# Contenu



# Introduction

Ce document décrit comment installer un tunnel de la version 2 d'échange de clés Internet (IKE) de site à site (IKEv2) entre une appliance de sécurité adaptable Cisco (ASA) et un routeur qui exécute le logiciel d'Â® de Cisco IOS.

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 2 (IKEv2) d'échange de clés Internet (IKE)
- Certificats et Infrastructure à clés publiques (PKI)
- Protocole NTP (Network Time Protocol)

## Composants utilisés

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

- Serveur de sécurité adaptatif dédié de la gamme Cisco ASA 5510 qui exécute la version de logiciel 9.1(3)
- L'Integrated Services Router de gamme Cisco 2900 (ISR) ce exécute la version de logiciel 15.3(3)M1 de Cisco IOS

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.

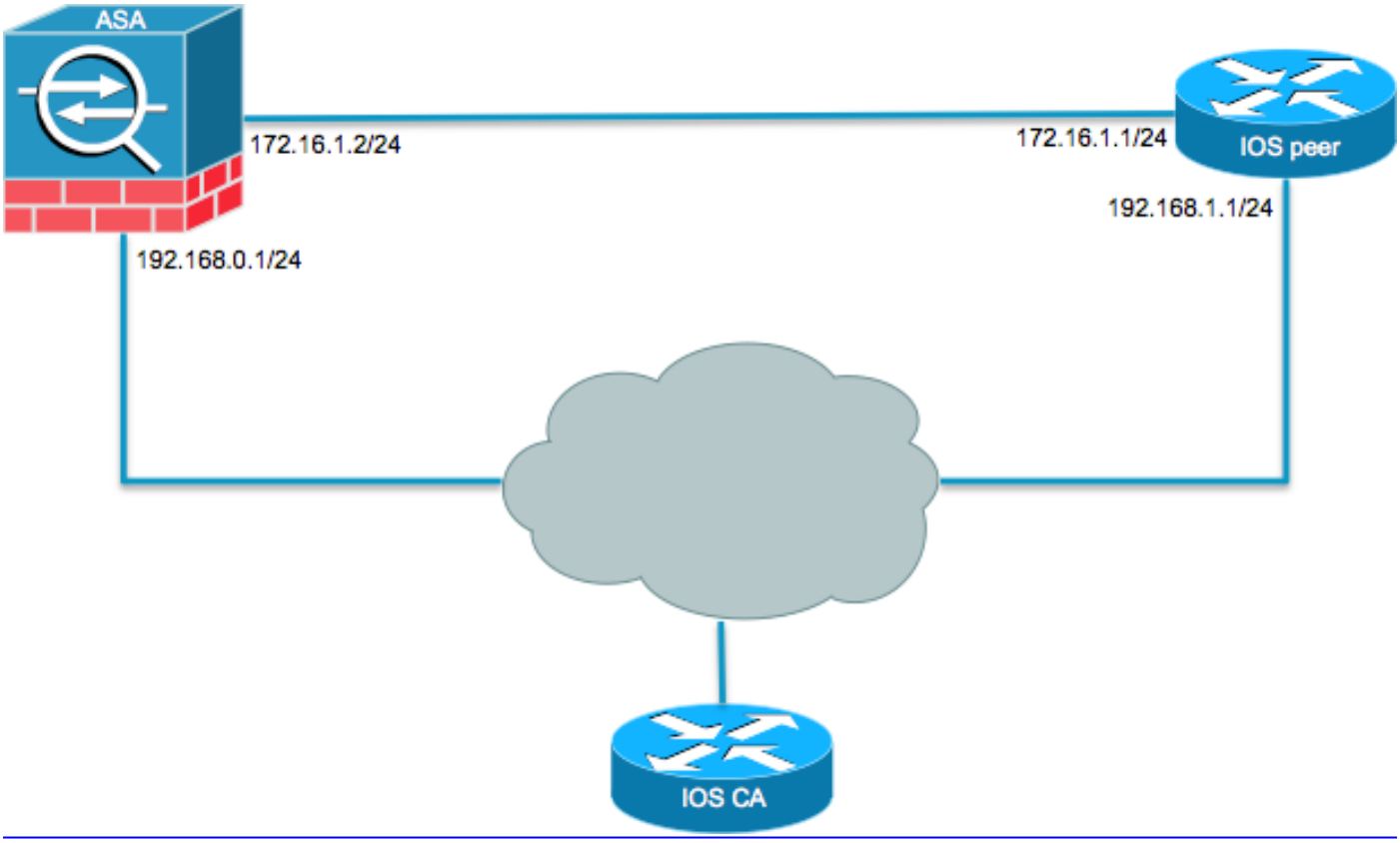
### Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Cisco ASA qui exécute la version de logiciel 8.4(1) ou plus tard
- La génération 2 (G2) de Cisco ISR cette exécute la version de logiciel 15.2(4)M de Cisco IOS ou plus tard
- Routeurs à services d'agrégation de la gamme Cisco ASR 1000 cette version 15.2(4)S ou ultérieures de Logiciel Cisco IOS XE version 2 de passage
- Routeurs Connected Grid de Cisco qui exécutent la version de logiciel 15.2(4)M ou plus tard

