Déploiement de la configuration

Ce chapitre décrit comment télécharger des modifications de configuration sur un ou plusieurs périphériques gérés.

À propos du déploiement de la configuration

Toute la configuration des périphériques est gérée par centre de gestion, puis déployées sur les périphériques gérés.

Modifications de la configuration qui nécessitent un déploiement

Le système signale les politiques périmées par un texte d'état rouge qui indique le nombre de périphériques ciblés nécessitant une mise à jour de la politique. Pour effacer cet état, vous devez redéployer la politique sur les périphériques.

Déploiement nécessaire

Voici les modifications de configuration qui nécessitent un déploiement :

- La modification d'une politique de contrôle d'accès : toute modification apportée aux règles de contrôle d'accès, à l'action par défaut, aux cibles de la politique, au filtrage Security Intelligence, aux options avancées, y compris le prétraitement, etc.
- La modification de toute politique appelée par la politique de contrôle d’accès : la politique SSL, les politiques d’analyse de réseau, les politiques de prévention des intrusions, les politiques de fichiers, les politiques d’identité ou les politiques DNS.
- La modification de tout objet réutilisable ou de toute configuration utilisée dans une politique de contrôle d’accès ou des politiques de contrôle d’accès appelées :
  - les objets de réseau, de port, de balise VLAN, d'URL et de géolocalisation

- Listes er flux de renseignements sur la sécurité
- filtres ou détecteurs d'application
- ensembles de variables de la politique de prévention des intrusions
- listes de fichiers
- les objets liés au déchiffrement et aux zones de sécurité;

- Mise à jour du logiciel système, des règles de prévention des intrusions ou de la base de données de vulnérabilités (VDB).

Gardez à l'esprit que vous pouvez modifier certaines de ces configurations à partir de plusieurs endroits de l'interface Web. Par exemple, vous pouvez modifier des zones de sécurité à l'aide du gestionnaire d'objets (**Objects (objets)** > **Object Management (gestion des objets)**), mais la modification d'un type d'interface dans la configuration d'un périphérique (**Devices (appareils)** > **Device Management (gestion des appareils)**) peut également modifier une zone et nécessiter un déploiement.

Déploiement non nécessaire

Notez que les mises à jour suivantes ne nécessitent **pas** de déploiement :

- mises à jour automatiques des flux de renseignements sur la sécurité et des ajouts à la liste globale de blocage ou de non-blocage des renseignements sur la sécurité à l'aide du menu contextuel.
- mises à jour automatiques des données de filtrage d'URL
- mises à jour planifiées de la base de données de géolocalisation (GeoDB)

Aperçu du déploiement

L'aperçu présente un résumé de tous les changements de politique et d'objet qui doivent être déployés sur le périphérique. Les changements de politique comprennent les nouvelles politiques, les changements apportés aux politiques existantes et les politiques supprimées. Les changements apportés aux objets incluent les objets ajoutés et modifiés qui sont utilisés dans les politiques. Les changements apportés aux objets inutilisés ne sont pas affichés, car ils ne sont pas déployés sur le périphérique.

L'aperçu affiche toutes les valeurs par défaut, même lorsqu'elles ne sont pas modifiées, aux côtés des autres paramètres configurés lorsqu'une interface ou une politique de paramètres de plateforme est ajoutée pour la première fois. De même, les politiques relatives à la haute disponibilité et les valeurs par défaut des paramètres sont affichées, même si elles ne sont pas modifiées, dans le premier aperçu après la configuration ou la perturbation d'une paire à haute disponibilité.

Pour afficher les modifications dues à une restauration automatique, consultez Modifier les paramètres de déploiement.

Fonctionnalités non prises en charge

- Les ajouts d'objets et les changements d'attributs ne sont affichés dans l'aperçu que si les objets sont associés à un périphérique ou à une interface. Les suppressions d'objets ne sont pas affichées.
- L'aperçu n'est pas pris en charge pour les politiques suivantes :
  - Haute disponibilité

- Détection du réseau
- Analyse du réseau
- Paramètres de l’appareil

- Les renseignements sur les utilisateurs au niveau de la règle ne sont pas disponibles pour les politiques en lien avec la prévention des intrusions.
- L'aperçu n'affiche pas la réorganisation des règles entre les politiques.

