Configuration avancée

Certaines fonctionnalités du périphérique sont configurées au moyen de commandes de configuration ASA. Bien que le Firepower Device Manager puisse configurer de nombreuses fonctionnalités basées sur les commandes, il ne les prend pas en charge toutes. Si vous devez utiliser certaines de ces fonctionnalités ASA qui ne sont pas prises en charge dans Firepower Device Manager, vous pouvez utiliser l'interface de ligne de commande Smart ou FlexConfig pour configurer manuellement les fonctionnalités.

Les rubriques suivantes expliquent ce type de configuration avancée plus en détail.

À propos de Smart CLI et de FlexConfig :

Firewall Threat Defense utilise des commandes de configuration ASA pour implémenter certaines fonctionnalités, mais pas toutes. Il n'y a pas d'ensemble unique de commandes de configuration Cisco Firewall Threat Defense.

Vous pouvez configurer les fonctionnalités de l'interface de ligne de commande en utilisant les méthodes suivantes :

- **Smart CLI** : (méthode préférée) Un modèle Smart CLI est un modèle prédéfini pour une fonctionnalité particulière. Toutes les commandes nécessaires à la fonctionnalité sont fournies, et vous devez simplement sélectionner les valeurs des variables. Le système valide votre sélection, ce qui vous permet de configurer plus facilement une fonctionnalité correctement. S'il existe un modèle Smart CLI pour la fonctionnalité souhaitée, vous devez utiliser cette méthode.
- **FlexConfig** : la politique FlexConfig est un ensemble d'objets FlexConfig. Les objets FlexConfig sont de forme plus libre que les modèles Smart CLI et le système n'effectue aucune validation de CLI, de variable ou de données. Vous devez connaître les commandes de configuration ASA et suivre les guides de configuration ASA pour créer une séquence valide de commandes.

L'objectif de Smart CLI et de FlexConfig est de vous permettre de configurer des fonctionnalités qui ne sont pas directement prises en charge par les politiques et les paramètres Firepower Device Manager.

Mise en garde Cisco recommande fortement d'utiliser les Smart CLI et FlexConfig uniquement si vous êtes un utilisateur avancé avec de solides connaissances en ASA, et ce, à vos propres risques. Vous pouvez configurer des commandes qui ne sont pas interdites. L'activation de fonctionnalités par le biais de Smart CLI et FlexConfig peut entraîner des résultats imprévus avec d'autres fonctionnalités configurées.

Vous pouvez communiquer avec le Centre d'assistance technique de Cisco pour obtenir de l'aide concernant les objets Smart CLI et FlexConfig que vous avez configurés. Le Centre d'assistance technique de Cisco ne conçoit ni n'écrit de configurations personnalisées au nom d'un client. Cisco n'exprime aucune garantie quant au bon fonctionnement ni à l'interopérabilité avec d'autres Cisco Firewall Threat Defense fonctionnalités. Les fonctionnalités Smart CLI et FlexConfig peuvent être obsolètes à tout moment. Pour obtenir une prise en charge des fonctionnalités entièrement garantie, vous devez attendre le soutien Firepower Device Manager. En cas de doute, n'utilisez pas Smart CLI ou FlexConfig.

Les rubriques suivantes expliquent ces fonctionnalités plus en détail.

Utilisation conseillée pour Smart CLI et FlexConfig

Il y a deux utilisations principales recommandées pour FlexConfig :

- Vous passez d'ASA à Cisco Firewall Threat Defense, et vous utilisez (et devez continuer à utiliser) des fonctions compatibles qui ne sont pas directement prises en charge par Firepower Device Manager. Dans ce cas, utilisez la commande **show running-config** sur l'ASA pour afficher la configuration de la fonctionnalité et créez vos objets FlexConfig pour la mettre en œuvre. Vérifiez en comparant la sortie **show running-config** sur les deux périphériques.
- Vous utilisez Cisco Firewall Threat Defense, mais il y a un paramètre ou une fonctionnalité que vous devez configurer. Par exemple, le centre d'assistance technique de Cisco vous indique qu'un paramètre particulier devrait résoudre un problème précis que vous rencontrez. Pour les fonctionnalités complexes, utilisez un appareil de laboratoire pour tester FlexConfig et vérifiez que vous obtenez le comportement attendu.

Avant d'essayer de recréer une configuration ASA, déterminez d'abord si vous pouvez configurer une fonctionnalité équivalente dans les politiques standard. Par exemple, la politique de contrôle d'accès comprend la détection et la prévention des intrusions, HTTP et d'autres types d'inspection de protocole, le filtrage d'URL, le filtrage d'applications et le contrôle d'accès, que l'ASA met en œuvre à l'aide de fonctionnalités distinctes. Étant donné que de nombreuses fonctionnalités ne sont pas configurées à l'aide des commandes CLI, vous ne verrez pas toutes les politiques représentés dans la sortie de **show running-config**.

Remarque Gardez à tout moment à l'esprit qu'il n'y a pas de recouvrement direct entre ASA et Cisco Firewall Threat Defense. N'essayez pas de recréer complètement une configuration ASA sur un périphérique Cisco Firewall Threat Defense. Vous devez tester attentivement toute fonctionnalité que vous configurez à l'aide de FlexConfig.

Commandes CLI dans les objets Smart CLI et les objets FlexConfig

Le Cisco Firewall Threat Defense utilise des commandes de configuration ASA pour configurer certaines fonctionnalités. Bien que toutes les fonctionnalités de l'ASA ne soient pas compatibles avec le Cisco Firewall Threat Defense, certaines fonctionnalités peuvent fonctionner sur le Cisco Firewall Threat Defense Firepower

Device Manager, mais que vous ne pouvez pas configurer dans les politiques. Vous pouvez utiliser Smart CLI et les objets FlexConfig pour préciser les commandes CLI requises pour configurer ces fonctionnalités.

Si vous décidez d'utiliser Smart CLI ou FlexConfig pour configurer manuellement une fonctionnalité, vous êtes responsable de connaître et de mettre en œuvre les commandes selon la syntaxe appropriée. FlexConfig ne valide pas la syntaxe des commandes CLI. Pour plus d'informations sur la syntaxe appropriée et la configuration des commandes CLI, utilisez la documentation d'ASA comme référence :

- Les guides de configuration de l'interface de ligne de commande ASA expliquent comment configurer une fonctionnalité. Vous trouverez les guides à l'adresse http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- Les références de commande ASA fournissent des informations supplémentaires triées par nom de commande. Vous trouverez les références à l'adresse http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

Les rubriques suivantes expliquent plus en détail les commandes de configuration.

Incidence des mises à niveau logicielles sur la politique FlexConfig

Chaque nouvelle version du logiciel Cisco Firewall Threat Defense ajoute une prise en charge pour la configuration des fonctionnalités dans Firepower Device Manager. Parfois, ces nouvelles fonctionnalités peuvent chevaucher des fonctionnalités que vous avez précédemment configurées à l'aide de FlexConfig.

Après la mise à niveau, vous devez examiner la politique et les objets FlexConfig. Si l'un d'eux contient des commandes qui sont devenues interdites en raison de l'ajout d'une prise en charge dans Firepower Device Manager ou de l'interface de ligne de commande Smart, les icônes dans la liste des objets et les messages indiquent le problème. Veuillez prendre le temps de refaire votre configuration. Utilisez la liste des commandes interdites pour déterminer où les commandes doivent maintenant être configurées.

Le système ne vous empêchera pas de déployer des modifications lorsque les objets FlexConfig associés à la politique FlexConfig contiennent des commandes nouvellement interdites. Cependant, vous ne pourrez pas créer de nouveaux objets Smart CLI tant que vous n'aurez pas résolu tous les problèmes observés dans la politique FlexConfig.

Vous pouvez simplement supprimer les objets problématiques de la politique FlexConfig, car la restriction s'applique uniquement aux objets que vous déployez activement dans la configuration du périphérique. Ainsi, vous pouvez supprimer les objets, puis les utiliser comme référence lorsque vous créez l'interface de ligne de commande Smart correspondante ou avez intégré la configuration Firepower Device Manager. Une fois que vous êtes satisfait de la nouvelle configuration, vous pouvez simplement supprimer les objets. Si les objets supprimés contiennent des éléments non interdits, vous pouvez les modifier pour supprimer les commandes non prises en charge, puis rassocier les objets à la politique FlexConfig.

Déterminer la version du logiciel du périphérique ASA et la configuration actuelle de la CLI

Comme le système utilise les commandes du logiciel ASA pour configurer certaines fonctionnalités, vous devez déterminer la version actuelle de l'ASA utilisée dans le logiciel s'exécutant sur le périphérique Cisco Firewall Threat Defense. Ce numéro de version indique quels guides de configuration de CLI ASA utiliser pour obtenir des instructions sur la configuration d'une fonctionnalité. Vous devez également examiner la configuration actuelle basée sur l'interface de ligne de commande et la comparer à la configuration ASA que vous souhaitez mettre en œuvre.

Gardez à l'esprit que toute configuration ASA sera très différente d'une configuration Cisco Firewall Threat Defense. De nombreuses politiques Cisco Firewall Threat Defense sont configurées en dehors de la CLI, de

sorte que vous ne pouvez pas voir la configuration en regardant les commandes. N'essayez pas de créer de correspondance un à un entre une configuration ASA et Cisco Firewall Threat Defense.

Pour afficher ces informations, soit ouvrez la console CLI dans le Firepower Device Manager, soit établissez une connexion SSH à l'interface de gestion du périphérique et saisissez les commandes suivantes :

- **show version system** et recherchez le numéro de la version logicielle du périphérique de sécurité adaptatif Cisco.
- **show running-config** pour afficher la configuration actuelle de l'interface de ligne de commande.
- **show running-config all** pour inclure toutes les commandes par défaut dans la configuration actuelle de l'interface de ligne de commande.

Commandes CLI interdites

Le but de Smart CLI et FlexConfig est de configurer les fonctionnalités disponibles sur les périphériques ASA que vous ne pouvez pas configurer sur les périphériques Cisco Firewall Threat Defense à l'aide du Firepower Device Manager.