## Configurez

### Diagramme du réseau



## Informations générales

La configuration d'un tunnel IKEv2 entre une ASA et un routeur avec l'utilisation des clés pré-partagées est simple. Cependant, quand vous utilisez l'authentification de certificat, il y a certaines mises en garde à maintenir dans l'esprit.

### NTP

L'authentification de certificat exige que les horloges sur tous les périphériques participants soient synchronisées à une source commune. Tandis que l'horloge peut être réglée manuellement sur chaque périphérique, ce n'est pas très précise et peut être encombrante. La méthode facile pour synchroniser les horloges sur tous les périphériques est d'utiliser le NTP. Le NTP synchronise la ponctualité parmi un ensemble de Serveurs de synchronisation et de clients distribués. Cette synchronisation permet des événements à corréler quand des logs système sont créés et quand d'autres événements de temps-particularité se produisent. Pour plus d'informations sur la façon configurer le NTP, référez-vous au Network Time Protocol : Livre Blanc de pratiques recommandées.

> **Conseil** : Quand un serveur d'Autorité de certification (CA) de logiciel de Cisco IOS est utilisé, il est dans pratique commune de configurer le même périphérique que le ntp master. Dans cet exemple, le serveur CA sert également de serveur de NTP.

### Consultation basée sur HTTP de certificat

La consultation de certificat basée sur l'URL HTTP évite la fragmentation cette des résultats quand de grands Certificats sont transférés. Cette caractéristique est activée sur des périphériques de logiciel Cisco IOS par défaut, ainsi le type 12 de req de CERT est utilisé par le logiciel de Cisco IOS.

Si des versions de logiciel qui n'ont pas la difficulté pour l'ID de bogue Cisco CSCul48246 sont utilisées sur l'ASA, alors la consultation basée sur HTTP n'est pas négociée sur l'ASA, et le logiciel de Cisco IOS entraîne la tentative d'autorisation d'échouer.

Sur l'ASA, si le protocole IKEv2 met au point sont activés, ces messages apparaissent :

Afin d'éviter cette question, n'employez l'**aucune crypto** commande de **CERT HTTP-URL ikev2** afin de désactiver cette configuration sur le routeur quand elle scrute avec une ASA.

### Validation d'ID de pair

Pendant des négociations AUTHENTIQUES de Protocole ISAKMP (Internet Security Association and Key Management Protocol) d'étape d'IKE, les pairs doivent s'identifier entre eux. Cependant, il y a une différence dans les Routeurs de manière et les ASA sélectionnent leur identité locale.

#### Sélection d'ID d'ISAKMP sur des Routeurs

Quand les tunnels IKEv2 sont utilisés sur des Routeurs, l'identité locale utilisée dans la négociation est déterminée par la commande **locale d'identité** sous le profil IKEv2 :

Par défaut, le routeur utilise l'adresse comme identité locale.

#### Validation d'ID d'ISAKMP sur des Routeurs

L'ID prévu de pair est également configuré manuellement dans le même profil avec la **remote command de match identity** :

#### Sélection d'ID d'ISAKMP sur des ASA

Sur des ASA, l'identité d'ISAKMP est sélectionnée globalement avec la commande de **crypto isakmp identity** :

Par défaut, le mode de commande est placé à l'automatique, ainsi il signifie que l'ASA détermine la négociation ISAKMP par le type de connexion :

- Adresse IP pour la clé pré-partagée.
- Nom unique de CERT pour l'authentification de certificat.

