DHCP et DDNS

Les rubriques suivantes expliquent les services DHCP et DDNS et la façon de les configurer sur les périphériques Threat Defense.

À propos des services DHCP et DDNS

Les rubriques suivantes décrivent le serveur DHCP, l'agent de relais DHCP et la mise à jour DDNS.

À propos du serveur DHCPv4

DHCP fournit des paramètres de configuration réseau, tels que des adresses IP, aux clients DHCP. Le périphérique appareil de défense contre les menaces peut fournir un serveur DHCP aux clients DHCP connectés aux interfaces appareil de défense contre les menaces . Le serveur DHCP fournit des paramètres de configuration réseau directement aux clients DHCP.

Un client DHCP IPv4 utilise une adresse de diffusion plutôt qu'une adresse de multidiffusion pour atteindre le serveur. Le client DHCP est à l'écoute des messages sur le port UDP 68; le serveur DHCP est à l'écoute des messages sur le port UDP 67.

Le serveur DHCP pour IPv6 n'est pas pris en charge; vous pouvez, cependant, activer le relais DHCP pour le trafic IPv6.

Options de DHCP

DHCP fournit une structure pour la transmission des informations de configuration aux hôtes sur un réseau TCP/IP. Les paramètres de configuration sont transportés dans des éléments étiquetés qui sont stockés dans le champ Options du message DHCP. Les données sont également appelées options. Les renseignements sur

le fournisseur sont également stockés dans Options, et tous les postes d'informations sur le fournisseur peuvent être utilisés comme options DHCP.

Par exemple, les téléphones IP Cisco téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un téléphone IP Cisco démarre, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une demande avec l'option 150 ou 66 au serveur DHCP pour obtenir cette information.

- L'option 150 de DHCP fournit les adresses IP d'une liste de serveurs TFTP.
- L'option DHCP 66 fournit l'adresse IP ou le nom d'hôte d'un seul serveur TFTP.
- L'option 3 de DHCP définit la voie de routage par défaut.

Une seule demande peut inclure les deux options 150 et 66. Dans ce cas, le serveur DHCP de l'ASA fournit des valeurs pour les deux options dans la réponse si elles sont déjà configurées sur l'ASA.

Vous pouvez utiliser les options DHCP avancées pour fournir les paramètres DNS, WINS et de nom de domaine aux clients DHCP. L'option DHCP 15 est utilisée pour le suffixe de domaine DNS. Vous pouvez également utiliser le paramètre de configuration automatique DHCP pour obtenir ces valeurs ou les définir manuellement. Lorsque vous utilisez plusieurs méthodes pour définir ces informations, elles sont transmises aux clients DHCP dans l'ordre suivant :

1. Paramètres configurés manuellement.
2. Paramètres des options DHCP avancées
3. Paramètres de configuration automatique de DHCP.

Par exemple, vous pouvez définir manuellement le nom de domaine que vous souhaitez que les clients DHCP reçoivent, puis activer la configuration automatique de DHCP. Bien que la configuration automatique de DHCP découvre le domaine ainsi que les serveurs DNS et WINS, le nom de domaine défini manuellement est transmis aux clients DHCP avec les noms de serveurs DNS et WINS découverts, car le nom de domaine découvert par le processus de configuration automatique de DHCP est remplacé par l' domaine défini.

À propos du serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces, en définissant un ensemble DHCP IPv6 et en l'affectant au serveur DHCPv6. Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que défense contre les menaces a reçu à l'aide de la délégation de préfixe.

À propos de l'agent relais DHCP

Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique appareil de défense contre les menaces , car il ne transfère

pas le trafic de diffusion. L'agent de relais DHCP vous permet de configurer l'interface du appareil de défense contre les menaces qui reçoit les diffusions pour transférer les demandes DHCP vers un serveur DHCP qui est disponible via une autre interface.

Exigences et prérequis DHCP et DDNS

Prise en charge des modèles

Défense contre les menaces

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Lignes directrices pour les services DHCP et DDNS

Cette section comprend des directives et des limites que vous devez vérifier avant de configurer les services DHCP et DDNS.

Mode pare-feu

- Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.
- Le serveur DHCP est pris en charge en mode de pare-feu transparent sur une interface de membre de groupe de ponts. En mode routé, le serveur DHCP est pris en charge sur l'interface BVI, pas sur l'interface des membres du groupe de ponts. Les BVI doivent avoir un nom pour que le serveur DHCP puisse fonctionner.
- DDNS n'est pas pris en charge en mode de pare -feu transparent ou en mode routé sur l'interface de BVI ou l'interface de membre du groupe de ponts.

IPv6

Ne prend pas en charge IPv6 pour le serveur DHCP; IPv6 pour le relais DHCP est pris en charge.

Serveur DHCPv4

- Le ensemble DHCP disponible maximal est de 256 adresses.
- Vous ne pouvez configurer qu'un seul serveur DHCP sur chaque interface. Chaque interface peut avoir son propre ensemble d'adresses à utiliser. Cependant, les autres paramètres DHCP, tels que les serveurs DNS, le nom de domaine, les options, le délai de ping et les serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.

- Vous ne pouvez pas configurer une interface en tant que client DHCP si un serveur DHCP est également activé sur cette interface; vous devez utiliser une adresse IP statique.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- appareil de défense contre les menaces ne prend pas en charge les serveurs DHCP QIP pour une utilisation avec le service mandataire DHCP.
- Le serveur DHCP ne prend pas en charge les demandes BOOTP.