Ainsi, vous ne pouvez pas configurer les fonctionnalités ASA qui ont des équivalents dans Firepower Device Manager. Le tableau suivant répertorie certaines de ces zones de commande interdites. Cette liste contient de nombreuses commandes parentes qui passent en mode de configuration. L'interdiction de la commande parente entraîne également l'interdiction des commandes enfants. lle comprend également la version **no** des commandes et les commandes **clear** associées.

L'éditeur d'objet FlexConfig vous empêche d'inclure ces commandes dans l'objet. Cette liste ne s'applique pas aux modèles Smart CLI, car ils comprennent uniquement les commandes que vous pouvez configurer validement.

Commandes CLI interdites	Commentaires
aaa	Utilisez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
aaa-server	Utilisez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
access-list	Partiellement bloqué. • Vous pouvez créer des listes d'accès **ethertype**. • Vous ne pouvez pas créer de listes d'accès **extended** et **standard**. Créez ces ACL à l'aide des objets Liste d'accès étendue ou Liste d'accès standard de Smart CLI. Vous pouvez ensuite les utiliser sur les commandes prises en charge par FlexConfig qui font référence à la liste de contrôle d'accès par nom d'objet, comme **match access-list** avec une liste de contrôle d'accès étendue pour les classes de trafic des politiques de service. • Vous ne pouvez pas créer de listes d'accès **advanced**, que le système utilise avec la commande **access-group**. Au lieu de cela, utilisez **Policies (Politiques)** > **Access Control (Contrôle d'accès)** pour configurer les critères d'accès. • Vous ne pouvez pas créer de listes d'accès **webtype**.

Commandes CLI interdites	Commentaires
anyconnect-custom-data	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer client AnyConnect.
asdm	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense.
as-path	Créez des objets de chemin AS pour Smart CLI et utilisez-les dans un objet BGP Smart CLI pour configurer un filtre de chemin de système autonome.
attribute	—
auth-prompt	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense.
boot	—
call-home	—
captive-portal	Utilisez **Policies (Politiques)** > **Identity (Identité** pour configurer le portail captif utilisé pour l'authentification active.
clear	—
client-update	—
clock	Utilisez **Device (Périphérique)** > **System Settings (Paramètres du système)** > **NTP** pour configurer l'heure du système.
cluster	—
command-alias	—
community-list	Créez des objets de liste de communauté étendue ou de liste de communauté standard Smart CLI et utilisez-les dans un objet BGP Smart CLI pour configurer un filtre de liste de communauté.
compression	—
configure	—
crypto	Sur la page **Objects** (Objets), utilisez **Certificates** (Certificats), **IKE Policies** (Politiques IKE), et **IPSec Proposals** (Propositions IPSec).
ddns	Utilisez **Device (Périphérique)** > **System Settings (Paramètres du système)** > **DDNS Service (Service DDNS)** pour configurer le DNS dynamique.
dhcp-client	—
dhcpd	Utilisez **Device (Périphérique)** > **System Settings (Paramètres du système)** > **DHCP Server (Serveur DHCP)**. Cependant, la commande **dhcpd option** est autorisée.

Configuration avancée

Commandes CLI interdites	Commentaires
dhcprelay	Utilisez plutôt la ressource dhcprelayservices dans l'API de défense contre les menaces.
dns	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
dns-group	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
domain-name	**Objects (Objets)** > **DNS Groups (Groupes DNS)** : vous pouvez maintenant configurer des groupes DNS à l'aide de **Device (Périphérique)** > **System Settings (Paramètres système)** > **DNS Server (Serveur DNS)**.
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—
event	—
failover	—
fips	—
firewall	Firewall Device Manager ne prend en charge que le mode de pare-feu routé.
hostname	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **Hostname (Nom d'hôte)**.
hpm	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense.
http	Utilisez l'onglet **Data Interfaces** (Interfaces de données) sur **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Access (Accès à l'interface de gestion**.
inline-set	—

Commandes CLI interdites	Commentaires
interface pour les BVI, l'interface de gestion, Ethernet, GigabitEthernet et les sous-interfaces.	Partiellement bloqué. Configurez les interfaces physiques, les sous-interfaces et les interfaces virtuelles de pont sur la page **Device (Périphérique)** > **Interfaces**. Vous pouvez ensuite configurer des options supplémentaires à l'aide de FlexConfig. Cependant, les commandes en mode **interface** suivantes sont interdites pour ces types d'interface. **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
interface pour **vni**, **redundant**, **tunnel**	Configurez les interfaces sur la page **Device (Périphérique)** > **Interfaces**. Firewall Device Manager ne prend pas en charge ces types d'interface.
ip audit	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense. Appliquez plutôt les politiques d'intrusion à l'aide des règles de contrôle d'accès.
ip-client	Pour configurer le système afin qu'il utilise les interfaces de données comme passerelle de gestion, utilisez **Device (Périphérique)** > **ystem Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.
ip local pool	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer des ensembles d'adresses.
ipsec	—
ipv6	Créez des objets de liste de préfixes IPv6 Smart CLI et utilisez-les dans un objet Smart CLI BGP pour configurer le filtrage de liste de préfixes pour IPv6.
ipv6-vpn-addr-assign	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** pour configurer des ensembles d'adresses.
isakmp	Utilisez **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.

Commandes CLI interdites	Commentaires
jumbo-frame	Le système active automatiquement la prise en charge des trames étendues si vous augmentez la MTU de n'importe quelle interface au-delà de la valeur par défaut de 1 500.
ldap	—
license-server	Utilisez **Device (Périphérique)** > **Smart License (Licence Smart)**.
logging	Utilisez **Objects (Objets)** > **Syslog Servers (Serveurs Syslog)** et **Device (Périphérique)** > **System Settings (Paramètres système)** > **Logging Settings (Paramètres de journalisation)**. Cependant, vous pouvez configurer la commande **logging history** dans FlexConfig.
management-access	—
migrate	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)** pour activer la prise en charge d'IKEv2.
mode	Firewall Device Manager ne prend en charge que le mode à contexte unique.
mount	—
mtu	Configurez la MTU par interface sur **Device (Périphérique)** > **Interfaces**.
nat	Utilisez **Policies (Politiques)** > **NAT**.
ngips	—
ntp	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **NTP**
object-group network **object network**	Utilisez **Objects (Objets)** > **Network (Réseau)**. Vous ne pouvez pas créer d'objets réseau ou de groupes dans FlexConfig, mais vous pouvez utiliser, en tant que variables, les objets réseau et groupes définis dans le gestionnaire d'objets à l'intérieur du modèle.
object service |natorigsvc **object service |natmappedsvc**	La commande **object service** st généralement autorisée, mais vous ne pouvez pas modifier les objets internes nommés |natorigsvc ou |natmappedsvc. Dans ces noms, la barre verticale est intentionnelle et il s'agit du premier caractère des noms d'objets restreints.
passwd **password**	—
password-policy	—

Commandes CLI interdites	Commentaires
policy-list	Créez des objets de liste des politiques Smart CLI et utilisez-les dans un objet Smart CLI BGP pour configurer une liste des politiques.
policy-map sous-commandes	Vous ne pouvez pas configurer les commandes suivantes dans une liste des politiques. **priority** **police** **match tunnel-group**
prefix-list	Créer des objets de liste de préfixes IPv4 Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer le filtrage des listes de préfixes IPv4.
priority-queue	—
privilege	—
reload	Vous ne pouvez pas planifier de rechargements. Le système n'utilise pas la commande **reload** pour redémarrer le système, il utilise la commande **reboot**.
rest-api	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense. L'API REST est toujours installée et activée.
route	Utilisez **Device (Périphérique)** > **Routing (Routage)** pour configurer les routes statiques.
route-map	Créer des objets de carte de routage Smart CLI et les utiliser dans un objet Smart CLI OSPF ou BGP pour configurer des cartes de routage.
router bgp	Utilisez les modèles Smart CLI pour BGP.
router eigrp	Utilisez les modèles Smart CLI pour EIGRP.
router ospf	Utilisez les modèles Smart CLI pour OSPF.
scansafe	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense. Configurez plutôt le filtrage d'URL dans les règles de contrôle d'accès.
setup	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense.
sla	—
snmp-server	Utilisez les ressources SNMP de l'API FTP pour configurer SNMP.
ssh	Utilisez l'onglet **Data Interfaces** (Interfaces de données) sur **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Access (Accès à l'interface de gestion**.

Commandes CLI interdites	Commentaires
ssl	Utilisez **Device (Périphérique)** > **System Settings (Paramètres système)** > **SSL Settings (Paramètres SSL)**
telnet	Firewall Threat Defense ne prend pas en charge les connexions Telnet. Utilisez SSH au lieu de Telnet pour accéder à l'interface de ligne de commande du périphérique.
time-range	—
tunnel-group	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.
tunnel-group-map	Utilisez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** et **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)**.
user-identity	Utiliser **Policies (Politiques)** > **Identity (Identité)**.
username	Pour créer des utilisateurs d'interface de ligne de commande, ouvrez une session SSH ou de console sur le périphérique et utilisez les commandes **configure user**.
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	Cette fonctionnalité ne s'applique pas à un système Cisco Firewall Threat Defense.

Modèles Smart CLI

Le tableau suivant explique les modèles d'interface de ligne de commande Smart en fonction de la fonctionnalité.

Remarque Vous configurez également OSPF et BGP à l'aide des modèles Smart CLI. Cependant, ces modèles sont disponibles dans la page **Device (Périphérique)** > **Routing (Routage)** plutôt que dans la page de configuration avancée.

Fonctionnalités	Modèles	Description
Objets : AS Path	ASPath	Créez des objets ASPath à utiliser avec des objets de protocole de routage.
Objets : Access List (liste d'accès)	Liste d'accès étendue Liste d'accès standard	Créez des listes de contrôle d'accès étendues ou standard à utiliser avec des objets de routage. Vous pouvez également faire référence à ces objets par nom à partir des objets FlexConfig qui configurent les commandes autorisées qui utilisent les listes de contrôle d'accès.
Objets : Community List (liste de communautés)	Liste de communauté élargie Liste de communauté standard	Créez des listes de communauté étendues ou standard à utiliser avec des objets de routage.
Objets : Prefix List (liste de préfixes)	Liste des préfixes IPV4 Liste des préfixes IPV6	Créez des listes de préfixes IPv4 ou IPv6 à utiliser avec des objets de routage.
Objets : Policy List (liste de politiques)	Liste des stratégies	Créez des listes de politiques à utiliser avec des objets de routage.
Objets : Route Map (Carte de routage)	Carte de routage	Créez des cartes de routage à utiliser avec des objets de routage.

