# VPN IPsec d'accès à distance



# Présentation des VPN d'accès à distance IPsec

Les VPN d'accès à distance permettent aux utilisateurs de se connecter à un site central par le biais d'une connexion sécurisée sur un réseau TCP/IP. Le protocole Internet Security Association and Key Management, également appelé IKE, est le protocole de négociation qui permet au client IPsec sur le PC distant et l'ASA de convenir de la manière de créer une association de sécurité IPsec. Chaque négociation ISAKMP est divisée en deux sections appelées Phase 1 et Phase 2.

La Phase 1 crée le premier tunnel pour protéger les messages de négociation ISAKMP ultérieurs. La Phase 2 crée le tunnel qui protège les données circulant sur la connexion sécurisée.

Pour définir les termes des négociations ISAKMP, vous créez une politique ISAKMP. Elle comprend les éléments suivants :

- Une méthode d'authentification pour garantir l'identité des homologues.
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour définir la taille de la clé de chiffrement.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Un ensemble de transformation combine une méthode de chiffrement et une méthode d'authentification. Lors de la négociation de l'association de sécurité IPsec avec ISAKMP, les pairs conviennent d'utiliser un ensemble de transformation particulier pour protéger un flux de données particulier. L'ensemble de transformation doit être le même pour les deux homologues.

Un ensemble de transformation protège les flux de données pour l'ACL spécifiée dans l'entrée de carte de chiffrement associée. Vous pouvez créer des ensembles de transformation dans la configuration ASA, puis spécifier un maximum de 11 d'entre eux dans une carte de chiffrement ou une entrée de carte de chiffrement dynamique. Pour obtenir plus de renseignements, y compris un tableau qui répertorie les méthodes de chiffrement et d'authentification valides, consultez Créer un ensemble de transformation IKEv1 ou une proposition IKEv2, à la page 6.

Vous pouvez configurer l'ASA pour attribuer une adresse IPv4, une adresse IPv6 ou à la fois une adresse IPv4 et une adresse IPv6 à Secure Client (services client sécurisés) en créant des regroupements internes d'adresses sur l'ASA ou en attribuant une adresse dédiée à un utilisateur local sur l'ASA.

Le point terminal doit être doté du protocole à double pile dans son système d'exploitation pour attribuer les deux types d'adresses. Dans les deux scénarios, lorsqu'il n'y a plus d'ensembles d'adresses IPv6 mais que les adresses IPv4 sont disponibles ou lorsqu'il n'y a plus d'ensembles d'adresses IPv4 mais que les adresses IPv6 sont disponibles, la connexion se produit toujours. Le client n'est pas informé ; cependant, l'administrateur doit consulter les journaux ASA pour obtenir les détails.

L'attribution d'une adresse IPv6 au client est prise en charge pour le protocole SSL.

# À propos des VPN Mobike et d'accès à distance

Mobile IKEv2 (mobike) étend les VPN d'accès à distance ASA pour prendre en charge l'itinérance des périphériques portables. Cette prise en charge signifie que l'adresse IP de point terminal de l'association de sécurité IKE/IPSEC d'un périphérique portable peut être mise à jour plutôt que d'être supprimée lorsque le périphérique passe de son point de connexion actuel à un autre.

Mobike est disponible par défaut sur les ASAs depuis la version 9.8(1), ce qui signifie que Mobike est « toujours activé ». Mobike est activé pour chaque SA uniquement lorsque le client le propose et que l'ASA l'accepte. Cette négociation se produit dans le cadre de l'échange IKE_AUTH.

Une fois la SA établie avec la prise en charge de mobike activée, le client peut modifier son adresse à tout moment et notifier l'ASA à l'aide de l'échange INFORMATIONAL avec la charge utile UPDATE_SA_ADDRESS indiquant la nouvelle adresse. L'ASA traitera ce message et mettra à jour la SA avec la nouvelle adresse IP du client.

**Remarque** Vous pouvez utiliser la commande `show crypto ikev2 sa detail` pour déterminer si mobike est activé pour tous les SA actuels.