  Pour les politiques DNS, les règles réorganisées apparaissent dans la liste d'aperçu sous la forme d'ajouts et de suppressions de règles. Par exemple, le déplacement d’une règle de la position 1 à la position 3 dans l’ordre des règles s’affiche comme si la règle était supprimée de la position 1 et ajoutée en tant que nouvelle règle à la position 3. De même, lorsqu'une règle est supprimée, les règles afférentes sont répertoriées comme règles modifiées, car leurs positions ont été modifiées. Les modifications sont affichées dans l’ordre final dans lequel elles apparaissent dans la politique.
- La prévisualisation n'est pas prise en charge dans les scénarios de haute disponibilité suivants :
  - Si un périphérique était en mode autonome et si une chaîne est réalisée, un déploiement automatique est déclenché. Pour cette tâche en particulier, la prévisualisation n’est pas prise en charge. Lorsque vous passez le curseur sur le **Aperçu** (), un message indique qu’il s’agit d’un déploiement de démarrage à haute disponibilité et qu’aucun aperçu n’est pris en charge.
  - **Groupes de configuration** : Prenons l'exemple d'un flux dans lequel un périphérique est initialement autonome. Par la suite, trois déploiements ont eu lieu. Lors du quatrième déploiement, le périphérique était un déploiement de démarrage en mode haute disponibilité (HA bootstrap). Ensuite, l’utilisateur déploie les périphériques 5, 6 et 7. Le déploiement 7 est un déploiement avec rupture de la haute disponibilité, et l’utilisateur déploie les périphériques 8, 9 et 10.

    Dans ce flux, l’aperçu entre 3 et 5 n’est pas pris en charge, car la valeur 4 était un déploiement de haute disponibilité. De même, l’aperçu entre 8 et 3 n’est pas non plus pris en charge. L’aperçu est pris en charge uniquement pour les versions 3 à 1, 7,6, 5, 4 et 10, 9 et 8.
  - Si un périphérique est défectueux (la haute disponibilité est défectueuse), le nouveau périphérique est considéré comme un tout nouveau périphérique.

Déploiement sélectif des politiques

Le centre de gestion vous permet de sélectionner une politique particulière dans la liste de toutes les modifications sur le périphérique qui doivent être déployées et de déployer uniquement la politique sélectionnée. Le déploiement sélectif est disponible uniquement pour les politiques suivantes :

- Politiques de contrôle d’accès
- Politique de prévention des intrusions
- Politiques relatives aux fichiers et aux logiciels malveillants
- Politiques DNS
- Politiques d’identité
- Politiques SSL

- Politiques de QOS
- Règles du préfiltre
- Détection du réseau
- Politiques NAT
- Politiques de routage
- Politiques VPN

Il y a certaines limites au déploiement sélectif des politiques. Suivez le contenu du tableau ci-dessous pour comprendre quand le déploiement sélectif des politiques peut être utilisé.

Tableau 1 : Limitations du déploiement sélectif

Type	Description	Scénarios
Déploiement complet	Le déploiement complet est nécessaire pour des scénarios de déploiement particuliers, et le centre de gestionne prend pas en charge le déploiement sélectif dans de tels scénarios. Si vous rencontrez une erreur dans de tels scénarios, vous pouvez choisir de continuer en sélectionnant toutes les modifications à déployer sur le périphérique.	Les scénarios dans lesquels un déploiement complet est requis sont les suivants : • Le premier déploiement après la mise à niveau de défense contre les menaces ou de centre de gestion. • Le premier déploiement après que vous ayez restauré défense contre les menaces . • Le premier déploiement après des modifications dans les paramètres de l'interface de défense contre les menaces . • Le premier déploiement après les modifications des paramètres du routeur virtuel. • Lorsque le périphérique défense contre les menaces est déplacé vers un nouveau domaine (global vers sous-domaine ou sous-domaine vers global).