Lignes directrices et limites de Smart CLI et FlexConfig

Veuillez garder les éléments suivants à l'esprit lors de la configuration des fonctionnalités par le biais de l'interface de ligne de commande Smart ou de FlexConfig.

- Les commandes définies dans les objets FlexConfig sont déployées après toutes les commandes pour les fonctionnalités définies par Firepower Device Manager, y compris Smart CLI. Ainsi, vous pouvez dépendre des objets, des interfaces, etc. configurés avant que ces commandes ne soient transmises au périphérique. Si vous devez utiliser un élément déployé par FlexConfig dans un modèle d'interface de ligne de commande Smart, créez et déployez FlexConfig avant de créer et de déployer le modèle d'interface de ligne de commande Smart. Par exemple, si vous souhaitez utiliser le modèle d'interface de ligne de commande Smart OSPF pour redistribuer les routes EIGRP, utilisez d'abord FlexConfig pour configurer EIGRP, puis créez le modèle d'interface de ligne de commande Smart OSPF.
- Si vous souhaitez supprimer une fonctionnalité ou une partie d'une fonctionnalité que vous avez configurée par le biais de FlexConfig, mais qu'un modèle d'interface de ligne de commande Smart fait référence à

cette fonctionnalité, vous devez d'abord supprimer les commandes du modèle d'interface de ligne de commande Smart qui utilisent la fonctionnalité. Ensuite, déployez la configuration afin que la fonctionnalité configurée via Smart CLI n'y fasse plus référence. Vous pouvez ensuite supprimer la fonctionnalité de FlexConfig, puis redéployer la configuration afin de l'éliminer complètement.

Configuration des objets Smart CLI

Les objets Smart CLI définissent des fonctionnalités qui ne peuvent pas être configurées ailleurs dans le Firepower Device Manager. Les objets Smart CLI fournissent un niveau d'accompagnement pour configurer une fonctionnalité. Pour une fonctionnalité (modèle) donnée, toutes les commandes possibles sont préchargées et les variables que vous saisissez sont validées. Ainsi, bien que vous utilisiez toujours les commandes CLI pour configurer une fonctionnalité, les objets Smart CLI ne sont pas aussi libres que les objets FlexConfig.

Bien que les modèles Smart CLI fournissent un certain encadrement, vous devez toujours lire les guides de configuration ASA et les références de commande pour comprendre l'utilisation des commandes afin de choisir des valeurs qui fonctionnent correctement pour votre réseau. Idéalement, vous avez déjà une configuration ASA à partir de laquelle travailler et vous n'avez qu'à créer la même séquence de commandes dans l'objet Smart CLI.

Les objets Smart CLI sont regroupés selon le domaine de fonctionnalité.

Remarque Tous les objets Smart CLI que vous définissez sont déployés. Contrairement à FlexConfig, vous ne pouvez pas créer plusieurs objets Smart CLI, puis sélectionner lequel déployer. Créez des objets Smart CLI uniquement pour les fonctionnalités que vous souhaitez configurer.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur la zone de fonctionnalité appropriée sous **Smart CLI** dans la table des matières de Advanced Configuration (Configuration avancée).

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Entrez un nom pour l'objet et, facultativement, une description.

Étape 5 Sélectionnez le **CLI Template** (Modèle CLI) pour la fonctionnalité que vous configurez.

Le système charge le modèle de commande dans la fenêtre **Template** (Modèle). Au départ, seules les commandes requises sont affichées. Il s'agit de la configuration minimale requise pour le modèle.

Étape 6 Remplissez les variables et ajoutez des commandes selon les besoins dans le modèle.

Idéalement, vous utilisez une configuration existante provenant d'un appareil ASA ou Firewall Threat Defense (géré par Firewall Management Center). Avec une configuration en main, vous devez simplement rendre le modèle conforme à celle-ci, en modifiant des variables telles que les adresses IP et les noms d'interfaces en fonction de l'emplacement de cet appareil spécifique dans votre réseau.

Voici quelques conseils pour remplir le modèle :

- Pour sélectionner une valeur pour une variable, cliquez sur la variable et saisissez la valeur appropriée ou sélectionnez-la dans une liste (dans le cas des valeurs énumérées). Le déplacement du curseur sur les variables qui nécessitent une saisie affiche les valeurs valides pour l'option, comme une plage de nombres. Dans certains cas, la valeur conseillée est mentionnée.

  Par exemple, dans le modèle OSPF, la commande requise **router ospf** *process-id* affiche « Process ID (ID de processus) (1-65535) » au survol de la souris, et lorsque vous cliquez sur *process-id*, le champ est mis en surbrillance. Tapez simplement le numéro que vous souhaitez.

- Lorsque vous sélectionnez une option pour une variable, s'il existe d'autres commandes possibles pour configurer l'option, celles-ci sont automatiquement affichées et désactivées ou activées, le cas échéant. Surveillez ces commandes supplémentaires.

- Utilisez le lien **Show**/**Hide Disabled** (Afficher/Masquer désactivés) au-dessus du modèle pour contrôler l'affichage. Les commandes désactivées ne seront pas configurées, mais vous devez les afficher pour les configurer. Pour voir le modèle complet, cliquez sur le lien **Show Disabled** (Afficher désactivés) au-dessus du modèle. Pour voir uniquement les commandes qui seront configurées, cliquez sur le lien **Hide Disabled (Masquer désactivés)** au-dessus du tableau.

- Pour effacer toutes vos modifications depuis le dernier enregistrement de l'objet, cliquez sur le lien **Reset** (Réinitialiser) au-dessus du modèle.

- Pour activer une commande facultative, cliquez sur le bouton **+** à gauche du numéro de ligne.

- Pour désactiver une commande facultative, cliquez sur le bouton **-** à gauche du numéro de ligne. Si vous avez modifié la ligne, vos modifications ne sont pas supprimées.

- Pour dupliquer une commande, cliquez sur le bouton Options **...** et sélectionnez **Duplicate** (Dupliquer). Vous êtes autorisé à dupliquer les commandes uniquement s'il est valide d'entrer la commande plus d'une fois.

- Pour supprimer une commande en double, cliquez sur le bouton Options **...** et sélectionnez **Delete (Supprimer)**. Vous ne pouvez pas supprimer les commandes qui font partie du modèle de base.

Étape 7 Cliquez sur **OK**.

Configurer la politique FlexConfig

La politique FlexConfig est simplement une liste des objets FlexConfig que vous souhaitez déployer dans la configuration du périphérique. Seuls les objets inclus dans la politique sont déployés, tous les autres sont simplement définis et inutilisés.

Les commandes définies dans les objets FlexConfig sont déployées après toutes les commandes pour les fonctionnalités définies par Firepower Device Manager, y compris Smart CLI. Ainsi, vous pouvez dépendre des objets, des interfaces, etc. configurés avant que ces commandes ne soient transmises au périphérique. Si vous devez utiliser un élément déployé par FlexConfig dans un modèle d'interface de ligne de commande

Smart, créez et déployez FlexConfig avant de créer et de déployer le modèle d'interface de ligne de commande Smart. Par exemple, si vous souhaitez utiliser le modèle d'interface de ligne de commande Smart OSPF pour redistribuer les routes EIGRP, utilisez d'abord FlexConfig pour configurer EIGRP, puis créez le modèle d'interface de ligne de commande Smart OSPF.

Remarque S'il existe un modèle d'interface de ligne de commande Smart pour une fonctionnalité, vous ne pouvez pas la configurer à l'aide de FlexConfig. Vous devez utiliser l'objet Smart CLI.

Avant de commencer

Créer les objets FlexConfig. Consultez les rubriques suivantes:

- Configurer les objets FlexConfig, à la page 15
- Création de variables dans un objet FlexConfig, à la page 17
- Configuration des objets de clé secrète, à la page 24

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Policy (Politique FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Gérer la liste des objets dans la **Group List** (Liste des groupes).

- Pour créer un objet, cliquez sur le bouton **+**. Si l'objet n'existe pas encore, cliquez sur **Create New FlexConfig Object** (Créer un nouvel objet FlexConfig) pour le définir.
- Pour supprimer un objet, cliquez sur le bouton **X** à droite de l'entrée de l'objet.

Remarque
Nous recommandons que chaque objet soit complètement autonome et ne dépende pas de la configuration définie dans un autre objet FlexConfig. Cela vous permet d'ajouter ou de supprimer des objets sans affecter les autres objets.

Étape 4 Évaluez les commandes proposées dans le volet **Preview** (Aperçu).

Vous pouvez cliquer sur le bouton **Expand** (Développer) (puis **Collapse** (Réduire)) pour élargir l'écran afin de pouvoir voir les commandes longues plus clairement.

L'aperçu évalue les variables et produit les commandes exactes qui seront émises. Assurez-vous que ces commandes sont correctes et valides. Vous êtes responsable de vous assurer que les commandes n'entraîneront pas d'erreurs ou de mauvaises configurations qui rendront l'appareil inutilisable.

Mise en garde
Le système ne valide pas les commandes. Il vous est possible de déployer des commandes non valides et même potentiellement destructrices. Examinez l'aperçu très attentivement avant de déployer les modifications.

Étape 5 Cliquez sur **Save** (enregistrer).

Prochaine étape

Après avoir modifié la politique FlexConfig, examinez attentivement les résultats du prochain déploiement. S'il y a des erreurs, corrigez l'interface de ligne de commande dans l'objet. Consultez Dépannage de la politique FlexConfig, à la page 25.

Configurer les objets FlexConfig

Un objet FlexConfig contient les commandes ASA nécessaires pour configurer une fonctionnalité particulière que vous ne pouvez pas configurer autrement à l'aide de Firepower Device Manager. Vous êtes responsable de vous assurer de saisir la bonne séquence de commandes, sans faute de frappe. Le système ne valide pas le contenu des objets FlexConfig.

Nous vous recommandons de créer des objets distincts pour chaque fonctionnalité générale que vous souhaitez configurer. Par exemple, si vous souhaitez définir des bannières et configurer le protocole de routage RIP, utilisez 2 objets distincts. L'isolation des fonctionnalités dans des objets distincts vous permet de sélectionner plus facilement les objets à déployer et facilite le dépannage.