L'implémentation actuelle de Mobike prend en charge les éléments suivants :

- Adresses IPv4 :
- Modifications des mappages NAT
- Connectivité du chemin et détection des pannes au moyen de la vérification facultative de la route de retour
- Basculement actif/de secours

- Équilibrage de la charge VPN

Si la fonction de vérification de retour de routage (RRC) est activée, un message RRC est envoyé au client mobile pour confirmer la nouvelle adresse IP avant la mise à jour de la SA.

# Exigences de licence pour le module AnyConnect VPN de Cisco Secure Client

**Remarque** Cette fonctionnalité n'est pas disponible dans les modèles sans chiffrement de charge utile.

Si vous souhaitez déployer Cisco Secure Client (y compris AnyConnect) à partir d'une tête de réseau Secure Firewall ASA et utiliser les modules VPN et Secure Firewall Posture ou HostScan, une licence Advantage ou Premier est requise. Des licences d'essai sont disponibles. Consultez le guide de commande Cisco Secure Client. Consultez les licences pour fonctionnalités de la gamme Cisco ASA pour connaître les valeurs maximales par modèle.

# Restrictions pour le VPN IPsec d'accès à distance

- Directives relatives au mode pare-feu : prises en charge uniquement en mode de pare-feu routé. Le mode transparent n'est pas pris en charge.
- Directives de basculement : les sessions VPN IPsec sont répliquées uniquement dans les configurations de basculement actif/veille. Les configurations de basculement actif/actif ne sont pas prises en charge.
- Les modifications de configuration sont bloquées pendant la synchronisation à haute disponibilité. Si un utilisateur tente de se connecter pendant ce temps, l'installation de la règle DACL dans le pare-feu peut échouer. Une fois la synchronisation HA terminée, l'utilisateur peut se connecter avec succès.
- L'ASA n'accepte pas les sessions VPN d'accès à distance si le client tiers envoie un agent utilisateur nul.
- L'utilisation de listes de contrôle d'accès (ACL) de nom de domaine complet (FQDN) pour un domaine qui se résout en plusieurs adresses IP qui changent fréquemment peut avoir une incidence sur la résolution des adresses DHCP dans un environnement VPN d'accès à distance. Ce problème peut se produire si un serveur DHCP externe est configuré et qu'une validation transactionnelle pour la traduction d'adresses réseau (NAT) est activée.
- L'évaluation de la posture à l'aide d'Advanced Endpoint Assessment peut entraîner des messages syslog de connexion SSL qui ne sont pas associés à un événement de connexion ou de déconnexion VPN.
- L'authentification locale n'est pas possible, car l'ASA ne termine aucune méthode EAP.

  L'ASA prend en charge EAP uniquement en relais et exige l'authentification par certificat pour les clients VPN dans le cadre de l'authentification EAP des clients. Lorsque vous configurez le protocole EAP comme méthode d'authentification à distance, veillez à configurer l'authentification par certificat pour les clients VPN. Des erreurs s'affichent même si plusieurs méthodes d'authentification à distance, telles que EAP, PSK ou des certificats, sont configurées avec EAP.

# Configurer les VPN d'accès à distance IPsec

Cette section décrit comment configurer les VPN d'accès à distance.

## Configurer une interface

Un ASA comporte au moins deux interfaces, appelées ici outside et inside. En règle générale, l'interface externe est connectée à l'Internet public, tandis que l'interface interne est connectée à un réseau privé et est protégée contre tout accès public.

Pour commencer, configurez et activez deux interfaces sur l'ASA. Attribuez ensuite un nom, une adresse IP et un masque de sous-réseau. Vous pouvez également configurer son niveau de sécurité, sa vitesse et son fonctionnement en duplex sur l'appareil de sécurité.

### Procédure

**Étape 1** Entrez le mode de configuration d'interface à partir du mode de configuration globale :

**interface** {*interface*}

**Exemple :**

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

**Étape 2** Définissez l'adresse IP et le masque de sous-réseau pour l'interface :

**ip address** *ip_address* [*mask*] [*standby ip_address*]

**Exemple :**

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

**Étape 3** Spécifiez un nom pour l'interface (maximum 48 caractères). Vous ne pourrez pas modifier ce nom ultérieurement.

