Résoudre les défaillances du contrôle d'intégrité des PDU MACSec MKA sur les commutateurs Nexus 9000

Table des matières

Problème

La sécurité MACSec (Media Access Control Security) configurée entre les commutateurs Nexus 9000 indique que la session MKA (MACsec Key Agreement) est « sécurisée », mais génère des messages d'erreur répétés environ toutes les deux secondes. Le modèle suivant inonde les journaux système :

```
device# %CTS-5-CTS_MKPDU_ICV_SUCCESS: MACSec: MKPDU verified. Primary keys match for Interface
device# %CTS-4-CTS_MKPDU_ICV_FAILURE: MACSec: MKA PDU integrity check failed for Interface
```

Ces messages alternatifs de réussite et d'échec créent des entrées de journal excessives qui doivent être corrigées tout en conservant la fonctionnalité MACSec.

Environnement

- Produit : commutateurs Cisco Nexus
- Technologie : MACSec (Link Encryption)

Résolution

Pour résoudre ce problème, modifiez la configuration de la chaîne de clés de secours afin d'utiliser des ID de clés différents de ceux configurés dans la chaîne de clés principale :

1. Passez en revue vos configurations de chaîne de clés MACSec existantes pour identifier les ID de clé correspondants entre les chaînes de clés principale et de secours à l'aide de cette commande.

```
device# show running-configuration
...
key chain primary macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
key chain fallback macsec
 key 01
 key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
...
```

2. Modifiez la chaîne de clés de secours pour utiliser un ID de clé différent avec ces commandes. Par exemple, si la chaîne de clés primaires utilise l'ID de clé 01, configurez la chaîne de clés de secours pour utiliser l'ID de clé 10 à la place.

```
device# configure terminal
device(config)# key chain fallback macsec
device(config)# no key 01
device(config)# key 10
device(config)# key-octet-string 7 <key> cryptographic-algorithm AES_256_CMAC
```

3. Surveillez les journaux système pour confirmer que les messages CTS_MKPDU_ICV_SUCCESS et CTS_MKPDU_ICV_FAILURE alternatifs n'apparaissent plus.

Motif

La cause principale est un conflit de configuration où la chaîne de clés de secours utilise le même ID de clé que la chaîne de clés principale. Cela crée de l'ambiguïté dans le protocole MKA, ce qui entraîne la réussite et l'échec alternatifs du contrôle d'intégrité lorsque le système bascule entre l'évaluation des clés primaire et de secours. Le Guide de configuration de Nexus MACSec indique, « L'ID de clé de secours ne doit correspondre à aucun ID de clé d'une chaîne de clés primaire » pour empêcher ce conflit.

Autres informations utiles

- Guide de configuration de Nexus MACSec
- Assistance technique de Cisco et téléchargements

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.