Remarque N'incluez pas les commandes **enable** et **configure terminal**. Le système passe automatiquement en mode adéquat pour les commandes de configuration.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Entrez un nom pour l'objet et, facultativement, une description.

Étape 5 Dans la section **Variables**, créez les variables que vous souhaitez utiliser dans le corps de l'objet.

Les seules variables que vous devez créer sont celles qui pointent vers des objets définis dans le Firepower Device Manager, en particulier les types de variables de réseau, de port et de clé secrète, ou la variable d'interface, qui pointe vers une interface nommée. Pour les autres types de variables, vous pouvez simplement saisir les valeurs dans le corps de l'objet.

Pour des informations détaillées sur la création et l'utilisation des variables, consultez Création de variables dans un objet FlexConfig, à la page 17.

Étape 6 Dans la section **Template** (Modèle), saisissez les commandes ASA requises pour configurer la fonctionnalité.

Vous devez entrer les commandes dans le bon ordre pour configurer la fonctionnalité. Utilisez les guides de configuration de l'interface de ligne de commande ASA pour apprendre comment saisir les commandes. Idéalement, vous devriez avoir un fichier de configuration prétesté provenant d'un ASA ou d'un autre périphérique Cisco Firewall Threat Defense que vous pouvez utiliser comme référence.

Vous pouvez également utiliser la notation Mustache pour faire référence et traiter les variables. Pour de plus amples renseignements, voir Référence aux variables FlexConfig et récupération de leurs valeurs, à la page 18.

Voici quelques conseils pour la création du corps de l'objet :

- Pour ajouter des lignes, placez le curseur à la fin d'une ligne et appuyez sur Entrée.
- Pour utiliser une variable, saisissez le nom de la variable entre doubles accolades : {{*variable_name*}}. Pour les variables qui font référence à des objets, vous devez inclure l'attribut dont vous récupérez la valeur : {{*variable_name.attribut*}}. Les attributs disponibles varient selon le type d'objet. Pour obtenir des renseignements complets, consultez Références de variable : {{variable}} ou {{{variable}}}, à la page 18.
- Pour utiliser un objet Smart CLI, saisissez le nom de l'objet. Si vous devez faire référence à un processus de routage configuré dans Smart CLI, saisissez l'identifiant du processus. Consultez Référence aux objets Smart CLI dans un objet FlexConfig, à la page 23.
- Cliquez sur le lien **Expand/Collapse** (Développer/Réduire) au-dessus du corps du modèle pour agrandir ou réduire ce dernier.
- Cliquez sur le lien **Reset** (Réinitialiser) pour effacer toutes les modifications que vous avez apportées depuis le dernier enregistrement de l'objet.

Étape 7 Dans la section **Negate Template** (Modèle de négation), saisissez les commandes nécessaires pour supprimer ou inverser les commandes configurées dans le corps de l'objet.

La section de négation est très importante et sert deux objectifs :

- Cela simplifie le déploiement. Avant de redéployer les commandes dans le corps, le système utilise ces commandes pour d'abord effacer ou annuler la configuration. Cela garantit un déploiement propre.
- Si vous décidez de supprimer la fonctionnalité en supprimant l'objet de la politique FlexConfig, le système utilise ces commandes pour supprimer les commandes du périphérique.

Si vous décidez de supprimer la fonctionnalité en retirant l'objet de la FlexConfig Policy (Politique FlexConfig), le système utilise ces commandes pour supprimer les commandes du périphérique. Cela prendra plus de temps pour le déploiement et perturbera le trafic. Assurez-vous que vous disposez de toutes et uniquement des commandes nécessaires pour annuler la configuration définie dans le corps de l'objet. Bien que les commandes d'annulation soient généralement sous la forme **no** ou **clear** des commandes du modèle, si vous désactivez une fonctionnalité qui était déjà activée, la commande « negate » (annuler) est en fait la forme positive de la commande, celle qui active la fonctionnalité.

Utilisez les guides de configuration ASA et la référence de commande pour déterminer les commandes appropriées. Parfois, vous pouvez annuler une configuration avec une seule commande. Par exemple, dans un objet qui configure RIP, une simple commande **no router rip** supprime l'ensemble de la configuration **router rip**, y compris les sous-commandes.

De même, si vous avez saisi plusieurs commandes **banner login** pour créer une bannière multilignes, une seule commande **no banner login** annule l'ensemble de la bannière de connexion.

Si votre modèle crée plusieurs objets imbriqués, le modèle d'annulation doit supprimer les objets dans l'ordre inverse, pour supprimer d'abord les références aux objets avant de supprimer les objets. Par exemple, si vous créez d'abord une liste de contrôle d'accès, puis y faites référence dans une classe de trafic, puis faites référence à la classe de trafic dans une carte de politiques et activez finalement la carte de politiques à l'aide d'une politique de service, le modèle d'annulation doit d'abord annuler la configuration en supprimant la politique de service, puis la carte de politiques, puis la classe de trafic et finalement l'ACL.

Étape 8 Cliquez sur **OK**.

Prochaine étape

La simple création d'un objet FlexConfig ne suffit pas pour le déployer. Vous devez ajouter l'objet à la politique FlexConfig. Seuls ces objets de la politique FlexConfig sont déployés. Cela vous permet d'affiner vos objets FlexConfig et d'en avoir certains prêts pour des utilisations spéciales, sans qu'ils soient tous automatiquement déployés. Consultez Configurer la politique FlexConfig, à la page 13.

Création de variables dans un objet FlexConfig

Les variables que vous utilisez dans un objet FlexConfig sont définies dans l'objet lui-même. Il n'y a pas de liste distincte de variables. Ainsi, vous ne pouvez pas définir une variable puis l'utiliser dans des objets FlexConfig distincts.

Les variables fournissent ces principaux avantages :

- Ils permettent de pointer vers des objets définis à l'aide de Firepower Device Manager. Cela inclut les objets de réseau, de port et de clé secrète.
- Ils isolent les valeurs qui pourraient changer à partir du corps de l'objet. Ainsi, si vous devez modifier une valeur, vous modifiez simplement la variable et vous n'avez pas besoin de modifier le corps de l'objet. Cela peut être particulièrement utile si vous devez faire référence à l'objet dans plusieurs lignes de commande.

Cette procédure explique le processus d'ajout de variables à un objet FlexConfig.

Procédure

Étape 1 Modifier ou créer un objet FlexConfig à partir de la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Consultez Configurer les objets FlexConfig, à la page 15.

Étape 2 Effectuez l'une des opérations suivantes dans la section **Variables** :

- Pour ajouter une variable, cliquez sur le bouton **+** (ou cliquez sur **Add Variable** (Ajouter une variable) s'il n'y en a aucune encore définie).
- Pour modifier une variable, cliquez sur l'icône de modification ( ) en regard de la variable.

Pour supprimer une variable, cliquez sur l'icône de la corbeille ( ) pour cette variable. Assurez-vous de supprimer toutes les références à cette variable dans le corps du modèle.

Étape 3 Saisissez un nom pour la variable et, au besoin, une description.

Étape 4 Sélectionnez un **type** de données pour la variable, puis saisissez ou sélectionnez la valeur.

Vous pouvez créer les types de variables suivants. Choisissez un type qui correspond aux exigences de données des commandes dans lesquelles vous utiliserez la variable.

- **Chaîne** : une chaîne de texte. Par exemple, les noms d'hôte, les noms d'utilisateur, etc.
- **Numérique** : un nombre entier. N'incluez pas de virgules, de décimales, de signes (comme le signe négatif) ou la notation hexadécimale. Pour les nombres non entiers, utilisez une variable de chaîne.
- **Booléen** : une valeur logique vraie ou fausse. Sélectionnez Vrai ou Faux.
- **Objet réseau** : un objet réseau ou un groupe défini sur la page Objets. Sélectionnez l'objet réseau ou le groupe.
- **Objet de port** : un objet de port TCP ou UDP défini sur la page Objets. Sélectionnez l'objet de port. Vous ne pouvez pas sélectionner de groupes ou d'objets pour d'autres protocoles.
- **Interface** : une interface nommée définie sur la page Device (Périphérique) > Interfaces. Sélectionnez l'interface. Vous ne pouvez pas sélectionner d'interfaces qui n'ont pas de nom.
- **Adresse IP** : une adresse IP IPv4 ou IPv6 unique, sans masque réseau ni longueur de préfixe.
- **Clé secrète** : un objet de clé secrète défini pour FlexConfig. Sélectionnez l'objet. Pour en savoir plus sur la création d'objets de clé secrète, consultez Configuration des objets de clé secrète, à la page 24.

Étape 5 Cliquez sur **Add** (Ajouter) ou **Save** (Enregistrer) dans la boîte de dialogue Variable.

Vous pouvez maintenant utiliser la variable dans le corps de l'objet FlexConfig. La façon dont vous faites référence à la variable diffère en fonction du type de variable. Pour plus de détails sur l'utilisation de ces variables, consultez les rubriques suivantes :

- Références de variable : {{variable}} ou {{{variable}}}, à la page 18
- Sections {{#key}} {{/key}} et sections inverses {{^key}} {{/key}}, à la page 21

Étape 6 Cliquez sur **OK** dans la boîte de dialogue de l'objet FlexConfig.

Référence aux variables FlexConfig et récupération de leurs valeurs

FlexConfig utilise Mustache comme langue de modèle, mais la prise en charge est limitée aux fonctionnalités expliquées dans les sections suivantes. Utilisez ces fonctionnalités pour faire référence aux variables, récupérer leurs valeurs et les traiter.

Références de variable : {{variable}} ou {{{variable}}}

Pour faire référence à une variable, que vous définissez dans un objet FlexConfig, utilisez la notation suivante :

{{*variable_name*}}

Ou :

{{{*variable_name*}}}

Cela est suffisant pour les variables simples qui sont des valeurs uniques, qui comprennent les variables des types suivants : **Numeric** (Numérique), **String** (Chaîne), **Boolean** (Booléen) et **IP**. Utilisez des accolades triples si la variable contient des caractères spéciaux tels que &. Sinon, vous pouvez toujours utiliser des accolades triples pour toutes les variables.