**nameif** *nom*

**Exemple :**

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

**Étape 4** Activez l'interface. Par défaut, les interfaces sont désactivées.

**Exemple :**

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

# Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe

**Procédure**

**Étape 1** Précisez la méthode d'authentification et l'ensemble de paramètres à utiliser lors de la négociation IKEv1.

La priorité identifie de manière unique la politique Internet Key Exchange (IKE) et lui attribue une priorité. Utilisez un entier de 1 à 65 534, 1 étant la priorité la plus élevée et 65 534 la priorité la plus basse.

Dans les étapes qui suivent, nous définissons la priorité à 1.

**Étape 2** Précisez la méthode de chiffrement à utiliser dans une politique IKE :

**crypto ikev1 policy** *priority* **encryption** {**aes-192** | **aes-256** | | }

**Exemple :**

**Étape 3** Précisez l'algorithme de hachage d'une politique IKE (également appelé variante HMAC) :

**crypto ikev1 policy** *priority* **hash** { | **sha**}

**Exemple :**

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

**Étape 4** Précisez le groupe Diffie-Hellman pour la politique IKE, le protocole cryptographique qui permet au client IPsec et à l'ASA d'établir une clé secrète partagée :

**crypto ikev1 policy** *priority* **group** {**14** | | | **19** | **20** | 21}

**Exemple :**

```
hostname(config)#crypto ikev1 policy 1 group 14
hostname(config)#
```

**Étape 5** Précisez la durée de vie de la clé de chiffrement : le nombre de secondes que chaque association de sécurité doit exister avant d'expirer :

**crypto ikev1 policy** *priority* **lifetime** {*seconds*}

La plage est comprise entre 120 et 2 147 483 647 secondes. Utilisez 0 seconde pour une durée de vie infinie.

**Exemple :**

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

**Étape 6** Activez ISAKMP sur l'interface nommée à l'extérieur :

**crypto ikev1 enable** *interface-name*

**Exemple :**

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

**Étape 7** Enregistrez les modifications de configuration :

**write memory**

# Configurer un ensemble d'adresses

L'ASA nécessite une méthode pour attribuer des adresses IP aux utilisateurs. Cette section utilise les ensembles d'adresses comme exemple.

### Procédure

Créez un ensemble d'adresses avec une plage d'adresses IP, à partir de laquelle l'ASA att

**ip local pool** *poolname first-address—last-address* [**mask** *mask*]

Le masque d'adresse est facultatif. Cependant, vous devez fournir la valeur de masque lorsque les adresses IP attribuées aux clients VPN appartiennent à un réseau non standard et que les données peuvent être acheminées incorrectement si vous utilisez le masque par défaut. Un exemple typique est lorsque l'ensemble local d'adresses IP contient 10.10.10.0/255.255.255.0, car il s'agit d'un réseau de classe A par défaut. Cela peut entraîner des problèmes de routage lorsque le client VPN doit accéder à différents sous-réseaux du réseau 10 sur différentes interfaces.

**Exemple :**

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

# Ajouter un utilisateur

### Procédure

Créez un utilisateur, un mot de passe et un niveau de privilège pour l'utilisateur :

**username** *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

**Exemple :**

```
Hostname(config)# username testuser password 12345678
```

# Créer un ensemble de transformation IKEv1 ou une proposition IKEv2

Cette section montre comment configurer un ensemble de transformation (IKEv1) ou une proposition (IKEv2), qui combine une méthode de chiffrement et une méthode d'authentification.

Les étapes suivantes montrent comment créer une proposition IKEv1 et IKEv2.

### Procédure

**Étape 1** Configurez un ensemble de transformation IKEv1 qui spécifie les algorithmes de chiffrement et de hachage IKEv1 d'IPsec à utiliser pour assurer l'intégrité des données.

**crypto ipsec ikev1 transform-set** *transform-set-name (nom d'ensemble de transformation) encryption-method (méthode de chiffrement)* [*authentication*]

Utilisez l'une des valeurs suivantes pour le chiffrement :

- esp-aes pour utiliser AES avec une clé de 128 bits.
- esp-aes-192 pour utiliser AES avec une clé de 192 bits.
- esp-aes-256 pour utiliser AES avec une clé de 256 bits.
- esp-null pour ne pas utiliser le chiffrement.

