Comprendre les compteurs ACL cryptographiques dans les tunnels VPN basés sur des politiques

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Topologie

Scénarios

- Scénario 1 : Trafic initié à partir du Router1 alors que le tunnel VPN est inactif
- Scénario 2 : Trafic initié à partir du Router2 alors que le tunnel VPN est actif

Configuration

- Configuration du cryptage sur Router1
- Configuration du chiffrement sur le routeur 2

Analyse comportementale des compteurs de la liste de contrôle d'accès cryptographique dans les tunnels VPN

- Scénario 1 : Trafic initié à partir du Router1 alors que le tunnel VPN est inactif
- Scénario 2 :Trafic initié depuis le routeur 2 alors que le tunnel VPN est actif

Conclusion:

Points importants :

Introduction

Ce document décrit le comportement des compteurs ACL (Access Control List) de chiffrement dans les tunnels VPN basés sur des politiques.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- VPN site à site basé sur des politiques sur la plate-forme Cisco IOS® /Cisco IOS® XE
- Listes de contrôle d'accès sur la plate-forme Cisco IOS/Cisco IOS XE

Composants utilisés

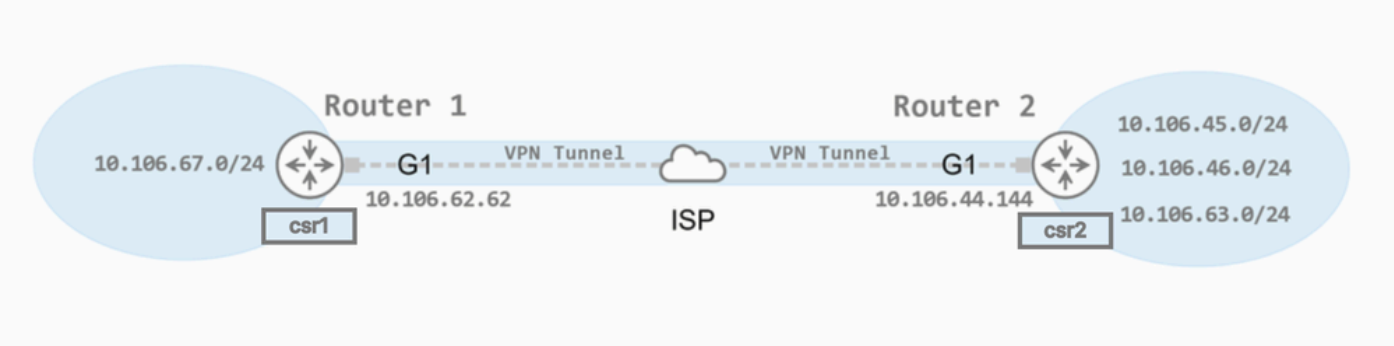
Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco C8kv, version 17.12.04(MD)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie



Topologie

Scénarios

En examinant deux scénarios distincts, nous cherchons à comprendre comment le nombre d'occurrences de la liste de contrôle d'accès est affecté lorsque le trafic est initié à partir de différents homologues et lorsque les tunnels sont réinitialisés.

1. Scénario 1 : Trafic initié à partir du Router1 alors que le tunnel VPN est inactif

   Dans ce scénario, les modifications du nombre de succès de la liste de contrôle d'accès sont analysées lorsque le tunnel VPN est initialement arrêté et le trafic est initié à partir du routeur 1. Cette analyse aide à comprendre la configuration initiale et la façon dont les compteurs de la liste de contrôle d'accès cryptographique réagissent à la première tentative de flux de trafic.

2. Scénario 2 : Trafic initié à partir du Router2 alors que le tunnel VPN est actif

   Dans ce scénario, le tunnel VPN est déjà établi et le trafic est initié à partir du routeur 2 est exploré. Ce scénario fournit des informations sur le comportement des compteurs ACL lorsque le tunnel est actif et que le trafic est introduit à partir d'un homologue différent.

En comparant ces scénarios, nous pouvons obtenir une compréhension complète de la dynamique des compteurs ACL dans les tunnels VPN dans des conditions variées.

Configuration

Nous avons configuré un tunnel VPN site à site basé sur des politiques entre deux routeurs Cisco C8kv, désignés comme homologues. Le routeur 1 est nommé « csr1 » et le routeur 2 « csr2 ».

Configuration du cryptage sur Router1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Configuration du chiffrement sur le routeur 2

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
```

```
GigabitEthernet4      10.106.63.13      YES     NVRAM        up          up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Analyse comportementale des compteurs de la liste de contrôle d'accès cryptographique dans les tunnels VPN

Initialement, les deux périphériques ont un nombre d'occurrences de liste de contrôle d'accès égal à zéro sur leurs listes d'accès de chiffrement respectives.