Toutefois, pour les variables qui pointent vers des éléments modélisés comme des objets dans la base de données de configuration, vous devez utiliser la notation par points et inclure le nom de l'attribut de l'objet que vous souhaitez récupérer. Vous pouvez trouver ces noms d'attribut en examinant les modèles dans l'outil API Explorer (Explorateur d'API) pour le type d'objet associé. Vous devez utiliser la notation suivante pour utiliser les variables des types suivants : **Secret**, **Network** (Réseau), **Port** et **Interface**.

{{*variable_name.attribute*}}

Par exemple, pour récupérer l'adresse d'une variable réseau nommée net-object1 (qui pointe vers un objet réseau, et non un groupe réseau), vous utiliserez :

{{net-object1.value}}

Si vous essayez de récupérer une valeur d'attribut d'un objet dans un objet, vous devez utiliser une série d'attributs séparés par des points pour accéder à la valeur souhaitée. Par exemple, les adresses IP d'une interface sont modélisées comme des sous-objets, nommés ipv4 et ipv6, dans l'objet de l'interface. Ainsi, pour récupérer l'adresse IPv4 et le masque de sous-réseau d'une variable d'interface nommée int-inside (qui pointe vers l'interface interne), vous utiliserez :

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

Remarque Pour ouvrir l'explorateur d'API, cliquez sur le bouton more options (plus d'options) (⋮) et choisissez **API Explorer** (Explorateur d'API).

Le tableau suivant répertorie les types de variables, la façon de les référencer et, pour les objets, le nom du modèle API et les références les plus susceptibles d'être utilisées.

Type de variable	Modèles de référence	Description

Booléen
(variable simple)
	Variable :
	{{*variable_name*}}
	Section :
	`{{#variable_name}}`
	`commands`
	`{{/variable_name}}`
	Section inverse :
	`{{^variable_name}}`
	`commands`
	`{{/variable_name}}`
		Une valeur logique vrai/faux. L'objectif principal des variables booléennes est de contrôler des sections ou des sections inverses. Vous pouvez modifier la valeur d'une variable booléenne pour activer ou désactiver une section de commandes, par exemple, si vous devez activer une fonctionnalité périodiquement ou dans des circonstances spéciales uniquement.
		Certains objets ont également des attributs booléens dans leurs modèles, que vous pouvez utiliser pour fournir le traitement facultatif d'une section.

Type de variable	Modèles de référence	Description

Interface
(variable d'objet : le modèle API est Interface)
	Variable :
	{{*variable_name*.*attribute*}}
	Section :
	`{{#variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
	Section inverse :
	`{{^variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
		Une interface nommée est définie sur la page Device (Périphérique) > Interfaces. Vous ne pouvez pas pointer vers des interfaces sans nom.
		Il existe une grande variété d'attributs disponibles dans le modèle d'interface. En outre, le modèle d'interface comprend des sous-objets, par exemple pour les adresses IP.
		Voici quelques-uns des principaux attributs que vous pourriez trouver utiles :
		• *variable_name*.**name** renvoie le nom logique de l'interface.
		• *variable_name*.**hardwareName** renvoie le nom du port de l'interface, tel que GigabitEthernet1/8.
		• *variable_name*.**managementOnly** est une valeur booléenne. TRUE (Vrai) signifie que l'interface est définie comme une interface de gestion uniquement. FALSE (Faux) signifie que l'interface est destinée au trafic traversant le périphérique. Vous pouvez utiliser cette option comme clé de section.
		• *variable_name*.**ipv4.ipAddress.ipAddress** renvoie l'adresse IPv4 de l'interface.
		• *variable_name*.**ipv4.ipAddress.netmask** renvoie le masque de sous-réseau pour l'adresse IPv4 de l'interface.

IP (variable simple)	**Variable :** {{*variable_name*}}	Une adresse IP IPv4 ou IPv6 unique, sans masque réseau ni longueur de préfixe.

Réseau
(variable d'objet : le modèle API est NetworkObject)
	Variable (Network Objects (Objets réseau)) :
	{{*variable_name*.*attribute*}}
	Section (Group Objects (Groupe d'objets)) :
	`{{#variable_name.networkObjects}}`
	`commands referring to one of`
	`  {{value}}`
	`  {{name}}`
	`{{/variable_name.networkObjects}}`
		Un objet réseau ou un groupe défini sur la page Objects (Objets). Vous pouvez utiliser des sections pour traiter des groupes réseau.
		Voici les principaux attributs que vous pourriez trouver utiles :
		• {{*variable_name*.**name**}} renvoie le nom de l'objet ou du groupe réseau.
		• {{*variable_name*.**value**}} renvoie le contenu de l'adresse IP d'un objet réseau (mais pas d'un groupe réseau). Veillez à utiliser un objet réseau qui a le type de contenu approprié pour une commande donnée, par exemple une adresse d'hôte plutôt qu'une adresse de sous-réseau.
		• {{*variable_name*.**groups**}} renvoie la liste des objets réseau contenus dans un groupe réseau. Utilisez-le uniquement avec les variables qui pointent vers des groupes de réseau et utilisez-le sur une balise de section pour traiter de manière itérative le contenu du groupe. Utilisez {{**value**}} ou {{**name**}} pour récupérer le contenu de chaque objet réseau à tour de rôle.

Type de variable	Modèles de référence	Description
Numérique (variable simple)	**Variable :** {{*variable_name*}}	Un nombre entier. N'incluez pas de virgules, de décimales, de signes (comme le signe négatif) ou la notation hexadécimale. Pour les nombres non entiers, utilisez une variable de chaîne.
Port (variable d'objet : le modèle API est PortObject, tcpports ou udpports)	**Variable :** {{*variable_name.attribute*}}	Un objet de port TCP ou UDP défini sur la page Objects (Objets). Il doit s'agir d'un objet de port et non d'un groupe de ports. Voici les principaux attributs que vous pourriez trouver utiles : • {{*variable_name*.**port**}} renvoie le numéro de port. Le protocole n'est pas inclus. • {{*variable_name*.**name**}} renvoie le nom de l'objet de port.
Secret (variable d'objet : le modèle API est Secret)	**Variable :** {{*variable_name*.**password**}} Ou : {{{*variable_name*.**password**}}}	Un objet de clé secrète défini pour FlexConfig. La seule référence que vous devez faire est à l'attribut **password**, qui renvoie la chaîne chiffrée. Si le mot de passe comprend des caractères spéciaux tels que &, utilisez des accolades triples.
Chaîne (variable simple)	**Variable :** {{*variable_name*}}	Une chaîne de texte. Par exemple, les noms d'hôte, les noms d'utilisateur, etc.

Sections {{#key}} {{/key}} et sections inverses {{^key}} {{/key}}

Une section ou une section inverse est un bloc de commandes entre les balises de début et de fin de section, qui utilisent une clé comme critère de traitement. La façon dont la section est traitée dépend de s'il s'agit d'une section normale ou inverse :

- Une section normale (ou simplement une section) est traitée si la clé est TRUE (vrai) ou a un contenu non vide. Si la clé est FALSE (faux) ou si l'objet n'a pas de contenu, les commandes de la section ne sont pas configurées. La section est contournée.

  Voici la syntaxe d'une section normale.

  ```
  {{#key}}
  one or more commands
  {{/key}}
  ```

- Une section inverse est l'opposé d'une section. Elle est traitée si la clé est FALSE (faux) ou si l'objet n'a pas de contenu. Si la clé est TRUE (vrai) ou si l'objet a du contenu, la section inverse est contournée.

  Voici la syntaxe d'une section inverse. La seule différence est qu'un signe d'attention remplace la balise de hachage.

  ```
  {{^key}}
  one or more commands
  {{/key}}
  ```

Les rubriques suivantes expliquent les principales utilisations des sections et des sections inverses.

Comment traiter les variables à valeurs multiples

Le principal exemple de traitement d'une variable à valeurs multiples est une variable réseau qui pointe vers un groupe de réseaux. Comme le groupe contient plusieurs objets (sous l'attribut **objects**), vous pouvez parcourir de manière itérative les valeurs du groupe de réseau pour configurer la même commande plusieurs fois avec des valeurs différentes.

Bien qu'un groupe d'objets définisse les objets réseau contenus dans l'attribut des objets, ces objets n'incluent pas le contenu des objets contenus. Au lieu de cela, vous utilisez l'attribut **networkObjects** pour obtenir le contenu des objets contenus.

Par exemple, si vous avez un groupe de réseau nommé net-group avec les hôtes 192.168.10.0, 192.168.20.0 et 192.168.30.0, vous pouvez utiliser la technique suivante pour configurer une commande réseau pour chaque adresse pour le routage RIP. Notez que vous utilisez l'attribut **value** de l'objet réseau, car l'utilisation de **net-group.networkObjects** dans le début de la section implique que l'attribut de valeur sera extrait uniquement des objets membres. (Vous ne créez pas de variable distincte pour l'attribut « value » dans l'objet FlexConfig.)

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

Le système traduit la structure de section comme suit :

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

Effectuer un traitement facultatif en fonction d'une valeur booléenne ou d'un objet vide

Remarque Les exemples de cette rubrique sont fournis uniquement à des fins d'illustration. Par exemple, vous ne pouvez pas utiliser FlexConfig pour configurer SNMP à partir de la version 6.7 ; vous devez plutôt utiliser la ressource SNMP de l'API Firewall Threat Defense.

Si le contenu de la variable dans la balise de début de section est TRUE (vrai), ou si un objet n'est pas vide, la section est traitée. Si une valeur booléenne est FALSE (faux) ou vide (comme un objet vide), la section est ignorée.

L'utilisation principale ici concerne les valeurs booléennes. Par exemple, vous pouvez créer une variable booléenne et placer des commandes dans une section régie par cette variable. Ensuite, si vous devez activer ou désactiver une section des commandes dans l'objet FlexConfig, il vous suffit de modifier la valeur de la variable booléenne; vous n'avez pas besoin de supprimer ces lignes du code. Cela permet d'activer ou de désactiver facilement les fonctionnalités.