Relais DHCP

- Vous pouvez configurer un maximum de 10 serveurs de relais DHCPv4, serveurs globaux et propres à l'interface combinés, avec un maximum de 4 serveurs par interface.
- Vous pouvez configurer un maximum de 10 serveurs relais DHCPv6. Les serveurs propres à une interface pour IPv6 ne sont pas pris en charge.
- Vous ne pouvez pas configurer un serveur DHCP et un relais DHCP sur le même périphérique, même si vous souhaitez les activer sur des interfaces différentes; vous ne pouvez configurer qu'un seul type de service.
- Les services de relais DHCP ne sont pas offerts dans le mode transparent du pare-feu. Vous pouvez, cependant, autoriser le trafic DHCP en utilisant une règle d'accès. Pour autoriser les demandes et les réponses DHCP par l'intermédiaire du appareil de défense contre les menaces , vous devez configurer deux règles d'accès, une qui autorise les demandes DHCP de l'interface interne vers l'extérieur (port de destination d'UDP 67) et une qui autorise les réponses du serveur de l'autre côté (port de destination UDP 68).
- Pour IPv4, les clients doivent être connectés directement à appareil de défense contre les menaces et ne peuvent pas envoyer de demandes par un autre agent de relais ou un routeur. Pour IPv6, appareil de défense contre les menaces prend en charge les paquets d'un autre serveur de relais.
- Les clients DHCP doivent se trouver sur des interfaces différentes des serveurs DHCP vers lesquels appareil de défense contre les menaces relaye les demandes.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.
- Le relais DHCP n'est pas pris en charge sur les interfaces de tunnel virtuel (VTI).

Configurer le serveur DHCPv4

Consultez les étapes suivantes pour configurer un serveur DHCPv4.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **DHCP > DHCP Server (serveur DHCP)**.

Étape 3 Configurez les options de serveur DHCP suivantes :

- **Ping Timeout**(délai d'expiration de ping) : durée en millisecondes pendant laquelle le périphérique défense contre les menaces attend pour rendre caduque une tentative de ping de DHCP. Les valeurs valides vont de 10 à 10000 millisecondes. La valeur par défaut est de 50 millisecondes.

  Pour éviter les conflits d'adresses, le périphérique défense contre les menaces envoie deux paquets Ping ICMP à une adresse avant d'affecter cette adresse à un client DHCP.

- **Durée du bail** : la durée en secondes pendant laquelle le client peut utiliser l'adresse IP qui lui a été attribuée avant l'expiration du bail. Les valeurs valides vont de 300 à 1 048 575 secondes. La valeur par défaut est de 3600 secondes (1 heure).

- (mode routage) **Auto-configuration** : active la configuration automatique de DHCP sur le périphérique défense contre les menaces . La configuration automatique permet au serveur DHCP de fournir aux clients DHCP des informations sur le serveur DNS, le nom de domaine et le serveur WINS obtenues d'un client DHCP qui s'exécute sur l'interface précisée. Sinon, vous pouvez désactiver la configuration automatique et ajouter les valeurs vous-même à l'étape 4.

- (Routed mode) **Interface** : spécifie l'interface à utiliser pour la configuration automatique. Pour un périphérique avec une capacité de routage virtuel, cette interface ne peut être qu'une interface de routeur virtuel global.

Étape 4 Pour remplacer les paramètres configurés automatiquement, procédez comme suit :

- Saisissez le nom de domaine de l'interface. Par exemple, votre périphérique peut faire partie du domaine Votre_entreprise.

- Dans la liste déroulante, choisissez les serveurs DNS (principaux et secondaires) configurés pour l'interface. Pour ajouter un nouveau serveur DNS, consultez Création d'objets réseau.

- Dans la liste déroulante, choisissez les serveurs WINS (principaux et secondaires) configurés pour l'interface. Pour ajouter un nouveau serveur WINS, consultez Création d'objets réseau.

Étape 5 Sélectionnez **Serveur**, cliquez sur **Ajouter** et configurez les options suivantes :

- **Interface** : Choisissez une interface dans la liste déroulante. En mode transparent, spécifiez une interface de membre de groupe de ponts nommée. En mode routage, spécifiez une interface routée nommée ou un BVI nommé; ne spécifiez pas l'interface des membres du groupe de ponts. Notez que chaque interface de membre de groupe de ponts pour les BVI doit également être nommée pour que le serveur DHCP puisse faire fonctionner.

- **Address Pool**(ensemble des adresses) : définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.

- **Enable DHCP Server** : activez le serveur DHCP sur l'interface sélectionnée.

Étape 6 Cliquez sur **OK** pour enregistrer la configuration du serveur DHCP.

Étape 7 (Facultatif) Sélectionnez **Advanced**(Avancé), cliquez sur **Add**(ajouter) et précisez le type d'informations que vous souhaitez que l'option renvoie au client DHCP :

- **Option Code** (Code d'option) : le périphérique défense contre les menaces prend en charge les options DHCP répertoriées dans RFC 2132, RFC 2562 et RFC 5510 pour l'envoi d'informations. Toutes les

options DHCP (1 à 255) sont prises en charge, à l'exception des 1, 12, 50 à 54,58 à 59, 61, 67 et 82. Consultez À propos du serveur DHCPv4, à la page 1pour en savoir plus sur les codes d'option DHCP.

Remarque Le périphérique défense contre les menaces ne vérifie pas que le type et la valeur d'option que vous fournissez correspondent au type et à la valeur attendus pour le code d'option, comme défini dans la RFC 2132. Pour en savoir plus sur les codes d'option, les types associés et les valeurs attendues, consultez la RFC 2132.