Utilisez l'une des valeurs suivantes pour l'authentification :

- esp-md5-hmac pour utiliser MD5/HMAC-128 comme algorithme de hachage.
- esp-sha-hmac pour utiliser SHA/HMAC-160 comme algorithme de hachage.
- esp-none pour ne pas utiliser l'authentification HMAC.

**Exemple :**

Pour configurer un ensemble de transformation IKEv1 à l'aide d'AES :

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

**Étape 2** Configurez un ensemble de propositions IKEv2 qui spécifie le protocole IPsec IKEv2 et les algorithmes de chiffrement et d'intégrité à utiliser.

esp spécifie le protocole IPsec d'Encapsulating Security Payload (ESP) (actuellement le seul protocole pris en charge pour IPsec).

**crypto ipsec ikev2 ipsec-proposal** *proposal_name*

**protocol** {**esp**} {**encryption** { | | **aes** | **aes-192** | **aes-256** | } | **integrity** { | **sha-1**}

Utilisez l'une des valeurs suivantes pour le chiffrement :

- aes pour utiliser AES (par défaut) avec un chiffrement de clé de 128 bits pour ESP.
- aes-192 pour utiliser AES avec un chiffrement de clé de 192 bits pour ESP.
- aes-256 pour utiliser AES avec un chiffrement de clé de 256 bits pour ESP.

Utilisez l'une des valeurs suivantes pour l'intégrité :

- sha-1 (par défaut) spécifie l'algorithme de hachage sécurisé (SHA) SHA-1, défini dans la norme FIPS (Federal Information Processing Standard) des États-Unis, pour la protection de l'intégrité d'ESP.

Pour configurer une proposition IKEv2 :

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal
```

```
hostname(config-ipsec-proposal)# protocol esp encryption aes intergrity sha-1
```

# Définir un groupe de tunnels

Un groupe de tunnels est un ensemble de politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Il existe deux groupes de tunnels par défaut dans le système ASA : DefaultRAGroup, qui est le groupe de tunnels d'accès à distance par défaut, et DefaultL2Lgroup, qui est le groupe de tunnels par défaut de LAN à LAN. Vous pouvez modifier ces groupes, mais pas les supprimer. L'ASA utilise ces groupes pour configurer les paramètres de tunnel par défaut pour les groupes de tunnels d'accès à distance et de réseau local (LAN) lorsqu'aucun groupe de tunnels spécifique n'est identifié lors de la négociation du tunnel.

### Procédure

**Étape 1** Créez un groupe de tunnels d'accès à distance IPsec (également appelé profil de connexion) :

**tunnel-group** *name* **type** *type*

**Exemple :**

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

**Étape 2** Entrez le mode d'attributs généraux du groupe de tunnels où vous pouvez saisir une méthode d'authentification :

**tunnel-group** *name* **general-attributes**

**Exemple :**

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```

**Étape 3** Précisez un ensemble d'adresses à utiliser pour le groupe de tunnels :

**address-pool** [*(nom de l'interface)*] *address_pool1* [*...address_pool6*]

**Exemple :**