Par exemple, vous pourriez vouloir pouvoir désactiver les interruptions SNMP si vous utilisez FlexConfig pour activer SNMP. Vous pouvez créer une variable booléenne nommée enable-traps et la définir initialement à TRUE (vrai). Ensuite, si vous devez désactiver les interruptions, vous n'avez qu'à modifier la variable, la remplacer par FALSE (faux), enregistrer l'objet, puis redéployer la configuration. La séquence de commandes pourrait ressembler à ce qui suit :

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

Vous pouvez également effectuer ce type de traitement en fonction de valeurs booléennes à l'intérieur d'un objet. Par exemple, vous pouvez vérifier si une interface est réservée à la gestion avant de configurer une caractéristique sur celle-ci. Dans l'exemple suivant, int-inside est une variable d'interface qui pointe vers l'interface nommée inside. FlexConfig configure les options d'interface liées à EIGRP sur l'interface uniquement si celle-ci n'est pas définie comme interface de gestion uniquement. Vous utiliserez une section inverse afin que les commandes ne soient configurées que si la valeur booléenne est FALSE (faux).

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

Référence aux objets Smart CLI dans un objet FlexConfig

Lorsque vous créez un objet FlexConfig, vous pouvez utiliser des variables pour pointer vers des objets que vous pouvez configurer dans le Firepower Device Manager. Par exemple, vous pouvez créer des variables qui pointent vers des éléments d'interface ou des objets réseau.

Cependant, vous ne pouvez pas pointer vers des objets Smart CLI de la même manière.

Au lieu de cela, si vous créez un objet Smart CLI que vous devez utiliser dans une politique FlexConfig, vous saisissez simplement le nom de l'objet Smart CLI à l'emplacement approprié.

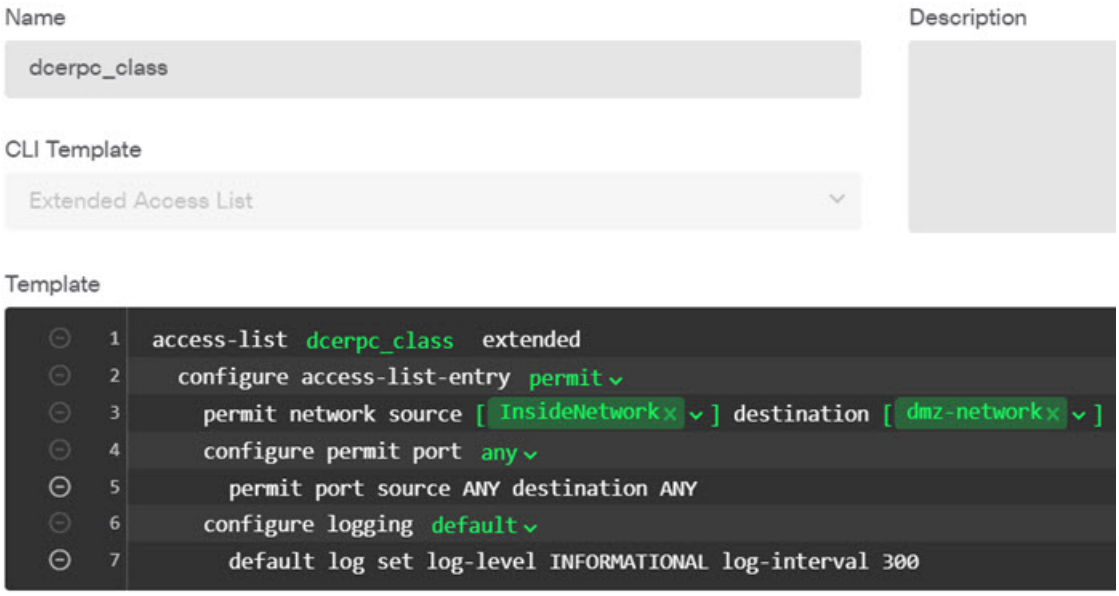
Par exemple, vous pouvez utiliser une liste d'accès étendue comme classe de trafic lorsque vous configurez l'inspection de protocole. Comme il existe un objet Smart CLI pour les listes d'accès étendues, vous devez utiliser l'objet Smart CLI pour créer l'ACL : vous ne pouvez pas utiliser la commande **access-list** dans l'objet FlexConfig.

Par exemple, si vous souhaitez activer l'inspection DCERPC entre les réseaux 192.168.1.0/24 et 192.168.2.0/24 globalement, vous procéderez comme suit.

Procédure

Étape 1 Créez des objets réseau distincts pour les deux réseaux. Par exemple, InsideNetwork et dmz-network.

Étape 2 Utilisez ces objets dans un objet de liste d'accès étendu Smart CLI.



Étape 3 Créez un objet FlexConfig qui pointe vers l'objet Smart CLI par son nom.

Par exemple, si l'objet est nommé « dcerpc_class », votre objet FlexConfig peut ressembler à ce qui suit. Notez que dans le modèle d'annulation, vous n'annulez pas la liste d'accès créée par l'objet Smart CLI, car cet objet n'est pas réellement créé par FlexConfig.

Étape 4 Ajoutez l'objet à la politique FlexConfig.

Configuration des objets de clé secrète

Le but d'un objet de clé secrète est de masquer les mots de passe ou les chaînes sensibles. Si vous ne voulez pas risquer que quelqu'un voie une chaîne utilisée dans un objet FlexConfig ou un modèle Smart CLI, créez un objet de clé secrète pour cette chaîne.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **Clés secrètes** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Entrez un nom pour l'objet et, facultativement, une description.

Étape 4 Saisissez le mot de passe ou une autre chaîne secrète dans les champs **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe).

Le système masque le texte pendant que vous tapez.

Étape 5 Cliquez sur **OK**.

Prochaine étape

- S'il s'agit d'un nouvel objet, pour l'utiliser dans FlexConfig, modifiez un objet FlexConfig, créez une variable du type de clé secrète et sélectionnez l'objet. Ensuite, faites référence à la variable dans le corps de l'objet. Pour en savoir plus, consultez Création de variables dans un objet FlexConfig, à la page 17.
- Si vous modifiez un objet existant qui est utilisé dans un objet FlexConfig qui fait partie de la politique FlexConfig, vous devez déployer la configuration pour mettre à jour le périphérique avec la nouvelle chaîne.
- Dans les modèles Smart CLI, si une commande nécessite une clé secrète, vous verrez une liste de ces objets lors de la modification de la propriété concernée. Sélectionnez la clé appropriée selon l'usage prévu.

Dépannage de la politique FlexConfig

Après avoir modifié la politique FlexConfig, examinez attentivement les résultats du prochain déploiement. Si vous recevez un message « Le dernier déploiement a échoué » dans la boîte de dialogue Pending Changes (Modifications en attente), cliquez sur le lien **See Details** (Voir les détails). Le lien vous mène vers le journal d'audit, où vous pouvez trouver la tâche de déploiement qui a échoué. Ouvrez la tâche pour trouver les messages d'erreur spécifiques.

Si le déploiement échoue en raison d'un problème FlexConfig, les détails indiqueront l'objet FlexConfig contenant la commande incorrecte et afficheront la commande qui a échoué. Utilisez ces renseignements pour corriger l'objet et réessayer le déploiement. Le nom de l'objet est un lien. Cliquez dessus pour ouvrir la boîte de dialogue Edit (Modifier) de l'objet.

Par exemple, vous pourriez vouloir configurer la taille maximale de segment TCP (TCP MSS). Vous pouvez contrôler ce paramètre avec la commande **sysopt connection tcpmss**. Lorsqu'elle est configurée par Firepower

Device Manager, la valeur par défaut Firewall Threat Defense pour cette option est 0, par rapport à la valeur ASA par défaut de 1380.

La valeur par défaut de l'ASA est conçue pour un traitement optimal lors de l'exécution d'un VPN IPv4 sur des interfaces qui utilisent la MTU par défaut de 1 500. Le système a besoin de 120 octets pour les en-têtes VPN. Pour IPv6, le système a besoin de 140 octets. La Firewall Threat Defense par défaut de 0 permet simplement aux points terminaux de négocier le MSS, qui est le paramètre idéal pour le trafic normal, surtout si vous utilisez différentes MTU sur les interfaces du périphérique, y compris des MTU supérieures à 1 500. Étant donné que le MSS TCP est un paramètre global et non propre à une interface, vous ne le modifieriez que si un pourcentage important de votre trafic passe par le VPN et que vous constatez une fragmentation excessive. Dans ce cas, vous pouvez définir le MSS TCP à MTU moins 120 (pour IPv4) ou 140 (pour IPv6), et utiliser la même MTU pour toutes les interfaces. Notez que même si vous définissez explicitement un MSS, si un composant comme le déchiffrement TLS/SSL ou la découverte de serveur nécessite un MSS particulier, il définira ce MSS en fonction de la MTU de l'interface et ignorera votre réglage MSS.

À titre d'illustration, supposons que vous souhaitiez définir le MSS TCP à 3 octets. La commande prend 48 octets comme valeur minimale, vous obtiendrez donc une erreur de déploiement semblable à ce qui suit :

L'erreur se compose des éléments suivants :

1. Le message d'erreur de déploiement, qui comprend le nom de l'objet FlexConfig qui a causé l'erreur. Le nom de l'objet est lié à la boîte de dialogue Edit (Modifier) afin que vous puissiez ouvrir rapidement l'objet et corriger l'erreur. Il s'agit de la première phrase du message.
2. Le texte commençant par « ERROR : » est le message renvoyé par le périphérique. C'est exactement ainsi qu'un ASA répondrait si vous saisissiez la commande erronée, sans le formatage d'un client SSH. Dans cet exemple, le message d'erreur est « ERROR : [3] est inférieur au MSS minimal autorisé de 48 par la RFC 791 ». Le texte qui commence par « Config Error » mentionne la ligne précise qui a généré le message d'erreur.
3. Le texte en noir correspond à la ligne réelle de l'objet FlexConfig qui a causé l'erreur. Vous devez corriger cette ligne. Dans cet exemple, si vous essayez d'adapter le trafic VPN IPv4 sur des interfaces MTU 1500 (cas courant), vous remplaceriez 3 par 1 380.

   Pour corriger cet exemple, vous pouvez laisser la console d'interface de ligne de commande ouverte et utiliser **show running-config all sysopt** pour voir tous les paramètres de commande **sysopt**. La plupart des commandes **sysopt** possèdent des valeurs par défaut adaptées à la plupart des usages, de sorte qu'elles n'apparaissent pas dans la configuration active. Le mot-clé **all** inclut ces paramètres par défaut dans la sortie.