- **Type** : Type d'option DHCP. Les options disponibles comprennent **IP**, **ASCII**et **HEX**. Si vous avez choisi IP, vous devez ajouter des adresses IP dans les champs IP Address (adresse IP). Si vous avez choisi ASCII, vous devez ajouter la valeur ASCII dans le champ ASCII. Si vous avez choisi HEX, vous devez ajouter la valeur HEX dans le champ HEX.
- **IP Address 1** et **IP Address 2** : adresses IP à renvoyer avec ce code d'option. Pour ajouter une nouvelle adresse IP, consultez Création d'objets réseau.
- **ASCII** : valeur ASCII renvoyée au client DHCP. La chaîne de caractères ne peut pas inclure d'espaces.
- **HEX** : valeur HEX renvoyée au client DHCP. La chaîne de caractères doit avoir un nombre pair de chiffres et aucun espace. Vous n'avez pas besoin d'utiliser le préfixe 0x.

Étape 8 Cliquez sur **OK** pour enregistrer la configuration de code d'option.

Étape 9 Cliquez sur **Save** (Enregistrer) sur la page DHCP pour enregistrer vos modifications.

Configurer le serveur sans état DHCPv6

Pour les clients qui utilisent SLAAC (StateLess Address Auto Configuration) conjointement avec la fonctionnalité de délégation de préfixe, vous pouvez configurer le défense contre les menaces pour qu'il fournisse des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces .

Créer un ensemble d'adresses IPv6 du DHCP

Créer un ensemble DHCP IPv6 à utiliser avec le serveur DHCPv6. Le serveur DHCPv6 fournit des informations telles que le serveur DNS ou le nom de domaine lorsque les clients envoient des paquets de demande d'information (IR) à défense contre les menaces . Le regroupement IPv6 du DHCP définit les paramètres à envoyer dans les messages IR.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

Procédure

Étape 1 Choisissez **Objects (objets)** > **Object Management (gestion des objets)**.

Étape 2 Sélectionnez **DHCP IPv6 Pool** (Regroupement IPv6 DHCP) dans la liste des types d'objets.

Étape 3 Cliquez sur **Ajouter** ( ).

Étape 4 Configurez le **serveur DNS** et le **nom de domaine**.

Vous pouvez soit définir manuellement les valeurs et cliquer sur **Add** (Ajouter), soit cocher **Import** (importer) pour utiliser un ou plusieurs paramètres que défense contre les menaces a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et utiliser également **Importer**.

Illustration 1 : Définir manuellement les valeurs

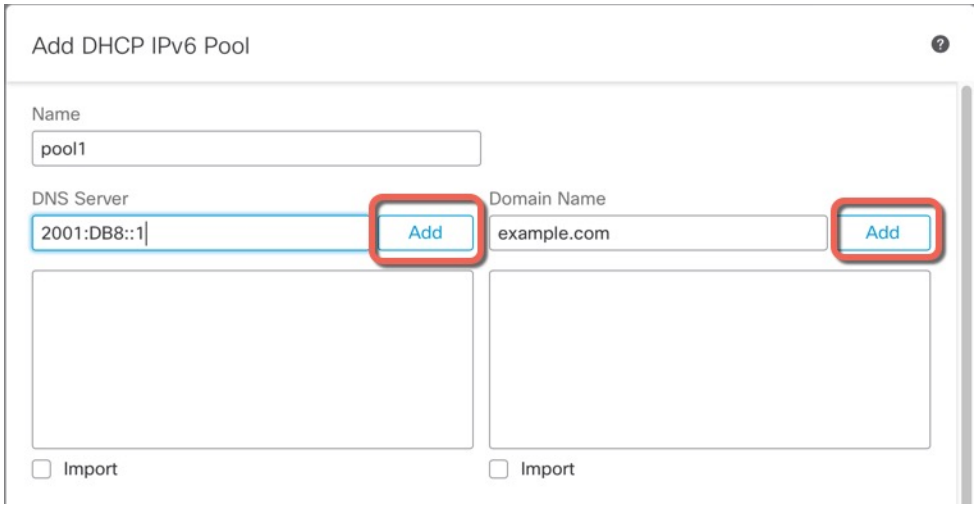
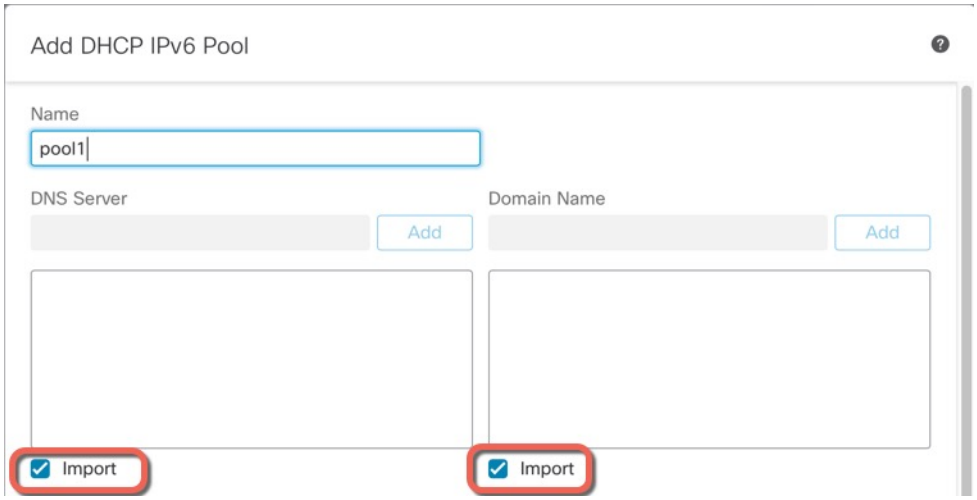