```
hostname(config-general)# address-pool testpool
```

**Étape 4** Entrez en mode d'attributs IPsec de groupe de tunnels où vous pouvez entrer des attributs spécifiques à IPsec pour les connexions IKEv1 :

**tunnel-group** *name* **ipsec-attributes**

**Exemple :**

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

**Étape 5** (Facultatif) Configurez une clé prépartagée (IKEv1 uniquement). La clé peut comporter entre 1 et 128 caractères alphanumériques.

Les clés de l'appareil de sécurité adaptatif et du client doivent être identiques. Si un client VPN Cisco avec une clé prépartagée de taille différente tente de se connecter, le client consigne un message d'erreur indiquant qu'il n'a pas réussi à authentifier l'homologue.

**ikev1 pre-shared-key** *key*

**Exemple :**

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

# Créer une carte de chiffrement dynamique

Les cartes de chiffrement dynamiques définissent des modèles de politique dans lesquels tous les paramètres ne sont pas configurés. Cela permet à l'ASA de recevoir des connexions d'homologues qui ont des adresses IP inconnues, comme les clients d'accès à distance.

Les entrées de carte de chiffrement dynamique identifient l'ensemble de transformation pour la connexion. Vous pouvez également activer le routage inverse, ce qui permet à l'ASA d'apprendre les informations de routage pour les clients connectés et de les annoncer via RIP ou OSPF.

## Procédure

**Étape 1** Créez une carte de chiffrement dynamique et spécifiez un ensemble de transformation IKEv1 ou une proposition IKEv2 pour la carte :

- Pour IKEv1, utilisez cette commande :

  **crypto dynamic-map** *dynamic-map-name seq-num* **set ikev1 transform-set** *transform-set-name*

- Pour IKEv2, utilisez cette commande :

  **crypto dynamic-map** *dynamic-map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name*

**Exemple :**

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#

hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

**Étape 2** (Facultatif) Activez l'injection de route inverse pour toute connexion basée sur cette entrée de carte de chiffrement :

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set reverse-route**

**Exemple :**

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

# Créer une entrée de carte de chiffrement pour utiliser la carte de chiffrement dynamique

Créez une entrée de carte de chiffrement qui permet à l'ASA d'utiliser la carte de chiffrement dynamique pour définir les paramètres des associations de sécurité IPsec.

Dans les exemples suivants pour cette commande, le nom de la carte de chiffrement est mymap, le numéro de séquence est 1 et le nom de la carte de chiffrement dynamique est dyn1, que vous avez créée dans la rubrique Créer une carte de chiffrement dynamique.

**Procédure**

**Étape 1** Créez une entrée de carte de chiffrement qui utilise une carte de chiffrement dynamique :

**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

**Exemple :**

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

**Étape 2** Appliquez la carte de chiffrement à l'interface externe :

**crypto map** *map-name* **interface** *interface-name*

**Exemple :**