Exemples de FlexConfig

Les rubriques suivantes fournissent quelques exemples d'utilisation de FlexConfig pour configurer les fonctionnalités.

Comment activer et désactiver les inspections globales par défaut

Certains protocoles intègrent des informations d'adressage IP dans le paquet de données de l'utilisateur ou ouvrent des canaux secondaires sur les ports affectés dynamiquement. Ces protocoles nécessitent que le système effectue une inspection approfondie des paquets afin que la NAT puisse être appliquée et que les canaux secondaires puissent être autorisés. Plusieurs moteurs d'inspection courants sont activés sur le système par défaut, mais vous devrez peut-être en activer d'autres ou désactiver les inspections par défaut, en fonction de votre réseau.

Pour voir la liste des inspections actuellement activées, utilisez la commande **show running-config policy-map**, soit dans la console CLI, soit dans une session SSH. Voici ce que vous verriez sur un système où aucune modification n'a été apportée à la configuration d'inspection. Dans cette sortie, la liste des commandes **inspect** à la fin de la sortie indique les inspections de protocole activées. Les commandes précédentes activent ces inspections sur la classe de trafic inspection_default (qui contient les protocoles normaux et, le cas échéant, les numéros de port pour le protocole inspecté). Cette classe fait partie de la carte de politiques global_policy, qui applique ces inspections à toutes les interfaces à l'aide d'une commande service-policy qui ne s'affiche pas dans la sortie. Par exemple, l'inspection ICMP est effectuée sur tout le trafic ICMP qui passe par le périphérique.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

Remarque Pour une description détaillée de chaque inspection, consultez le *Guide de configuration des pare-feu Cisco ASA* disponible sur le site https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

La procédure suivante vous montre comment activer ou désactiver les inspections dans cette classe d'inspection par défaut appliquée globalement. À des fins d'illustration, l'exemple :

- Active le PPTP (Protocole Point-to-Point Tunneling). Ce protocole est utilisé pour tunnelliser une connexion point à point entre deux points terminaux.
- Désactive le SIP (Session Initiation Protocol). Vous ne devez généralement désactiver le protocole SIP que si l'inspection cause des problèmes dans le réseau. Toutefois, si vous désactivez le protocole SIP, vous devez vous assurer que vos stratégies de contrôle d'accès autorisent le trafic SIP (UDP/TCP 5060) et tous les ports alloués dynamiquement, et que vous n'avez pas besoin de prise en charge de la NAT pour les connexions SIP. Ajustez les politiques de contrôle d'accès et de NAT en conséquence à l'aide des pages standard, et non par l'intermédiaire de FlexConfig.

Avant de commencer

Une bonne planification vous aidera à utiliser FlexConfig efficacement. Dans cet exemple, nous modifions deux inspections différentes et non liées, bien que nous apportions les modifications dans la même classe de trafic. Mais il est fort possible que si vous devez modifier ces politiques, vous le fassiez de manière indépendante.

Par conséquent, nous vous recommandons de créer des objets FlexConfig distincts pour chaque inspection dans cet exemple. De cette façon, vous pouvez facilement modifier vos paramètres pour une inspection sans modifier l'autre et sans avoir à modifier l'objet FlexConfig.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Créez l'objet pour activer l'inspection PPTP.

a) Cliquez sur le bouton + pour créer un nouvel objet.

b) Saisissez un nom pour l'objet. Par exemple, **Enable_PPTP_Global_Inspection**.

c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Tout comme vous devez inclure les commandes parentes pour entrer dans le sous-mode approprié pour une commande afin de l'activer, vous devez également inclure ces commandes dans le modèle de négation.

Le modèle d'annulation sera appliqué si vous supprimez cet objet de la politique FlexConfig (après l'avoir déployé avec succès), et également lors d'un déploiement infructueux (pour réinitialiser la configuration à son état précédent).

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
policy-map global_policy
 class inspection_default
```

```
no inspect pptp
```

L'objet doit ressembler à ce qui suit :

Remarque
Comme la classe inspection_default comporte d'autres commandes d'inspection activées, vous ne souhaitez pas annuler la classe entière. De même, la carte de politiques global_policy comprend ces autres inspections, et vous ne souhaitez pas non plus annuler la carte de politiques.

e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 4 Créez l'objet pour désactiver l'inspection SIP.

a) Cliquez sur le bouton **+** pour créer un nouvel objet.
b) Saisissez un nom pour l'objet. Par exemple, **Disable_SIP_Global_Inspection**.
c) Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

La commande « negate » pour une commande « no » de désactivation est la commande qui active la fonctionnalité. Ainsi, le modèle « annuler » ne comprend pas seulement les commandes pour désactiver

une fonctionnalité, il s'agit des commandes pour inverser ce que vous faites dans le modèle « positif ». L'objectif du modèle d'annulation est d'annuler vos modifications.

Ainsi, pour cet exemple, le modèle de négation serait le suivant :

```
policy-map global_policy
 class inspection_default
  inspect sip
```

L'objet doit ressembler à ce qui suit :

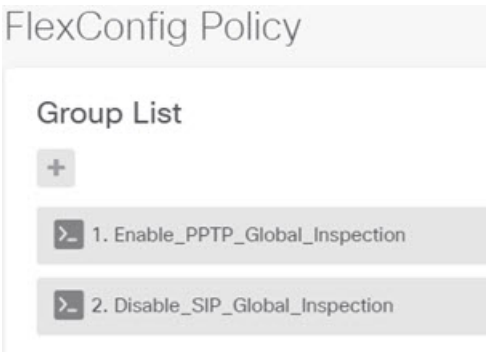
e) Cliquez sur **OK** pour enregistrer l'objet.

Étape 5 Ajoutez les objets à la politique FlexConfig.

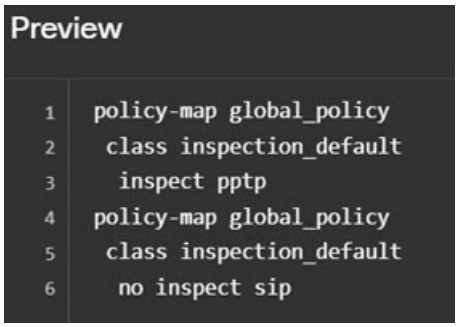
La création d'un objet n'est pas suffisante. Les objets sont déployés uniquement si vous les ajoutez à la politique FlexConfig (et enregistrez vos modifications). Cela vous permet de tester des objets (et de les laisser partiellement terminés) sans risquer d'échecs de déploiement sur un travail inachevé. Vous pouvez ensuite activer ou désactiver facilement des fonctionnalités en ajoutant et en supprimant des objets : il n'est pas nécessaire de recréer l'objet à chaque fois.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur + dans la liste des groupes.
c) Sélectionnez les objets Enable_PPTP_Global_Inspection et Disable_SIP_Global_Inspection, puis cliquez sur **OK**.

La liste des groupes doit ressembler à ce qui suit :



L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.



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

Vous pouvez maintenant déployer la politique.

Étape 6 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 7 Dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config policy-map** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Dans la sortie suivante, notez que **inspect pptp** est ajouté au bas de la classe inspection_default et que **inspect sip** ne figure plus dans la classe. Cela confirme que les modifications définies dans l'objet FlexConfig ont été déployées avec succès.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
```

```
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

Comment annuler vos modifications FlexConfig

Si vous saisissez un modèle de négation correct dans un objet FlexConfig, la suppression des modifications apportées à l'aide de cet objet est simple. Vous supprimez simplement l'objet de la politique FlexConfig et lors du prochain déploiement, le système utilise votre modèle de négation pour annuler vos modifications.

Vous n'avez pas besoin de créer un nouvel objet pour annuler vos modifications.

L'exemple suivant montre comment réactiver l'inspection SIP globale. L'exemple rétablit la modification expliquée dans Comment activer et désactiver les inspections globales par défaut, à la page 27, qui a désactivé l'inspection SIP.

Avant de commencer

Vérifiez que l'objet FlexConfig dispose du bon modèle de négation. Si ce n'est pas le cas, modifiez l'objet pour corriger le modèle de négation.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Policy (Politique FlexConfig)** dans la table des matières de configuration avancée.

Étape 3 Cliquez sur le **X** à droite de l'entrée de l'objet **Disable_SIP_Global_Inspection** dans la politique FlexConfig pour le supprimer de la politique.

Les commandes de l'objet sont supprimées de l'aperçu. Les commandes d'annulation ne sont pas ajoutées à l'aperçu, elles seront exécutées en arrière-plan.

Étape 4 Cliquez sur **Save** (enregistrer).

Étape 5 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 6 Dans la console d'interface de ligne de commande ou une session SSH, utilisez la commande **show running-config policy-map** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Dans le résultat suivant, notez que **inspect sip** est ajouté au bas de la classe inspection_default. Cela confirme que les modifications définies dans l'objet FlexConfig ont été déployées avec succès. (L'ordre n'est pas important dans cette classe, donc peu importe que **inspect sip** se trouve à la fin et non à son emplacement d'origine.)

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
!
```

Comment activer les inspections pour les classes de trafic uniques

Dans cet exemple, nous activerons l'inspection PPTP pour le trafic entre deux points terminaux sur une interface spécifique. Cela cible l'inspection uniquement sur les points terminaux qui ont un tunnel point à point configuré entre eux.

L'interface de ligne de commande requise pour activer l'inspection PPTP entre 2 points terminaux implique les éléments suivants :

1. Une liste de contrôle d'accès avec la source et la destination définies pour les adresses IP des hôtes du terminal.
2. Une classe de trafic qui fait référence à cette liste de contrôle d'accès.
3. Une carte de politiques qui comprend la classe de trafic et qui active l'inspection PPTP sur la classe de trafic.
4. Une politique de service qui applique la carte de politiques à l'interface souhaitée. Il s'agit de l'étape qui active la politique et permet l'inspection.