Illustration 2 : Importer les valeurs



Étape 5 Définissez **Autres options de serveur**

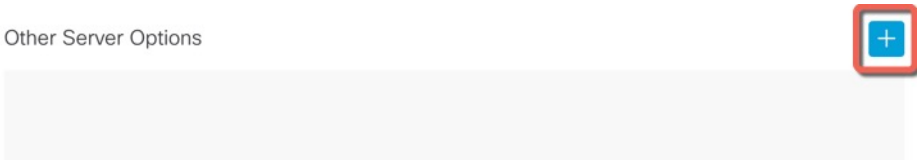
Vous pouvez définir le nom de domaine et l'adresse IP des serveurs suivants :

- NIS
- NISP
- SIP

- SNTP

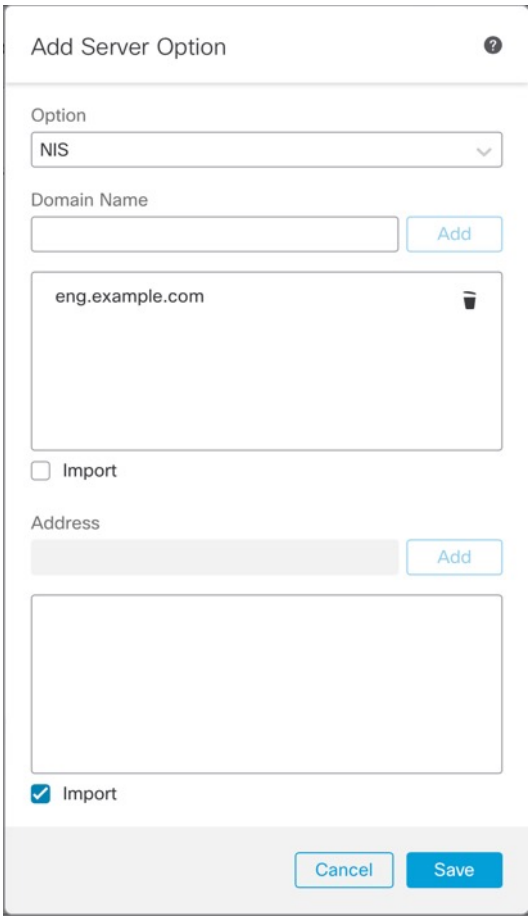
a) Cliquez sur **Ajouter** ( ).

Illustration 3 : Autres options de serveur



b) Choisissez le type de serveur sous **Option** et définissez manuellement le **nom de domaine** et l'**adresse** ou cochez **Importer**.

Illustration 4 : Définir le nom de domaine et l'adresse du serveur



import (Importer) utilise un ou plusieurs paramètres que défense contre les menaces a obtenus du serveur DHCPv6 sur l'interface client de délégation de préfixe. Vous pouvez combiner des paramètres configurés manuellement avec des paramètres importés; cependant, vous ne pouvez pas configurer le même paramètre manuellement et utiliser également **Importer**.

c) Cliquez sur **Save** (enregistrer).

d) Répétez l'opération pour chaque type de serveur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Utilisez ce regroupement avec le serveur DHCPv6. Consultez Activer le serveur sans état DHCPv6, à la page 9.

Activer le serveur sans état DHCPv6

Pour les clients qui utilisent la configuration automatique des adresses sans état (SLAAC) conjointement avec la fonctionnalité de délégation de préfixe (Activer le client de délégation de préfixe IPv6), vous pouvez configurer les défense contre les menaces pour fournir des informations telles que le serveur DNS ou le nom de domaine lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que le défense contre les menaces a reçu à l'aide de la délégation de préfixe.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

Avant de commencer

Ajouter un objet de regroupement IPv6 de DHCP. Consultez Créer un ensemble d'adresses IPv6 du DHCP, à la page 6. L'objet définit les paramètres de serveur inclus dans les messages de demande d'information (IR).

Procédure

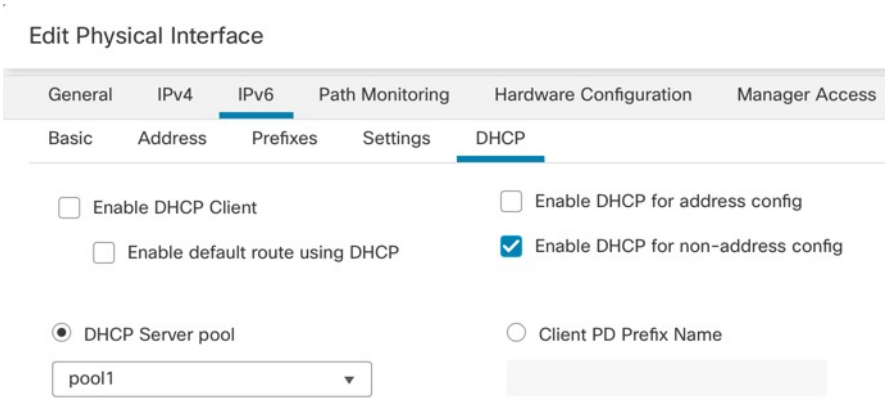
Étape 1 Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

Étape 2 Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur la page **IPv6**, puis sur **DHCP**.

Étape 4 Cliquez sur **DHCP Server Pool**(regroupement de serveurs DHCP) et choisissez l'objet que vous avez créé précédemment.

Illustration 5 : Activer le serveur DHCPv6



Étape 5 Cochez la case **Activer DHCP pour la configuration sans adresse** pour informer les clients SLAAC à propos du serveur DHCPv6.

Cet indicateur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

Configurer les agents de relais DHCP.