  Remarque: L'ID de bogue Cisco CSCul48099 est une demande d'amélioration pour que la capacité configure sur une base de par-tunnel-groupe plutôt qu'en configuration globale.

#### Validation d'ID d'ISAKMP sur l'ASA

La validation distante d'ID est faite automatiquement (déterminé par le type de connexion) et ne peut pas être changée. La validation peut être activée ou désactivée sur une base de par-tunnel-groupe avec la commande de pair-id-**validation** :

#### Problèmes d'interopérabilité

La différence dans des causes de sélection/validation d'ID deux problèmes d'interopérabilité distincts :

1. Quand le CERT authentique est utilisé sur l'ASA, les essais ASA pour valider l'ID de pair du nom alternatif soumis (SAN) sur le certificat reçu. Si la validation d'ID de pair est activée et si la plate-forme IKEv2 met au point sont activées sur l'ASA, ceux-ci met au point apparaissent :
   Pour cette question, ou l'adresse IP du certificat doit être incluse dans le certificat du pair, ou la validation d'ID de pair doit être désactivée sur l'ASA.
2. De même, par défaut l'ASA sélectionne l'ID local automatiquement ainsi, quand le CERT authentique est utilisé, qu'il envoie le nom unique (DN) comme identité. Si le routeur est configuré pour recevoir l'adresse comme ID distant, la validation d'ID de pair échoue sur le routeur. Si IKEv2 met au point est activé sur le routeur, ceux-ci met au point apparaît :
   Pour cette question, configurez le routeur afin de valider le nom de domaine complet (FQDN) ou configurer l'ASA afin d'utiliser l'adresse comme ID d'ISAKMP.Remarque: Sur le routeur, une carte de certificat qui est reliée au profil IKEv2 doit être configurée afin d'identifier le DN. Référez-vous au certificat à la section de mappage de profil d'ISAKMP de l'*échange de clés Internet (IKE) pour le guide de configuration d'IPsec VPN,* document Cisco de la *release 3S de Cisco IOS XE* pour des informations sur la façon établir ceci.

### Taille de la charge utile authentique

Si des Certificats (plutôt que des clés pré-partagées) sont utilisés pour l'authentification, les charges utiles authentiques sont considérablement plus grandes. Ceci a habituellement comme conséquence la fragmentation, qui peut alors faire échouer l'authentification si un fragment est perdu ou abandonné dans le chemin. Si le tunnel ne monte pas en raison de la taille de la charge utile authentique, les causes habituelles sont :

1. Contrôlez le plan maintenant l'ordre sur le routeur qui pourrait bloquer les paquets.
2. Négociation maximum incorrecte d'unité de transition (MTU), qui peut être corrigée avec la **crypto** commande de *taille de* **mtu de la fragmentation ikev2**.

### Allocation de ressources en mode de Multi-contexte sur l'ASA

En date de la version 9.0 ASA, l'ASA prend en charge un VPN en mode de multi-contexte. Cependant, quand vous configurez le VPN en mode de multi-contexte, soyez sûr d'allouer les ressources appropriées dans le système qui utilisera le VPN.

Le pour en savoir plus, se rapportent aux informations sur la section de gestion des ressources du guide de configuration CLI de gamme de Cisco ASA, 9.0.

### Validation de la liste des révocations de certificat

Un Liste des révocations de certificat (CRL) est une liste de certi retiré ? cates qui ont été émis et ultérieurement retirés par un CA donné Certi ? des cates pourraient être retirés pour un certain nombre de raisons comme :

- Panne ou compromission d'un périphérique qui utilise un certificat donné.
- Compromission de la paire de clés utilisée par un certi ? cate.
- Erreurs dans un certi émis ? cate, tel qu'une identité incorrecte ou la nécessité de faciliter un changement de nom.

Le mécanisme utilisé pour le certi ? la révocation de cate dépend du certi retiré par CA ? des cates sont représentés dans le CRL par leurs numéros de série. Si tentatives d'un périphérique de réseau de vérifier la validité d'un certi ? cate, il télécharge et balaye le courant CRL pour le numéro de série du certificat présenté. Par conséquent, si la validation CRL est activée sur l'un ou l'autre de pair, un URL CRL approprié doit être aussi bien configuré ainsi la validité des Certificats d'ID peut être vérifiée.