```
hostname(config)# crypto map mymap interface outside
```

**Étape 3** Enregistrez les modifications dans la configuration :

**write memory**

# Configurer un VPN d'accès à distance IPSec IKEv2 en mode multicontexte

Pour plus d'informations sur la configuration des VPN d'accès à distance IPsec, consultez les sections suivantes :

# Authentification VPN à l'aide de clés prépartagées post-quantiques

Vous pouvez configurer IKEv2 avec une nouvelle clé, une clé prépartagée (PPK) post-quantique, ainsi que des clés prépartagées (PSK) pour sécuriser la communication IPsec entre Secure Client et un ASA contre les attaques d'ordinateurs quantiques. Vous devez configurer des ensembles correspondants de PPK et de PSK sur le client et l'ASA pour une connexion IPsec sécurisée. Secure Client et ASA utilisent les clés PPK et PSK pour obtenir les clés de chiffrement et de déchiffrement du trafic réseau.

Les PPK sont générés par chiffrement au format binaire. Pour les configurations ASA et Secure Client, vous devez convertir le PPK binaire en une chaîne hexadécimale de 256 bits et de 64 caractères.

## Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

- Licence : l'ASA doit disposer d'une licence de cryptage renforcé
- Versions prises en charge
  - ASA Version 9.18.1 et ultérieures
  - Secure Client Version 5.1.8.x et ultérieures
- Configurez tous les autres paramètres sur l'ASA pour la connexion VPN d'accès à distance IPsec/IKEv2, comme l'ensemble d'adresses, la proposition IKEv2 et la carte de chiffrement
- Générez le PPK binaire.
- Convertissez le PPK binaire en chaîne hexadécimale de 64 caractères sur 256 bits.
- Configurez à la fois le PPK et les deux PSK pour Secure Client dans le Windows Credential Manager (WCM) de votre machine cliente. Consultez, Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager, à la page 13.
- Configurez les attributs PPK dans le profil VPN de Secure Client. Consultez, Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique, à la page 14.
- Assurez-vous que les valeurs PPK et PPK ID sont identiques sur l'ASA et dans Secure Client.

## Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

### Directives

- L'administrateur doit assurer la génération, la qualité et la distribution des PPK et des PSK sur chaque périphérique client.

### Restrictions

- Prend en charge uniquement IKEv2 avec PSK et PPK.
- Prend en charge uniquement Windows pour Secure Client.
- Le client ne peut stocker les informations d'authentification que pour un seul ASA dans WCM.

# Flux de travail pour l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

*Tableau 1 : Flux de travail pour l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN*

| Étape | Action | Autres renseignements |
|---|---|---|
| 1 | Générez le PPK binaire et convertissez-le en une chaîne hexadécimale de 256 bits et 64 caractères. | - |
| 2 | Configurez le PPK et le PSK dans le gestionnaire d'informations d'authentification Windows (WCM). | Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager, à la page 13 |
| 3 | Configurez le profil VPN de Secure Client avec les paramètres PPK. | Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique, à la page 14 |
| 4 | Configurez le groupe de tunnels de l'ASA. | Configurer l'authentification VPN sur ASA à l'aide de clés prépartagées post-quantiques, à la page 14 |
| 5 | L'utilisateur ouvre une session dans Secure Client pour se connecter à l'ASA. | - |
| 6 | Secure Client utilise le PPK_ID dans le profil VPN pour récupérer le PPK et deux PSK à partir du WCM. | - |
| 7 | Secure Client vérifie les paramètres PPK et PSK du WCM par rapport aux paramètres du groupe de tunnels de l'ASA. | - |
| 8 | Secure Client établit une connexion VPN avec l'ASA si les PPK et les PSK de Secure Client et de l'ASA correspondent.<br>La connexion VPN avec l'ASA échoue si les PPK et PSK ne correspondent pas. | - |

# Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager

Vous devez configurer des entrées d'informations d'authentification distinctes pour un PPK, un PSK local et un PSK distant.

### Avant de commencer

Assurez-vous d'avoir consulté Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN, à la page 11 et Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN, à la page 11.

### Procédure

**Étape 1** Sur votre ordinateur client Windows, choisissez **Control Panel (Panneau de configuration) > User Accounts (Comptes d'utilisateurs) > Credential Manager (Gestionnaire d'informations d'authentification)**.

**Étape 2** Cliquez sur l'onglet **Windows Credentials** (Informations d'authentification Windows).

**Étape 3** Cliquez sur **Add a Generic Credential** (Ajouter une information d'identification générique).

**Étape 4** Dans le champ **Internet or network address** (Adresse Internet ou réseau), spécifiez l'une des valeurs suivantes :

- Pour un PPK, spécifiez la valeur suivante : **AC/PPK/**<HostAddress> : une clé prépartagée post-quantique. Il est stocké sous forme de 64 caractères hexadécimaux dans WCM et le client le convertit en binaire, puis inclut la clé dans la dérivation des clés de chiffrement et de déchiffrement dans IKEv2.
- Pour une clé PSK locale, spécifiez la valeur suivante : **AC/PSK_Local/**<HostAddress> : PSK du client.
- Pour une clé PSK distante, spécifiez la valeur suivante : **AC/PSK_Remote/**<HostAddress> : PSK de l'ASA.

**Étape 5** Dans le champ **User name (Nom d'utilisateur)**, spécifiez la valeur **n/a**, car elle n'est pas utilisée par Secure Client.

**Étape 6** Dans le champ **Password** (Mot de passe), spécifiez l'une des valeurs suivantes :

- Pour un PPK, spécifiez une chaîne hexadécimale de 64 caractères de 256 bits.
- Pour un PSK local et distant, spécifiez une chaîne qui définit l'alias du groupe de tunnels.

**Étape 7** Cliquez sur **OK**.

Lorsque le client et l'ASA sont correctement configurés, le client utilise le PPK_ID dans le profil VPN pour récupérer le PPK et les deux PSK à partir de WCM. Secure Client utilise les valeurs PPK et PSK ci-dessus, convertit le PPK en binaire, fait correspondre les valeurs PPK et PSK avec la configuration de l'ASA, puis effectue l'authentification VPN. Aucune autre entrée n'est requise pour l'établissement de la connexion VPN, car ces trois clés sont les informations d'authentification.

# Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique

Le paramètre **HostEntry** dans le profil VPN comprend les nouveaux champs suivants pour configurer les paramètres PPK pour Secure Client :

- **IKEIdentity** : spécifiez une chaîne pour identifier l'ASA homologue. Cette chaîne doit correspondre au nom du groupe de tunnels dans l'ASA.
- **PPK_ID** : spécifiez une chaîne unique pour identifier le PPK. Cette valeur doit correspondre à l'ID PPK dans l'ASA.
- **PPK_mandatory** : spécifiez la valeur « true » si le PPK est obligatoire pour la connexion VPN. Si vous ne configurez pas cette valeur, la configuration PPK sera facultative.

### Exemple

Un exemple d'entrée d'hôte dans le profil VPN est donné ci-dessous :