Type	Description	Scénarios
Déploiement connexe de politiques	Le centre de gestion détermine les politiques interdépendantes qui sont liées entre elles. Lorsqu'une des politiques interconnectées est sélectionnée, les politiques interconnectées restantes sont automatiquement sélectionnées.	Scénarios dans lesquels une politique associée est automatiquement sélectionnée : • Lorsqu'un nouvel objet est associé à une politique existante. • Lorsque l'objet d'une politique existante est modifié. Scénarios dans lesquels plusieurs politiques sont automatiquement sélectionnées : • Lorsqu'un nouvel objet est associé à une politique existante et que le même objet est déjà associé à d'autres politiques, toutes les politiques associées sont automatiquement sélectionnées. • Lorsqu'un objet partagé est modifié, toutes les politiques associées sont automatiquement sélectionnées.
Modifications de politique interdépendantes (affichées à l'aide de balises à code de couleur)	Le centre de gestion détecte dynamiquement les dépendances entre les politiques, et entre les objets partagés et les politiques. L'interdépendance des objets ou des politiques est indiquée à l'aide de balises de couleur.	Scénarios dans lesquels des politiques ou objets interdépendants codés par couleur sont automatiquement sélectionnés : • Lorsque toutes les politiques obsolètes ont des changements interdépendants. Par exemple, lorsqu'une politique de contrôle d'accès, une politique de prévention des intrusions et une politique NAT sont obsolètes. Puisque la politique de contrôle d'accès et la politique NAT partagent un objet, toutes les politiques sont sélectionnées ensemble pour le déploiement. • Lorsque toutes les politiques obsolètes partagent un objet et que l'objet est modifié.

Type	Description	Scénarios
Spécifications du groupe de politiques d'accès	Les politiques du groupe de politiques d'accès sont répertoriées dans la fenêtre d'aperçu sous **Access Policy Group** (groupe de politiques d'accès) lorsque vous cliquez sur **Afficher ou masquer la politique** ().	Les scénarios et le comportement attendu des politiques de groupe de politiques d'accès sont les suivants : • Si la politique de contrôle d'accès est obsolète, exception faite des politiques de fichiers et des politiques de prévention des intrusions, toutes les autres politiques obsolètes de ce groupe sont sélectionnées lorsque la politique de contrôle d'accès est sélectionnée pour le déploiement. Toutefois, si la politique de contrôle d'accès est obsolète, les politiques de prévention des intrusions et de fichier peuvent être sélectionnées ou désélectionnées individuellement, que la politique de contrôle d'accès soit sélectionnée ou non, à moins qu'il y ait des changements dépendants. Par exemple, si une nouvelle politique d'intrusion est affectée à une règle de contrôle d'accès, cela indique qu'il y a des changements dépendants, alors la politique de contrôle d'accès et la politique de prévention des intrusions seront automatiquement sélectionnées lorsque l'une d'elles sera sélectionnée. • Si aucune politique de contrôle d'accès n'est obsolète, vous pouvez sélectionner et déployer d'autres politiques obsolètes dans ce groupe.

Nom d'utilisateur du système

Le centre de gestion présente le nom d'utilisateur en tant que **système** pour les opérations suivantes :

- Restauration
- Mise à jour
- Défense contre les menaces Sauvegarde et restauration
- Mise à jour de la SRU
- Mise à jour du LSP
- Mise à jour de la VDB

Détecteurs d'application à activation automatique

Si vous effectuez un contrôle des applications, mais désactivez les détecteurs requis, le système activera automatiquement les détecteurs appropriés fournis par le système lors du déploiement de la politique. S'il n'y en a pas, le système activera le détecteur défini par l'utilisateur le plus récemment modifié pour l'application.

Redécouverte des ressources à la suite de modifications apportées à une politique de découverte du réseau

Lorsque vous déployez des modifications apportées à une politique de découverte de réseau, le système supprime puis redécouvre les informations d'adresse MAC, de durée de vie et de sauts sur la carte réseau pour les hôtes de vos réseaux surveillés. En outre, les périphériques gérés rejettent toutes les données de découverte qui n'ont pas encore été envoyées au centre de gestion.

Scénarios de redémarrage de Snort

Lorsque le moteur d'inspection du trafic appelé *processus Snort* redémarre, l'inspection est interrompue jusqu'à la reprise du processus. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 9 pour obtenir de plus amples renseignements. En outre, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection lors du déploiement, que le processus Snort soit redémarré ou non.

N'importe lequel des scénarios présentés dans le tableau suivant entraîne le redémarrage du processus Snort.