Pour plus d'informations sur CRL, référez-vous au ce qui est une section CRL du guide de configuration d'infrastructure de clé publique, la release 3S de Cisco IOS XE.

### Validation de la chaîne de certificat

Si l'ASA est configurée avec un certificat qui a l'intermédiaire CAs et il est pair pourrait ou ne pourrait pas avoir la même intermédiaire CA, alors l'ASA doit être explicitement configurée pour envoyer la chaîne de certificat complète au routeur. Le routeur fait ceci par défaut. Afin de faire ceci, quand vous définissez le point de confiance sous le crypto map ajoutent le mot clé à chaînes comme affiché ici :

Si ceci n'est pas fait, alors le le tunnel obtiendra seulement négocié tant que l'ASA est le

responder. Si c'est un demandeur, le tunnel échouera et le PKI et l'IKEv2 met au point sur le routeur afficheront ceci :

### Configuration de l'échantillon ASA

### Configuration de routeur d'échantillon

### Configuration IOS CA témoin

## Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Ces commandes travaillent aux ASA et aux Routeurs :

- **affichez cryptos ikev2 SA** - Affiche l'état de l'association de sécurité de la phase 1 (SA).
- **show crypto ipsec sa** - Affiche l'état de SA de la phase 2.

> Remarque: Dans cette sortie, à la différence de dans IKEv1, les affichages parfaits de valeur de groupe de Protocole DH (Diffie-Hellman) de secret d'expédition (PFS) en tant que « PFS (Y/N) : N, groupe CAD : aucun » pendant la première négociation de tunnel ; après qu'un rekey se produise, les valeurs correctes apparaissent. Ce n'est pas une bogue quoique le comportement soit décrit dans l'ID de bogue Cisco CSCug67056.
>
> La différence entre IKEv1 et IKEv2 est que, dans IKEv2, l'enfant SAS sont créés en tant qu'élément de l'échange AUTHENTIQUE lui-même. Le groupe configuré CAD sous le crypto map est utilisé seulement pendant un rekey. Ainsi, vous voyez le « PFS (Y/N) : N, groupe CAD : aucun » jusqu'au premier rekey. Avec IKEv1, vous voyez un comportement différent parce que la création d'enfant SA se produit pendant le mode rapide, et le message CREATE_CHILD_SA a la disposition de porter la charge utile de Key Exchange, qui spécifie les paramètres CAD pour dériver le nouveau secret partagé.

### Vérification de Phase 1

Cette procédure vérifie l'activité de la phase 1 :

1. Sélectionnez la **crypto** commande d'**ikev2 SA d'exposition** sur le routeur :
2. Écrivez le **crypto sacommand ikev2 d'exposition** sur l'ASA :

### Vérification de Phase 2

Cette procédure décrit comment vérifier si l'index de paramètre de Sécurité (SPI) a été négocié

correctement sur les deux pairs :

1. Entrez dans le **show crypto ipsec sa |** commande du **spi i** sur le routeur :
2. Entrez dans le **show crypto ipsec sa | spicommand i** sur l'ASA :

Cette procédure décrit comment confirmer si la circulation à travers le tunnel :

1. Entrez dans le **show crypto ipsec sa |** commande des **paquets i** sur le routeur :
2. Entrez dans le **show crypto ipsec sa | pktscommand i** sur l'ASA :

# Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

## Debugs sur l'ASA

> **Attention** : Sur l'ASA, vous pouvez placer divers mettez au point des niveaux ; par défaut, le niveau 1 est utilisé. Si vous changez le niveau de débogage, la verbosité du met au point pourrait augmenter. Faites ceci avec prudence, particulièrement dans les environnements de production !

L'ASA met au point pour la négociation de tunnel sont :

- **protocole du debug crypto ikev2**
- **plate-forme du debug crypto ikev2**

L'ASA mettent au point pour l'authentification de certificat est :

- **debug crypto Ca**

## Debugs sur le routeur

Le routeur met au point pour la négociation de tunnel sont :

- **debug crypto ikev2**
- **erreur du debug crypto ikev2**
- **debug crypto ikev2 interne**

Le routeur met au point pour l'authentification de certificat sont :

- **mettez au point la validation de PKI de cri**
- **mettez au point la transaction de PKI de cri**
- **mettez au point les messages de PKI de cri**