Vous pouvez configurer un agent de relais DHCP pour transférer les demandes DHCP reçues sur une interface vers un ou plusieurs serveurs DHCP. Les clients DHCP utilisent les diffusions UDP pour envoyer leurs premiers messages DHCPDISCOVER, car ils ne disposent pas d'informations sur le réseau auquel ils sont connectés. Si le client se trouve sur un segment de réseau qui n'inclut pas de serveur, les diffusions UDP ne sont normalement pas transférées par le périphérique défense contre les menaces , car il ne transfère pas le trafic de diffusion.

Vous pouvez remédier à cette situation en configurant l'interface du périphérique défense contre les menaces qui reçoit les diffusions pour qu'elle transmette les demandes DHCP à un serveur DHCP situé sur une autre interface.

Remarque Le relais DHCP n'est pas pris en charge en mode transparent de pare-feu.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Sélectionnez **DHCP** > **DHCP Relay** (Relais DHCP).

Étape 3 Dans les champs **IPv4 Relay Timeout** (Délai d'expiration de relais IPv4) et **IPv6 Relay Timeout** (Délai d'expiration de relais IPv6), saisissez le délai en secondes pendant lequel le périphérique défense contre les menaces attend la fin du délai d'expiration de l'agent de relais DHCP. Les valeurs valides vont de 1 à 3 600 secondes. La valeur par défaut est 60 secondes.

Le délai d'expiration est destiné à la négociation de l'adresse par l'agent de relais DHCP local.

Étape 4 Dans l'onglet **DHCP Relay Agent** (Agent de relais DHCP) , cliquez sur **Add** (Ajouter) et configurez les options suivantes :

- **Interface** : interface connectée aux clients DHCP.
- **Enable IPv4 Relay**(activer le relais IPv4) : active le relais DHCP IPv4 pour cette interface.
- **Set Route** (Définir la voie de routage) : (pour IPv4) Modifie l'adresse de la passerelle par défaut dans le message DHCP du serveur en lui donnant celle de l'interface de périphérique défense contre les menaces qui est la plus proche du client DHCP, qui a relayé la requête DHCP initiale. Cette action permet au client de configurer sa route par défaut pour qu'elle pointe vers le défense contre les menaces périphérique, même si le serveur DHCP spécifie un routeur différent. S'il n'y a pas d'option de routeur par défaut dans le paquet, le périphérique défense contre les menaces en ajoute une contenant l'adresse de l'interface.
- **Enable IPv6 Relay**(activer le relais IPv6) : active le relais DHCP IPv6 pour cette interface.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications de l'agent de relais DHCP.

Étape 6 Dans la page **DHCP Servers** (serveurs DHCP), cliquez sur **Add** (ajouter) puis configurez les options suivantes :

Ajoutez les adresses des serveurs IPv4 et IPv6 comme entrées distinctes, même si elles appartiennent au même serveur.

- **Server** (serveur) : l'adresse IP du serveur DHCP. Choisissez une adresse IP dans la liste déroulante. Pour en ajouter une nouvelle, consultez Création d'objets réseau
- **Interface** : l'interface à laquelle le serveur DHCP spécifié est connecté. L'agent relais DHCP et le serveur DHCP ne peuvent pas être configurés sur la même interface.

Étape 7 Cliquez sur **OK** pour enregistrer les modifications du serveur DHCP.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page DHCP pour enregistrer vos modifications.

Configuration du DNS dynamique

Lorsqu'une interface utilise l'adressage IP DHCP, l'adresse IP attribuée peut changer lors du renouvellement du bail DHCP. Lorsque l'interface doit être accessible à l'aide d'un nom de domaine complet (FQDN), le changement d'adresse IP peut rendre périmés les enregistrements de ressources du serveur DNS. Le DNS dynamique (DDNS) fournit un mécanisme pour mettre à jour les programmes de routage du DNS chaque fois

que l'adresse IP ou le nom d'hôte change. Vous pouvez également utiliser DDNS pour les adresses IP statiques ou PPPoE.

DDNS met à jour les réflecteurs de routage suivants sur le serveur DNS : le RR A comprend le mappage nom-adresse IP, tandis que le RR PTR mappe les adresses aux noms.

défense contre les menaces prend en charge les méthodes de mise à jour DDNS suivantes :

- DDNS standard : La méthode de mise à jour DDNS standard est définie par la RFC 2136.

  Avec cette méthode, le défense contre les menaces et le serveur DHCP utilisent les requêtes DNS pour mettre à jour les taux de renouvellement (RR) DNS. Le défense contre les menaces ou le serveur DHCP envoie une requête DNS à son serveur DNS local pour obtenir des informations sur le nom d'hôte et, en fonction de la réponse, détermine le serveur DNS principal qui possède les RR. Le serveur défense contre les menaces ou DHCP envoie ensuite une demande de mise à jour directement au serveur DNS principal. Consultez les scénarios typiques suivants.

  - défense contre les menaces met à jour le RR de A et le serveur DHCP met à jour le RR des PTR.

    En règle générale, défense contre les menaces « possède » le RR de A, tandis que le serveur DHCP « possède » le taux de renouvellement (RR) PTR, de sorte que les deux entités doivent demander les mises à jour séparément. Lorsque l'adresse IP ou le nom d'hôte changent, le défense contre les menaces envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR du PTR.

  - Le serveur DHCP met à jour les taux de renouvellement A et PTR.

    Utilisez ce scénario si défense contre les menaces n'a pas l'autorité pour mettre à jour le RR de A. Lorsque l'adresse IP ou le nom d'hôte change, le défense contre les menaces envoie une requête DHCP (y compris l'option FQDN) au serveur DHCP pour l'informer qu'il doit demander une mise à jour des RR A et PTR.