```
<HostEntry>
<HostName> ASAv_PPK</HostName>
<HostAddress>192.168.1.2</HostAddress>
<UserGroup>IPSec_Profile</UserGroup>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true</StandardAuthenticationOnly>
 <IKEIdentity>secure_client_PPK</IKEIdentity>
 <PPK_ID>PPKID_test</PPK_ID>
</PrimaryProtocol>
</HostEntry>
```

# Configurer l'authentification VPN sur ASA à l'aide de clés prépartagées post-quantiques

Les groupes de tunnels sur l'ASA identifient la stratégie de groupe d'une connexion VPN. Vous pouvez configurer la stratégie du groupe de tunnels pour activer l'authentification VPN à l'aide de PPK et de PSK.

### Avant de commencer

Assurez-vous d'avoir consulté Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN, à la page 11 et Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN, à la page 11.

### Procédure

**Étape 1** Configurez les attributs IPsec du groupe de tunnels.

**tunnel-group** *name* **ipsec-attributes**

**Exemple :**

```
hostname(config)# tunnel-group secure_client_PPK ipsec-attributes
hostname(config-tunnel-ipsec)#
```

**Étape 2** Configurez le PSK du client.

**ikev2 remote-authentication pre-shared-key** *key*

**Exemple :**

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key *****
```

**Étape 3** Configurer le PSK de l'ASA

**ikev2 local-authentication pre-shared-key** *key*

**Exemple :**

```
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key *****
```

**Étape 4** Configurer le PPK du client

**ikev2 remote-authentication post-quantum-key** *key* **identifier** *id* mandatory

- key (clé) : spécifiez la clé PPK.
- ID : spécifiez la chaîne unique permettant d'identifier le PPK. Cette valeur doit correspondre à l'ID PPK dans le profil VPN de Secure Client.
- mandatory (obligatoire) : spécifiez si PPK est obligatoire pour la connexion VPN. Si vous ne spécifiez pas obligatoire, la configuration PPK sera facultative.

**Exemple :**

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication post-quantum-key  *****
 identifier PPKID_test mandatory
```

---

L'exemple suivant montre un extrait de la configuration du groupe de tunnels de l'ASA à l'aide de PPK et de PSK :

**Exemple**

```
tunnel-group secure_client_PPK ipsec-attributes
       ikev2 remote-authentication pre-shared-key *****
       ikev2 local-authentication pre-shared-key *****
       ikev2 remote-authentication post-quantum-key ***** identity PPKID_test mandatory
```

Tenez compte des points suivants :

- Le nom du groupe de tunnels doit correspondre à la chaîne IKEIdentity du profil VPN.
- L'ID PPK dans la configuration du groupe de tunnels doit correspondre à l'ID_PPK du profil VPN.

**Références supplémentaires**

- RFC 8784
- Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect), version 5

# Exemples de configuration pour les VPN d'accès à distance IPsec

L'exemple suivant montre comment configurer un VPN IPsec/IKEv1 d'accès à distance :

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

L'exemple suivant montre comment configurer un VPN IPsec/IKEv2 d'accès à distance :

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

# Exemples de configuration pour le VPN d'accès à distance IPsec IKEv2 basé sur les normes en mode multi-contexte

Les exemples suivants montrent comment configurer l'ASA pour le VPN d'accès à distance IPsec/IKEv2 basé sur les normes en mode multicontexte. Les exemples fournissent respectivement des renseignements sur les configurations du contexte système et du contexte d'utilisateur.

Pour la configuration de contexte système :

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%


hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

Pour la configuration en contexte d'utilisateur :

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

Les connexions d'accès à distance IPsec/IKEv2 des clients basés sur des normes aboutissent par défaut au groupe de tunnels DefaultRAGroup :

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
```

```
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#
```

# Exemples de configuration pour le VPN d'accès à distance Secure Client (services client sécurisés) IPSec IKEv2 en mode multicontexte

Les exemples suivants montrent comment configurer l'ASA pour le VPN d'accès à distance IPsec/IKEv2 Secure Client (services client sécurisés) en mode multicontexte. Les exemples fournissent respectivement des renseignements sur les configurations du contexte système et du contexte d'utilisateur.