La liste de contrôle d'accès a atteint zéro sur leurs listes d'accès de chiffrement respectives sur les deux périphériques homologues.

Scénario 1 : Trafic initié à partir du Router1 alors que le tunnel VPN est inactif

État initial :

Le tunnel VPN connectant le routeur 1 (IP: 10.106.67.27) et Router2 (IP : 10.106.45.145) est actuellement inactif.

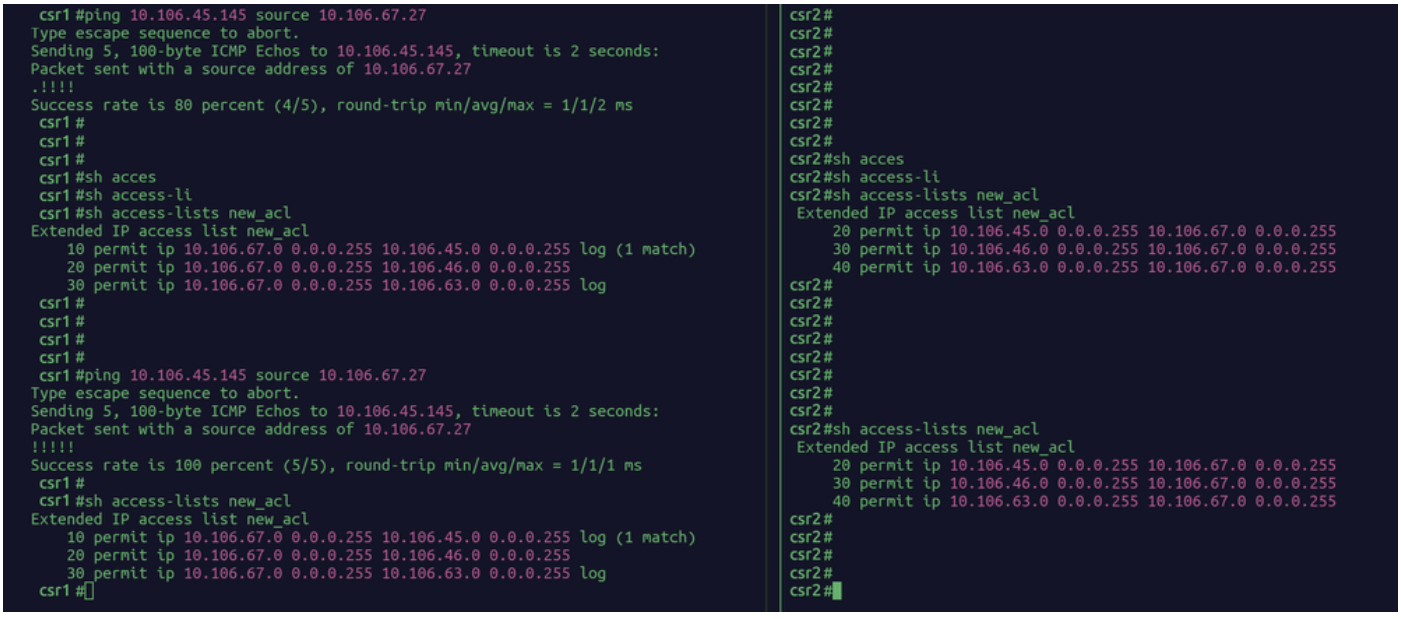
Mesure prise:

Le trafic est initié à partir du routeur 1, destiné à établir la communication avec le routeur 2.

Observations :

1. Comportement du compteur ACL :
   a. Lors de l'initialisation du trafic à partir du routeur 1, il y a un incrément notable dans le compteur de la liste de contrôle d'accès (ACL) sur le routeur 1. Cette augmentation ne se produit qu'une seule fois au moment où le tunnel tente de s'établir.
   b. L'augmentation du compteur de liste de contrôle d'accès est observée exclusivement sur le routeur initiateur, qui est le routeur 1 dans ce scénario. À ce stade, le routeur 2 ne reflète aucune modification de son compteur de liste de contrôle d'accès.
2. Établissement du tunnel :
   a. Après l'incrément initial correspondant à l'initiation du trafic, le tunnel entre le premier routeur et le routeur 2 est établi avec succès.
   b. Après l'établissement du tunnel, le compteur de liste de contrôle d'accès sur le routeur 1 se stabilise et ne présente pas d'incréments supplémentaires, ce qui indique que la règle de liste de contrôle d'accès a été mise en correspondance et autorise désormais de manière cohérente le trafic à traverser le tunnel établi.
3. Réinitialisation du tunnel :
   Le compteur de liste de contrôle d'accès sur Router1 subit un autre incrément uniquement si le tunnel est abandonné et nécessite un rétablissement. Cela suggère que la règle de la liste de contrôle d'accès est déclenchée par l'initiation initiale du trafic qui tente d'établir le tunnel, plutôt que par le transfert de données en cours une fois que le tunnel est actif.