Remarque Pour obtenir une description détaillée des politiques de service liées aux inspections, consultez le *guide de configuration de pare-feu Cisco ASA* disponible sur le site https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

Étape 2 Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

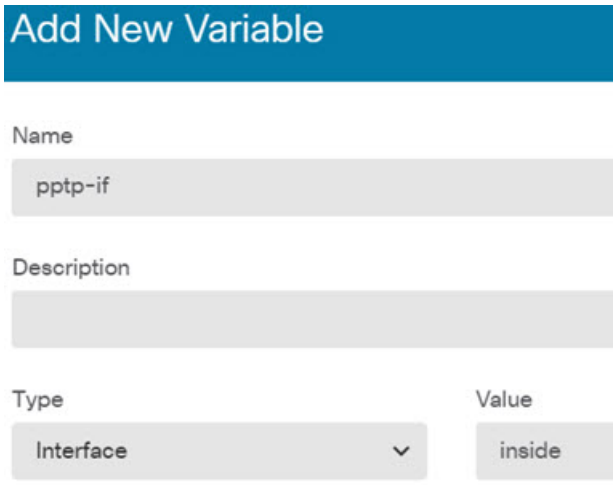
Étape 3 Cliquez sur le bouton + pour créer un nouvel objet.

Étape 4 Saisissez un nom pour l'objet. Par exemple, **Enable_PPTP_Inspection_on_Interface**.

Étape 5 Ajoutez une variable pour l'interface interne.

a) Cliquez sur le signe + au-dessus de la liste des variables.
b) Saisissez un nom pour la variable, par exemple, **pptp-if**.
c) Pour **Type**, sélectionnez **Interface**.
d) Pour **Value** (Valeur), sélectionnez l'interface **inside**.

La boîte de dialogue doit ressembler à ce qui suit :



e) Cliquez sur **Add** (ajouter).

Étape 6 Dans l'éditeur **Template** (Modèle), saisissez les lignes suivantes, y compris les indentations.

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

Notez que pour utiliser la variable, vous devez saisir le nom de la variable entre double crochets. Vous devez également utiliser la notation par point pour choisir l'attribut que vous souhaitez récupérer, car l'objet qui définit une interface comporte de nombreux attributs. Comme le nom de l'interface est contenu dans l'attribut « name », la saisie de **{{pptp-if.name}}** récupère la valeur de l'attribut de nom de l'interface attribuée à la variable. Si vous devez modifier l'interface pour l'inspection PPTP, il vous suffit de sélectionner une interface différente dans la définition de la variable.

Étape 7 Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Pour cet exemple, nous supposerons que la carte de classes, la carte de politiques et la politique de service existent dans le seul but d'appliquer l'inspection PPTP. Ainsi, dans le modèle d'annulation, nous souhaitons supprimer tous ces éléments.

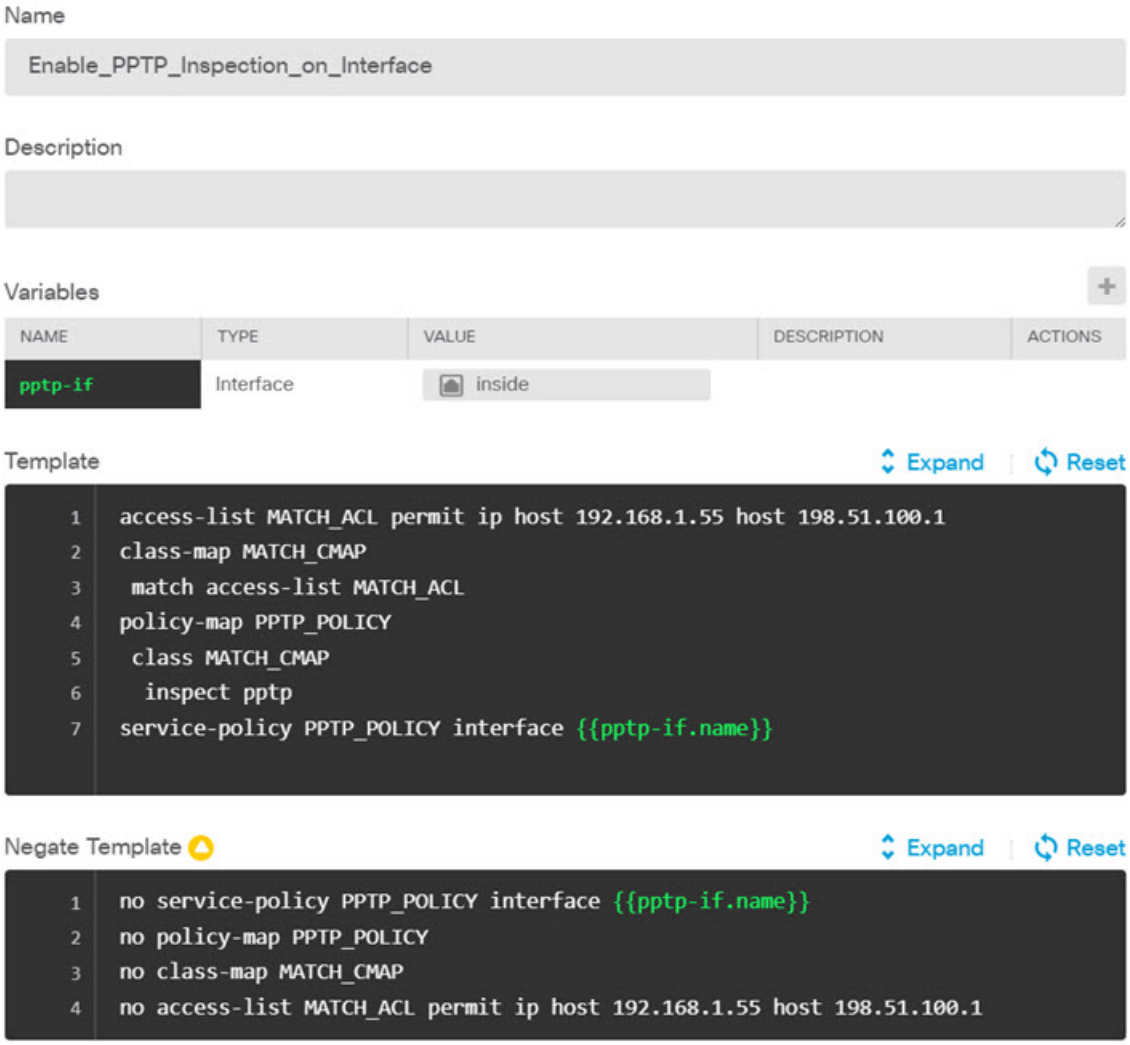
Si, toutefois, vous ajoutez actuellement l'inspection PPTP à une politique de service existante sur une interface, vous n'annulerez pas la carte de politiques ou la politique de service. Vous pouvez soit annuler la classe de la carte des politiques, soit désactiver simplement l'inspection au sein de la classe au sein de la carte des politiques. Vous devez avoir une compréhension claire de ce que vous mettez en œuvre dans les autres objets FlexConfig pour vous assurer que votre modèle d'annulation n'a pas de conséquences inattendues.

Lors de la suppression d'éléments imbriqués, vous devez le faire dans l'ordre inverse dans lequel vous les avez créés. Ainsi, vous commencez par supprimer la politique de service et terminez par la suppression de la liste d'accès. Sinon, vous tenteriez de supprimer des objets qui sont en cours d'utilisation, et le système renvoyera des erreurs et ne vous permettra pas de le faire.

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
```

```
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

Le corps de l'objet doit ressembler à ce qui suit :



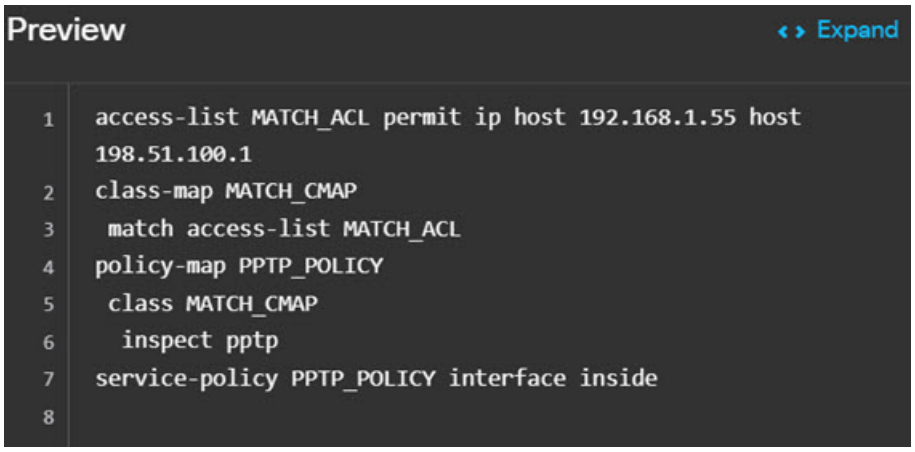
Étape 8 Cliquez sur **OK** pour enregistrer l'objet.

Étape 9 Ajoutez les objets à la politique FlexConfig.

a) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.
b) Cliquez sur + dans la liste des groupes.
c) Sélectionnez l'objet **Enable_PPTP_Inspection_on_Interface** et cliquez sur **OK**.

La liste des groupes doit ressembler à ce qui suit :

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues, comme le montre le graphique suivant. Remarquez que la variable d'interface se résout en nom « inside » dans l'aperçu. Portez une attention particulière aux variables : si elles ne se résolvent pas correctement dans l'aperçu, elles ne seront pas déployées correctement. Modifiez l'objet FlexConfig jusqu'à ce que vous obteniez la traduction de variable correcte dans l'aperçu.



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

Vous pouvez maintenant déployer la politique.

Étape 10 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Étape 11 Dans la console d'interface de ligne de commande ou une session SSH, utilisez des variantes de la commande **show running-config** et vérifiez que la configuration en cours d'exécution comporte les modifications correctes.

Vous pouvez saisir **show running-config** et examiner l'ensemble de la configuration CLI, ou utiliser les commandes suivantes pour vérifier chaque partie de cette configuration :

- **show running-config access-list MATCH_ACL** pour vérifier l'ACL.

- **show running-config class** pour vérifier la carte de classe. Cette commande affichera toutes les cartes de classe.
- **show running-config policy-map PPTP_POLICY** pour vérifier la configuration des classes et de la carte de politiques.
- **show running-config service-policy** pour vérifier que la carte des politiques a été appliquée à l'interface. Cela affichera toutes les politiques de service.

Le résultat suivant montre cette séquence de commandes, et vous pouvez voir que la configuration est correctement appliquée.

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

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.