Pour la configuration de contexte système :

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%


hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts using
 class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

La création d'un système de fichiers virtuel pour chaque contexte peut contenir des fichiers Secure Client (services client sécurisés) comme l'image et le profil.

```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

Pour la configuration en contexte d'utilisateur :

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
hostname/CTX3(config-webvpn)#tunnel-group-list enable


hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
```

```
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes


hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

Dans l'exemple ci-dessous, pour activer les services client, utilisez la commande **crypto ikev2 enable outside client-services**.

Le serveur de services client fournit un accès HTTPS (SSL) pour permettre au téléchargeur Secure Client de recevoir les mises à jour logicielles, les profils, les fichiers de localisation et de personnalisation, les CSD, les SCEP et les autres téléchargements de fichiers requis par le client. Si vous sélectionnez cette option, précisez le numéro de port des services client. Si vous n'activez pas le serveur de services client, les utilisateurs ne pourront pas télécharger les fichiers dont le Secure Client pourrait avoir besoin.

**Remarque** Vous pouvez utiliser le même port que celui que vous utilisez pour le VPN SSL sur le même périphérique. Même si vous avez configuré un VPN SSL, vous devez sélectionner cette option pour activer les téléchargements de fichiers sur SSL pour les clients IPsec-IKEv2.

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside


hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

# Historique des VPN d'accès à distance

| Nom de la caractéristique | Versions | Renseignements sur les fonctionnalités |
|---|---|---|
| VPN d'accès à distance pour IPsec IKEv1 et SSL. | 7.0 | Les VPN d'accès à distance permettent aux utilisateurs de se connecter à un site central par le biais d'une connexion sécurisée sur un réseau TCP/IP comme Internet. |
| VPN d'accès à distance pour IPsec IKEv2. | v 8.4(1) | Ajout de la prise en charge d'IPsec IKEv2 pour le Secure Client (services client sécurisés). |

| Nom de la caractéristique | Versions | Renseignements sur les fonctionnalités |
|---|---|---|
| Prise en charge automatique de MOBIKE pour les VPN d'accès à distance. | 9.8(1) | Ajout de la prise en charge de Mobile IKE (MOBIKE) pour les VPN d'accès à distance IPsec IKEv2. Mobike est toujours activé.<br>Ajout de la commande `ikev2 mobike-rrc` pour activer la vérification de la routabilité de retour pendant les communications mobike pour les connexions VPN IKEv2 RA. |
| Prise en charge des VPN d'accès à distance IPsec IKEv2 en mode multi-contexte | 9.9(2) | Prise en charge de la configuration d'ASA pour permettre à Secure Client (services client sécurisés) et aux clients VPN IPSec IKEv2 tiers basés sur les normes d'établir des sessions VPN d'accès à distance avec l'ASA fonctionnant en mode de contexte multiple.<br>Ajout de la commande `ikev2 rsa-sig-hash sha1` pour signer la charge utile d'authentification. |
| RSA avec algorithme de hachage SHA-1 pour signer la charge utile d'authentification | 9.12(1) | Prise en charge de la signature de la charge utile d'authentification avec l'algorithme de hachage SHA-1 lors de l'utilisation de clients VPN IPSec IKEv2 tiers basés sur les normes pour établir des sessions VPN d'accès à distance avec l'ASA. |
| Dépréciation des chiffrements IKE/IPsec (chiffrement et intégrité/PRF)<br>Prise en charge du groupe DH 14 pour IKEv1 | 9.13(1) | Les chiffrements/intégrité/PRF suivants sont obsolètes et seront supprimés dans la version ultérieure - 9.14(1) :<br>• Chiffrement 3DES<br>• Chiffrement DES<br>• Intégrité MD5<br>Ajout de la prise en charge du groupe DH 14 (par défaut) pour IKEv1. Les options de commande groupe 2 et groupe 5 ont été abandonnées et seront supprimées dans la version ultérieure - 9.14(1). |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.