Tableau 2 : Scénarios de redémarrage de Snort

Scénario de redémarrage	Autres renseignements
Déploiement d'une configuration spécifique nécessitant le redémarrage du processus Snort.	Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11
la modification d'une configuration qui redémarre immédiatement le processus Snort.	Modifications qui redémarrent immédiatement le processus Snort, à la page 13
Activation du trafic de la configuration de contournement automatique des applications (AAB) actuellement déployée.	Configurer le contournement automatique de l'application
Activation ou désactivation de la fonction « Journalisation des événements de connexion sur le disque RAM ».	Consultez la section **Log to Ramdisk** (Journaliser sur la RAM) dans le dépannage du vidage des événements non traités de FMC.

Sujets connexes

Paramètres avancés de politique de contrôle d'accès

Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11

Redémarrer les avertissements pour les appareils

Lorsque vous effectuez un déploiement, la colonne **Inspect Interruption interruption de l'inspection)** de la boîte de dialogue de déploiement indique si une configuration déployée redémarre le processus Snort sur

l'appareil défense contre les menaces . Lorsque le moteur d'inspection du trafic appelé *processus Snort* redémarre, l'inspection est interrompue jusqu'à la reprise du processus. L'interruption du trafic ou son passage sans inspection dépend de la gestion du trafic au niveau de l'appareil. Notez que vous pouvez procéder au déploiement, annuler le déploiement et modifier la configuration ou reporter le déploiement à un moment où le déploiement aurait le moins d'impact sur votre réseau.

Lorsque la colonne **Inspect Interruption** (inspecter l'interruption) indique **Yes** (oui) et que vous développez la liste de configuration du périphérique, le système indique tout type de configuration spécifique qui redémarrerait le processus Snort avec **Inspecter interruption** ( ). Lorsque vous passez la souris sur l'icône, un message vous informe que le déploiement de la configuration peut interrompre le trafic.

Le tableau suivant résume l'affichage des avertissements d'interruption d'inspection dans la page du déploiement.

Tableau 3 : Indicateurs d'interruption d'inspection

Type	Inspecter l'interruption	Description
Défense contre les menaces	**Inspecter interruption** ( )Oui	Au moins une configuration interromprait l'inspection de l'appareil si elle était déployée; elle pourrait aussi interrompre le trafic, selon la façon dont l'appareil gère le trafic. Vous pouvez développer la liste de configuration du périphérique pour obtenir plus d'informations.
	--	Les configurations déployées n'interrompent pas le trafic sur l'appareil.
	Indéterminé	Le système ne peut pas déterminer si une configuration déployée est susceptible d'interrompre le trafic sur le périphérique. Un état indéterminé s'affiche avant le premier déploiement, après une mise à niveau logicielle, ou, dans certains cas, lors d'un appel d'assistance.
	Erreurs ( )	Le système ne peut pas déterminer l'état en raison d'une erreur interne. Annulez l'opération et cliquez à nouveau sur **Deploy** (déployer) pour permettre au système de déterminer à nouveau l'état en lien avec **Inspect Interruption**. Si le problème persiste, communiquez avec le service d'assistance.
capteur	--	L'appareil déterminé comme *capteur* n'est pas l'appareil défense contre les menaces ; le système ne détermine pas si une configuration déployée peut interrompre le trafic sur cet appareil.

Pour en savoir plus sur toutes les configurations qui redémarrent le processus Snort pour tous les types d'appareils, consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11.

Inspecter le trafic pendant l'application de la stratégie

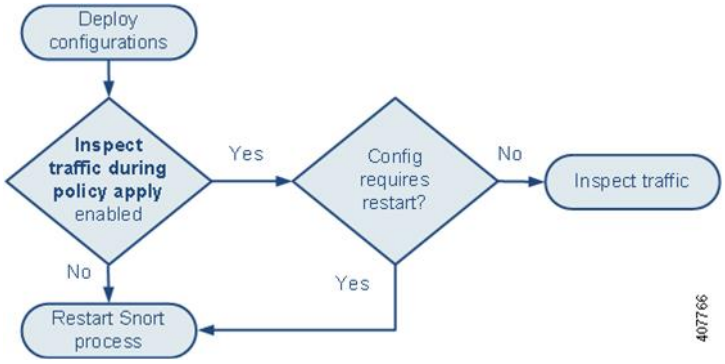
L'inspection du trafic pendant l'application de la politique est un paramètre général de contrôle d'accès avancé qui permet aux périphériques gérés d'inspecter le trafic tout en déployant des modifications de configuration. c'est le cas, sauf si une configuration que vous déployez nécessite le redémarrage du processus Snort. Vous pouvez configurer les options suivantes :

- Activé : le trafic est inspecté pendant le déploiement, sauf si certaines configurations nécessitent le redémarrage du processus Snort.