  Vous pouvez configurer différentes propriétés en fonction de vos besoins en matière de sécurité et des exigences du serveur DNS principal. Par exemple, pour une adresse statique, défense contre les menaces doit être propriétaire des mises à jour pour les deux enregistrements.

- Web : la méthode de mise à jour Web utilise la spécification de l'API distante DynDNS. (https://help.dyn.com/remote-access-api/).

  Avec cette méthode, lorsque l'adresse IP ou le nom d'hôte change, le défense contre les menaces envoie une requête HTTP directement à un fournisseur DNS auprès duquel vous avez un compte.

La page **DDNS** prend également en charge la définition des paramètres de serveur DHCP relatifs à DDNS.

Remarque DDNS n'est pas pris en charge sur les interfaces BVI ou de membre du groupe de ponts.

Avant de commencer

- Configurez un groupe de serveurs DNS sur **Objects (Objets)** > **Object Management (Gestion des objets)** > **DNS Server Group**, puis activez le groupe pour l'interface sur **Devices** > **Platform Settings** > **DNS** (Périphériques > Paramètres de la plateforme > DNS). Consultez DNS.

- Configurez le nom d'hôte du périphérique. Vous pouvez configurer le nom d'hôte lorsque vous effectuez la configuration initiale défense contre les menaces , ou en utilisant la commande **configure network hostname**. Si vous ne spécifiez pas de nom d'hôte par interface, le nom d'hôte du périphérique est utilisé.

Procédure

Étape 1 Sélectionnez **Devices (appareils)** > **Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .

Étape 2 Choisissez **DHCP** > **DDNS**.

Étape 3 Méthode standard DDNS : configurez une méthode de mise à jour DDNS pour activer les requêtes DNS de défense contre les menaces .

Vous n'avez pas besoin de configurer une méthode de mise à jour DDNS si le serveur DHCP effectue toutes les demandes.

a) Dans **Méthodes de mise à jour DDNS**, cliquez sur **Add** (ajouter).
b) Définissez le **nom de la méthode**.
c) Cliquez sur **DDNS**.
d) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).
e) Définissez les **Mises à jour des enregistrements** que vous souhaitez que défense contre les menaces mette à jour.

   Ce paramètre affecte uniquement les enregistrements que vous souhaitez mettre à jour directement à partir de défense contre les menaces ; Pour déterminer les enregistrements que vous souhaitez que le serveur DHCP mette à jour, configurez les paramètres du client DHCP par interface ou globalement. Consultez, Étape 5, à la page 14.

   - **Not Defined** (non défini) : désactive les mises à jour DNS à partir de défense contre les menaces .
   - **Enregistrements A et PTR** : définit défense contre les menaces pour mettre à jour les dossiers de routage A et PTR. Utilisez cette option pour les adresses IP statiques ou PPPoE.
   - **A Records** (enregistrements A) : définit les défense contre les menaces pour mettre à jour les RR A uniquement. Utilisez cette option si vous souhaitez que le serveur DHCP mette à jour le RR des PTR.

f) Cliquez sur **OK**.
g) Attribuez cette méthode à l'interface dans Étape 5, à la page 14.

Étape 4 Méthode Web : configurez une méthode de mise à jour DDNS pour activer les demandes de mise à jour HTTP à partir de défense contre les menaces .

a) Dans **Méthodes de mise à jour DDNS**, cliquez sur **Add** (ajouter).
b) Définissez le **nom de la méthode**.
c) Cliquez sur **Web**.
d) Définissez le **type de mise à jour Web** pour mettre à jour IPv4, IPv6 ou les deux types d'adresses.
e) Définissez l'**URL Web**. Précisez l'URL de mise à jour. Vérifiez auprès de votre fournisseur DNS pour connaître l'URL requise.

Utilisez la syntaxe suivante :

https://*username (nom d'utilisateur)***:***password (mot de passe)***@***provider-domain (domaine du fournisseur)*/*path (chemin)***?hostname=<h>&myip=<a>**

Exemple :

https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>

f) (Facultatif) Configurez l'**intervalle de mise à jour** entre les requêtes DNS. Par défaut, lorsque toutes les valeurs sont définies sur 0, des demandes de mise à jour sont envoyées à chaque changement de l'adresse IP ou du nom d'hôte. Pour envoyer des demandes régulièrement, définissez les paramètres **Days** (0-364), **Hours**, **Minutes** et **Seconds** Jours, Heures, Minutes, secondes).

g) Cliquez sur **OK**.

h) Attribuez cette méthode à l'interface dans Étape 5, à la page 14.

i) La méthode de type Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS. Consultez, Étape 9, à la page 16.

Étape 5 Configurez les paramètres d'interface pour DDNS, y compris la définition de la méthode de mise à jour, les paramètres du client DHCP et le nom d'hôte pour cette interface.

a) Dans **les paramètres d'interface DDNS**, cliquez sur **Add**(ajouter).

b) Choisissez **l'interface** dans la liste déroulante.

c) Choisissez le **nom de la méthode** que vous avez créé sur la page **DDNS Update Méthodes** (Méthode de mise à jour DDNS).

(Méthode DDNS standard) Vous n'avez pas besoin d'attribuer de méthode si vous souhaitez que le serveur DHCP effectue toutes les mises à jour.

d) Définissez le **nom d'hôte** pour cette interface.

Si vous ne définissez pas de nom d'hôte, le nom d'hôte du périphérique est utilisé. Si vous ne spécifiez pas de nom de domaine complet, le domaine par défaut du groupe de serveurs DNS est ajouté (pour les adresses IP statiques ou PPPoE) ou le nom de domaine du serveur DHCP est ajouté (pour les adresses IP DHCP).

e) Méthode DDNS standard : configurer les **demandes de client DHCP au serveur DHCP pour qu'il mette à jour les demandes** afin de déterminer quels enregistrements vous souhaitez que le serveur DHCP mette à jour.

