problème de configuration du serveur de clés

Vérifiez la configuration actuelle de la priorité clé-serveur sur les deux périphériques. La configuration problématique montrait :

Configuration du Catalyst 9500 :

```
mka policy MEHEALTH-ORG-XPN
  key-server priority 1
  macsec-cipher-suite gcm-aes-xpn-256
```

Configuration de Nexus :

```
macsec policy MEHEALTH-ORG-XPN
  key-server-priority 100
```

Étape 2: Mise en oeuvre de la solution de contournement des rôles serveur clé

Configurez le périphérique Nexus en tant que serveur de clés MACSec au lieu du Catalyst 9500. Cela implique de régler les valeurs de priorité de serveur de clés de sorte que Nexus assume le rôle de serveur de clés.

Modifiez la configuration Nexus pour avoir une valeur de priorité clé-serveur inférieure (les valeurs inférieures ont une priorité supérieure) :

```
macsec policy MEHEALTH-ORG-XPN  
  key-server-priority 1
```

Modifiez la configuration du Catalyst 9500 pour obtenir une valeur de priorité clé-serveur supérieure :

```
mka policy MEHEALTH-ORG-XPN  
  key-server priority 100  
  macsec-cipher-suite gcm-aes-xpn-256
```

Étape 3: Vérification du fonctionnement de MACSec

Après avoir mis en oeuvre le changement de rôle de serveur de clés, vérifiez que :

- Les sessions MKA s'établissent correctement sur les deux périphériques
- Le trafic de données passe par la liaison compatible MACSec
- Aucun paquet non valide n'est incrémenté dans les statistiques de l'association de sécurité Catalyst 9500
- Les erreurs d'entrée FCS ne se produisent pas sur l'interface physique

Cette solution de contournement permet à la configuration XPN MACSec de fonctionner correctement jusqu'à ce que l'étude de la plate-forme et la planification de la mise à niveau logicielle soient terminées.

Motif

La cause principale de ce problème est liée à l'ID de bogue Cisco CSCvs00410, qui décrit un scénario où les sessions MKA s'établissent correctement mais où les données ne peuvent pas passer à travers la liaison lors de l'utilisation d'AES-256-XPB avec un Catalyst 9500 dans le rôle de serveur clé dans certaines conditions d'interopérabilité avec les périphériques Nexus. Ce comportement se manifeste par une non-concordance de validation lorsque le Catalyst 9500 rejette des paquets chiffrés du Nexus, ce qui entraîne une augmentation du nombre de paquets non valides et des erreurs FCS. Il y avait une différence constatée concernant le fait que Cisco IOS était répertorié comme étant corrigé pour ce défaut, nécessitant une enquête plus approfondie de la part de l'équipe de la plate-forme Catalyst.

Autres informations utiles

- ID de bogue Cisco CSCvs00410 : session MKA active mais impossible de transmettre des données via la liaison lors de l'utilisation d'AES-256-XPB avec le rôle de serveur de clés Catalyst 9500

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.