  Lorsque les configurations que vous déployez ne nécessitent pas de redémarrage Snort, le système utilise initialement la politique de contrôle d'accès actuellement déployée pour inspecter le trafic et bascule pendant le déploiement vers la politique de contrôle d'accès que vous déployez.

- Désactivé : le trafic n'est pas inspecté pendant le déploiement. Le processus Snort redémarre toujours lorsque vous déployez.

Le graphique suivant illustre comment les redémarrages Snort peuvent se produire lorsque vous activez ou désactivez **le trafic d'inspection pendant l'application de la politique**.



Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 9 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11.

Comportement du trafic au redémarrage de Snort

Les tableaux suivants expliquent comment différents appareils gèrent le trafic au redémarrage du processus Snort.

Tableau 4 : Effets de Défense contre les menaces et de Défense contre les menaces virtuelles du redémarrage sur le trafic

Configuration de l'interface	Comportement du trafic au redémarrage
en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	abandonné

Configuration de l'interface	Comportement du trafic au redémarrage
en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	réussi sans inspection Certains paquets peuvent être retardés dans la mémoire tampon pendant plusieurs secondes avant que le système ne reconnaisse que Snort est en panne. Ce délai peut varier en fonction de la répartition de la charge. Cependant, les paquets mis en mémoire tampon finissent par être transmis.
routé, transparent (y compris EtherChannel, redondant, sous-interface) lorsque **preserve-connection** est activé (**configure snort preserve-connection enable**; réglage par défaut) Pour en savoir plus, consultez Référence des commandes de défense contre les menaces de Cisco Secure Firewall.	flux TCP/UDP existants : transmis sans inspection tant qu'au moins un paquet arrive alors que Snort est inactif flux TCP/UDP nouveaux et tous les flux qui ne font pas partie des protocoles TCP/UDP : abandon Signalons que trafic suivant est abandonné même lorsque l'option **preserve-connection** est activée : • texte en clair, trafic de tunnel de préfiltre intercommunication qui correspond à une action de règle **Analyze** ou à une action de politique par défaut **Analyze all tunnel traffic** • connexions qui ne correspondent pas à une règle de contrôle d'accès et sont plutôt gérées par l'action par défaut. • trafic TLS/SSL déchiffré • un flux de recherche sécurisée • un flux de portail captif
routé, transparent (y compris EtherChannel, redondant, sous-interface) : option **preserve-connection** désactivée (**configure snort preserve-connection disable**)	abandonné
en ligne : tap mode (mode Tap)	paquet de sortie immédiatement, copie contourne Snort
passif	sans interruption, sans inspection

Remarque Outre la gestion du trafic lorsque le processus Snort est arrêté pendant qu'il redémarre, le trafic peut également passer sans inspection ou être abandonné lorsque le processus Snort est occupé, selon la configuration de l'option Snort Fail Open (non-conformité de Snort) **Busy (occupé)** (voir Configurer un ensemble en ligne). Un périphérique prend en charge l'option Failsafe ou Snort Fail Open, mais pas les deux.

Remarque Lorsque le processus Snort est occupé, mais pas arrêté pendant le déploiement de la configuration, certains paquets peuvent être abandonnés sur les interfaces routées, commutées ou transparentes si la charge totale du CPU dépasse 60 %.

Avertissement Ne redémarrez pas le système pendant que la mise à niveau de la règle Snort est en cours.