En résumé, ce scénario démontre que le compteur de liste de contrôle d'accès sur le routeur 1 est sensible aux tentatives initiales de trafic pour la création de tunnel, mais reste statique une fois que le tunnel VPN est activé et opérationnel.



Scénario 2 :Trafic initié depuis le routeur 2 alors que le tunnel VPN est actif

État initial :

Le tunnel VPN connectant le routeur 1 (IP: 10.106.67.27) et Router2 (IP : 10.106.45.145) est actuellement actif et opérationnel.

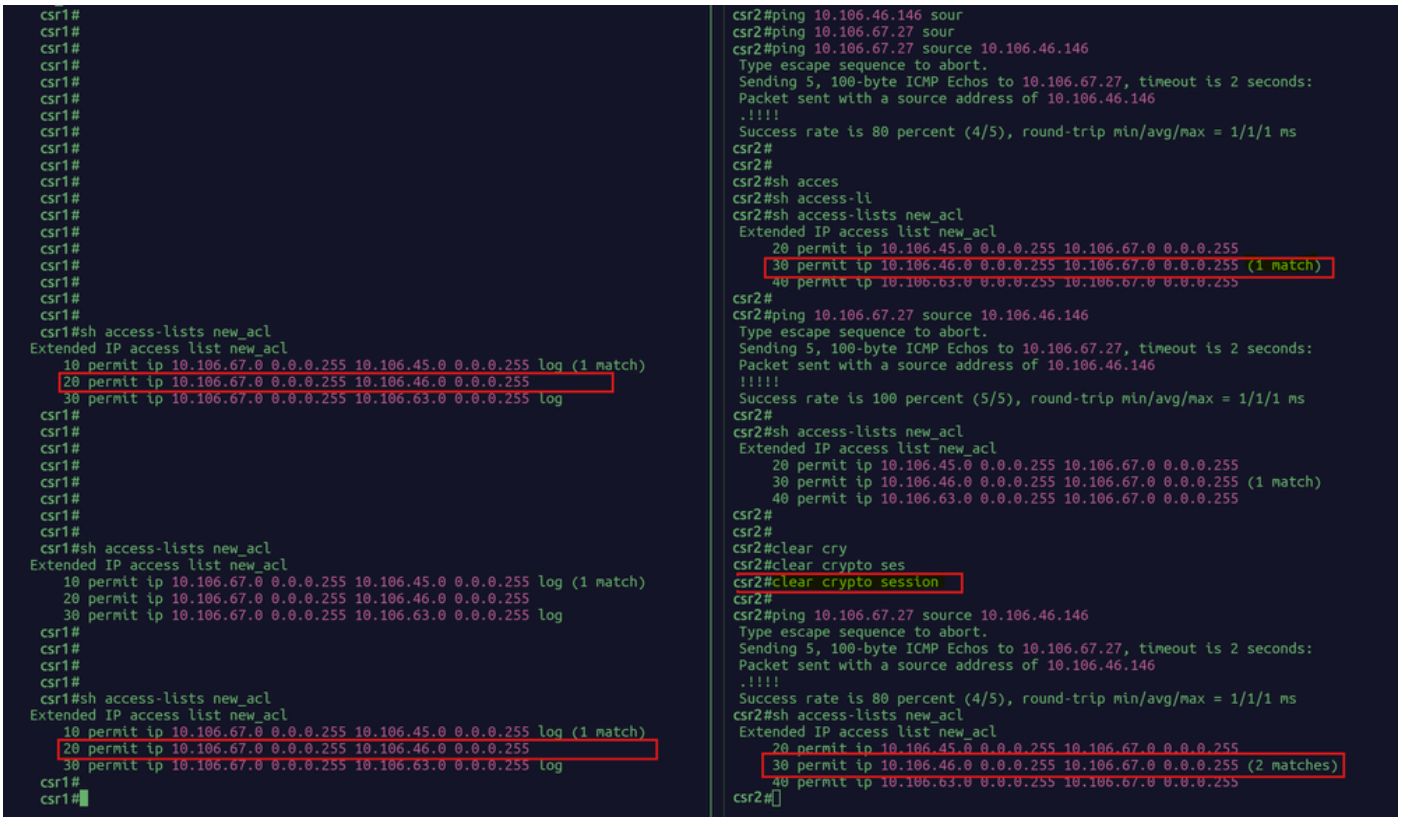
Mesure prise:

1. Le trafic est initié du routeur 2 vers le routeur 1 pendant que le tunnel est actif.
2. Ensuite, le tunnel est délibérément effacé (ou réinitialisé).
3. Une fois le tunnel effacé, le routeur 2 réinitialise le trafic pour rétablir la connexion.

Observations :

1. Initiation initiale du trafic :
   a. Lorsque le trafic est initié pour la première fois à partir du routeur 2 alors que le tunnel est déjà établi, il n'y a pas de changement immédiat dans le compteur de liste de contrôle d'accès (ACL).
   b. Cela indique que le trafic en cours dans un tunnel déjà établi ne déclenche pas l'incrément du compteur de liste de contrôle d'accès.
2. Suppression et réinitialisation du tunnel :
   a. Une fois le tunnel libéré, la connexion établie entre le premier routeur et le routeur 2 est temporairement interrompue. Cela nécessite un processus de rétablissement pour tout trafic ultérieur.
   b. Lorsque le trafic est réinitialisé à partir du Routeur2 après que le tunnel a été effacé, il y a un incrément observable dans le compteur ACL sur le Routeur2. Cet incrément signifie que les règles ACL sont engagées une fois de plus pour faciliter la création du tunnel.
3. Spécificité du compteur ACL :
   L'incrémentation du compteur de liste de contrôle d'accès se produit uniquement du côté de l'initiation du trafic, qui est dans ce cas le routeur 2. Ce comportement met en évidence le rôle de la liste de contrôle d'accès dans la surveillance et le contrôle des processus d'initiation du trafic du côté de l'origine, tandis que le compteur de liste de contrôle d'accès du routeur 1 n'est pas affecté pendant cette phase.

En résumé, ce scénario illustre que le compteur de liste de contrôle d'accès sur le routeur 2 réagit à l'initiation du trafic lors du rétablissement d'un tunnel VPN. Le compteur n'augmente pas avec le flux de trafic régulier dans un tunnel actif, mais réagit au besoin de rétablissement du tunnel, assurant un suivi précis des événements d'initiation du tunnel.



Scénario 2

Conclusion:

Le comportement des compteurs ACL de chiffrement révèle qu'ils enregistrent le nombre de succès exclusivement pendant la phase d'initiation du tunnel VPN.

Incrément spécifique à l'initiateur : Lorsque le tunnel est initié à partir du Routeur1, l'augmentation du nombre d'accès est observée uniquement sur le Routeur1. De même, si l'initiation se produit à partir du Routeur2, le nombre d'accès augmente uniquement sur le Routeur2. Cela met en évidence le rôle de la liste de contrôle d'accès dans la surveillance du processus d'initiation du trafic à la source.

Stabilité après établissement : Une fois que le tunnel est correctement établi, les compteurs ACL sur les deux homologues restent inchangés, ce qui indique qu'il n'y a pas d'autres occurrences. Cette stabilité persiste jusqu'à ce que le tunnel soit effacé ou réinitialisé, et que l'initiation du trafic soit tentée à nouveau.
Ce comportement souligne la fonctionnalité des listes de contrôle d'accès dans le suivi et le contrôle de la phase initiale de création du tunnel, assurant que le flux de données suivant dans le tunnel établi n'affecte pas le nombre de succès.

Points importants :

Comportement du compteur ACL : Les compteurs ACL enregistrent les incréments uniquement du côté de l'initiateur pendant le processus d'initiation du tunnel. Cela indique que les compteurs sont conçus pour surveiller le trafic initial qui déclenche l'établissement du tunnel.

Compteurs statiques Post-établissement : Une fois le tunnel actif et établi, les compteurs ACL restent inchangés. Elles ne reflètent aucune activité ultérieure, sauf si le tunnel est réinitialisé et doit être réinitialisé, ce qui souligne l'importance accordée aux événements de trafic initiaux.

Spécificité d'initialisation du trafic : Le nombre de succès de la liste de contrôle d'accès est spécifique à l'homologue initiant le tunnel. Cette spécificité assure un suivi précis de quel côté est responsable de l'établissement de la connexion VPN, ce qui permet une surveillance et un contrôle précis.

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.

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.