Le défense contre les menaces envoie les requêtes des clients DHCP au serveur DHCP. Notez que le serveur DHCP doit également être configuré pour prendre en charge DDNS. Le serveur peut être configuré pour répondre aux demandes du client ou il peut remplacer les commandes du client (auquel cas, il répondra au client pour que le client n'essaye pas également d'effectuer les mises à jour effectuées par le serveur).

Pour les adresses IP statiques ou PPPoE, ces paramètres sont ignorés.

Remarque Vous pouvez également définir ces valeurs globalement pour toutes les interfaces dans la page **DDNS**. Les paramètres par interface prévalent sur les paramètres globaux.

- **Not Selected** : Désactive les requêtes DDNS au serveur DHCP. Même si le client ne demande pas de mises à jour DDNS, le serveur DHCP peut être configuré pour envoyer quand même des mises à jour.
- **No Update** : demande au serveur DHCP de ne pas effectuer de mises à jour. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A et PTR** activés.

- **Only PTR** : demande au serveur DHCP d'effectuer la mise à jour des PTR RR. Ce paramètre fonctionne conjointement avec une méthode de mise à jour DDNS avec les **enregistrements A** activés.
- **Enregistrements A et PTR** : Demande au serveur DHCP d'effectuer les mises à jour des enregistrements A et PTR RR. Ce paramètre ne nécessite pas l'association d'une méthode de mise à jour DDNS à l'interface.

f) Cliquez sur **OK**.

Remarque Les paramètres de la mise à **jour dynamique du DNS** sont liés aux paramètres du serveur DHCP lorsque vous activez un serveur DHCP sur défense contre les menaces . Consultez Étape 6, à la page 15 pour obtenir de plus amples renseignements.

Étape 6 Si vous activez le serveur DHCP sur un défense contre les menaces , vous pouvez configurer les paramètres du serveur DHCP pour DDNS.

Pour activer le serveur DHCP, consultez Configurer le serveur DHCPv4, à la page 4). Vous pouvez configurer le comportement du serveur lorsque les clients DHCP utilisent la méthode de mise à jour DDNS standard. Si le serveur effectue des mises à jour, si le bail du client expire (et n'est pas renouvelé), le serveur demandera au serveur DNS de supprimer les programmes de routage dont il était responsable.

a) Vous pouvez configurer les paramètres de serveur globalement ou par interface. Pour les paramètres globaux, consultez la page **DDNS** principale. Pour les paramètres par interface, consultez la page **DDNS Interface Settings** (Paramètres de l'interface DDNS). Les paramètres d'interface prévalent sur les paramètres globaux.

b) Configurez les répertoires de routage DNS que vous souhaitez que le serveur DHCP mette à jour sous **Dynamic DNS Update** (Mise à jour du DNS dynamique).

- **Not Selected** (Non sélectionné) : les mises à jour DDNS sont désactivées, même si le client les demande.
- **Only PTR** (PTR uniquement) : Active les mises à jour DDNS. Si vous activez le paramètre **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP), le serveur ne mettra à jour que le RR des PTR. Sinon, le serveur mettra à jour les taux de renouvellement (RR) demandés par le client. Si le client n'envoie pas de demande de mise à jour avec l'option de nom de domaine complet, le serveur demandera une mise à jour pour lesRR de A et les PTR en utilisant le nom d'hôte découvert dans l'option 12 de DHCP.
- **Enregistrements A et PTR** : active les mises à jour DDNS. Si vous activez le paramètre **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP), le serveur mettra à jour les RR A et PTR. Sinon, le serveur mettra à jour les taux de renouvellement (RR) demandés par le client. Si le client n'envoie pas de demande de mise à jour avec l'option de nom de domaine complet, le serveur demandera une mise à jour pour lesRR de A et les PTR en utilisant le nom d'hôte découvert dans l'option 12 de DHCP.

c) Pour remplacer les actions de mise à jour demandées par le client DHCP, cochez **Override DHCP Client Requests** (Remplacer les requêtes des clients DHCP).

Le serveur répondra au client que la demande a été remplacée, de sorte que le client n'essaye pas également d'effectuer les mises à jour que le serveur effectue.

Étape 7 (Facultatif) Configurer les paramètres généraux du client DHCP. Ces paramètres ne sont pas liés au DDNS, mais au comportement du client DHCP.

a) Dans la page **DDNS**, cochez **Enable DHCP Client Broadcast** (activer la diffusion du client DHCP) pour demander au serveur DHCP de diffuser la réponse DHCP (DHCP option 1).

b) Pour forcer le stockage d'une adresse MAC dans un paquet de requête DHCP pour l'option 61 au lieu de la chaîne par défaut générée en interne, sur l'interface d'ID de client DHCP DDNS (**DDNS** > **DHCP Client ID Interface)**, choisissez l'interface dans la liste **Interfaces disponibles**, puis cliquez sur **Add** (ajouter) pour la déplacer vers la liste **Interfaces sélectionnées**.

   Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée. Ce paramètre n'est pas directement lié à DDNS, mais constitue un paramètre client DHCP général.

Étape 8 Cliquez sur **Save** (Enregistrer) sur la page Device (Périphérique) pour enregistrer vos modifications.