Les abandons Snort-busy se produisent lorsque Snort n'est pas en mesure de traiter les paquets assez rapidement. Lina ne sait pas si Snort est occupé en raison d'un retard de traitement, ou s'il est bloqué ou en raison d'un blocage d'appel. Lorsque la file d'attente de transmission est pleine, des abandons Snort-busy se produisent. En fonction de l'utilisation de la file d'attente de transmission, Lina tentera d'accéder si la file d'attente est traitée correctement.

Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation

Le déploiement de l'une des configurations suivantes, à l'exception de l'AAB, redémarre le processus Snort, comme décrit précédemment. Le déploiement d'AAB n'entraîne pas de redémarrage, mais une latence excessive des paquets active la configuration AAB actuellement déployée, entraînant un redémarrage partiel du processus Snort.

Paramètres avancés de politique de contrôle d'accès

- Procédez au déploiement lorsque l'option **Inspect Traffic During Policy Apply** (inspection du trafic pendant l'application de la politique) est désactivée.
- Ajoutez ou supprimez une politique SSL.

Politique de fichier

Déployez la première ou la dernière des configurations suivantes : vous observerez que même si le déploiement de ces configurations de politique de fichiers n'entraîne pas de redémarrage, le déploiement de configurations sans politique de fichier peut entraîner des redémarrages.

- Prenez l'une des mesures suivantes :
  - Activez ou désactivez **Inspect Archives** lorsque la politique de contrôle d'accès déployée comprend au moins une politique de fichiers.
  - Ajoutez la première ou supprimez la dernière règle de politique de fichier lorsque l'inspection des archives (**Inspect Archives**) est activée (notez qu'au moins une règle est nécessaire pour que l'**inspection des archives** ait un sens).
- Activez ou désactivez **Store files** (stocker des fichiers) dans une règle de détection de fichiers (**Detect Files**) ou de blocage de fichiers (**Block Files**).
- Ajoutez la première ou supprimez la dernière règle de fichier active qui combine l'action de règle de recherche de logiciels malveillants dans le nuage (**Malware Cloud Lookup**) ou de blocage de logiciels malveillants (**Block Malware**) avec une option d'analyse (**Spero Analysis ou MSEXE**, **Dynamic Analysis**, ou encore **Local Malware Analysis**) ou une option de stockage de fichiers (**Malware** pour

les programmes malveillants, **Unknown** pour les fichiers inconnus, **Clean** pour les fichiers fiables ou **Custom** pour un stockage personnalisé).

Notez que les règles de contrôle d'accès qui déploient ces configurations de politiques de fichiers vers des zones de sécurité ou des zones de tunnel engendrent un redémarrage uniquement lorsque votre configuration remplit les conditions suivantes :

- Les zones de sécurité source ou de destination dans votre règle de contrôle d'accès doivent correspondre aux zones de sécurité associées aux interfaces sur les appareils cibles.
- À moins que la zone de destination de votre règle de contrôle d'accès ne soit définie sur *any* (n'importe laquelle), une zone de tunnel source dans la règle doit correspondre à une zone de tunnel affectée à une règle de tunnel dans la politique de préfiltre.

Politique d'identité

- Lorsque le déchiffrement SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès n'inclut pas de politique SSL), ajoutez la première ou supprimez la dernière règle d'authentification active.

  Une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Détection du réseau

- Activez ou désactivez la détection d'utilisateur basée sur le trafic non autorisée sur les protocoles HTTP, FTP ou MDNS, en utilisant la politique de découverte de réseau.

Gestion des périphériques

- MTU : Modifiez la valeur MTU la plus élevée parmi toutes les interfaces qui ne sont pas des interface de gestion sur un périphérique.
- Automatic Application Bypass (AAB): La configuration AAB actuellement déployée s'active lorsqu'un dysfonctionnement du processus Snort ou une mauvaise configuration de l'appareil entraîne un temps de traitement excessif pour un seul paquet. Le résultat est un redémarrage partiel du processus Snort pour réduire la latence extrêmement élevée ou empêcher un blocage complet du trafic. Ce redémarrage partiel entraîne le passage de quelques paquets sans inspection, ou leur abandon, selon la configuration de la gestion du trafic sur l'appareil.