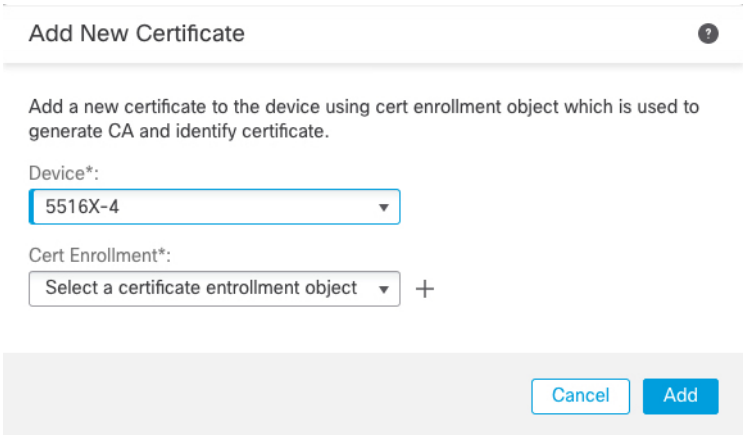
Étape 9 La méthode Web pour DDNS nécessite également que vous identifiiez l'autorité de certification racine du serveur DDNS pour valider le certificat du serveur DDNS pour la connexion HTTPS.

L'exemple suivant montre comment ajouter l'autorité de certification d'un serveur DDNS en tant que point de confiance.

a) Obtenez le certificat de l'autorité de certification du serveur DDNS. Cette procédure montre une importation manuelle au format PEM, mais vous pouvez également utiliser PKCS12.

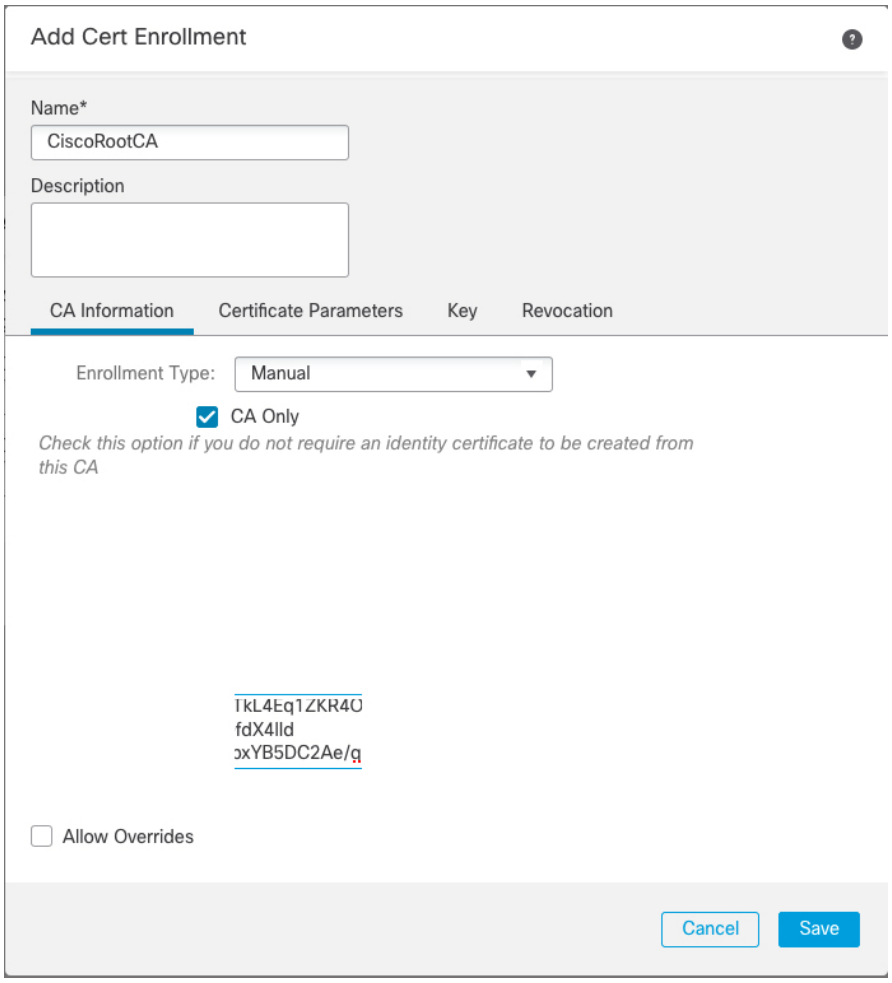
b) Dans centre de gestion, sélectionnez **Devices** > **Certificates** (Périphériques > Certificats) et cliquez sur **Add**(ajouter).

c) Sélectionnez un **périphérique**, puis cliquez sur **Ajouter** (+).



La boîte de dialogue **Add Cert Enrollment** (ajouter une inscription de certificat) s'affiche.

d) Remplissez les champs suivants, puis cliquez sur **Save**(Enregistrer) :



- Saisissez un **Nom**.
- Choisissez **Enrollment Type (Type d'inscription)** > **Manuel (manuel)**.
- Cliquez sur **Autorité de certification uniquement**.
- Collez le texte sur l'autorité de certification de l'étape 9.a, à la page 16.

e) Cliquez sur **Save** (enregistrer).

Historique de DHCP et DDNS

Fonctionnalité	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Serveur sans état DHCPv6	20221213	7.3.0	défense contre les menaces prend désormais en charge un serveur sans état DHCPv6 léger lors de l'utilisation du client de délégation de préfixe DHCPv6. défense contre les menaces fournit d'autres informations telles que le nom de domaine aux clients du SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) au défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Écrans nouveaux ou modifiés : • **Périphériques** > **Gestion des périphériques** > **Interfaces** > **Ajouter/modifier des interfaces** > **IPv6** > **DHCP** • **Objects (Objets)** > **Object Management (Gestion des objets)** > **DHCP IPv6 Pool (Bassin IPv6 DHCP)** Commandes nouvelles ou modifiées : **show ipv6 dhcp**

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.