Mises à jour

- Mise à jour du système : Déployez les configurations la première fois après une mise à jour logicielle qui comprend une nouvelle version du processus binaire Snort ou de la bibliothèque d'acquisition de données (DAQ).
- VDB : Pour les appareils gérés exécutant Snort 2, le déploiement de configurations la première fois après l'installation d'une mise à jour de base de données de vulnérabilités (VDB) qui inclut des modifications applicables aux appareils gérés nécessitera un redémarrage du moteur de détection et pourrait entraîner une interruption temporaire du trafic. Pour ces derniers, un message vous avertit lorsque vous sélectionnez le centre de gestion pour commencer l'installation. Le dialogue de déploiement fournit des avertissements

supplémentaires pour les défense contre les menaces appareils lorsque des modifications de la VDB sont en attente. Les mises à jour de la VDB qui s'appliquent uniquement à la centre de gestion ne provoquent pas de redémarrage du moteur de détection, et vous ne pouvez pas les déployer.

Pour les appareils gérés exécutant Snort 3, le déploiement des configurations la première fois après l'installation d'une mise à jour de la base de données de vulnérabilités (VDB) peut interrompre temporairement la détection des applications, mais il n'y aura aucune interruption de trafic.

Sujets connexes

Déployer les modifications de configuration, à la page 16
Scénarios de redémarrage de Snort, à la page 7

Modifications qui redémarrent immédiatement le processus Snort

Les modifications suivantes redémarrent immédiatement le processus Snort sans passer par le processus de déploiement. La façon dont le redémarrage influe sur le trafic dépend de la façon dont le périphérique cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort, à la page 9 pour obtenir de plus amples renseignements.

- Effectuez l'une des actions suivantes concernant les applications ou les détecteurs d'applications :
  - Activer ou désactiver un détecteur de système ou d'application personnalisée.
  - Supprimer un détecteur personnalisé activé.
  - **Enregistrer et réactiver** un détecteur personnalisé activé.
  - Créer une application définie par l'utilisateur

  Un message vous avertit de la poursuite du redémarrage du processus Snort et vous permet de l'annuler; le redémarrage se produit sur tout périphérique géré dans le domaine actuel ou dans l'un de ses domaines enfants.
- Créer ou rompre une paire défense contre les menaces à haute disponibilité

  Un message vous avertit que la poursuite de la création d'une paire à haute disponibilité redémarre le processus Snort sur les périphériques principal et secondaire et vous permet de l'annuler.

Exigences et conditions préalables pour la gestion des politiques

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin

- Administrateur de réseau
- Approbateur de sécurité

Bonnes pratiques pour le déploiement des modifications de configuration

Voici des consignes relatives au déploiement des modifications de configuration.

Connexion de gestion fiable

La connexion de gestion entre centre de gestion et le périphérique est un canal de communication sécurisé chiffré TLS-1.3 entre le périphérique et lui.

Vous n'avez pas besoin d'exécuter ce trafic sur un tunnel chiffré supplémentaire comme un VPN de site à site pour des raisons de sécurité. Si le VPN tombe en panne, par exemple, vous perdrez votre connexion de gestion. Nous vous recommandons donc un chemin de gestion simple.

⚠

Mise en garde Nous vous déconseillons de passer par un tunnel VPN qui se termine sur le périphérique lui-même. Si vous déployez une modification de configuration qui entraîne la panne du VPN, la connexion de gestion sera déconnectée et vous n'aurez aucun moyen de récupérer la configuration sans vous connecter directement au périphérique.

Si le trafic de gestion sort d'une interface de terminaison VPN, veillez à exclure le trafic de gestion du tunnel VPN.

Nombre maximal de déploiements simultanés

Vous ne devez pas déployer à plus de 25 % du nombre maximal de périphériques autorisés pour un centre de gestion dans une même tâche. Par exemple, pour FMCv300, la taille maximale de la tâche doit être de 75 périphériques (25 % de 300). Le déploiement simultané sur plus de périphériques peut entraîner des problèmes de performances.

Déploiement de politiques partagées

Pour de meilleures performances, déployez sur les périphériques qui utilisent les mêmes politiques. Créez des tâches de déploiement distinctes pour chaque groupe de périphériques qui partagent des politiques.

Temps de déploiement et limites de mémoire

Le temps nécessaire au déploiement dépend de plusieurs facteurs, notamment les suivants :

- Les configurations que vous envoyez à l'appareil. Par exemple, si vous augmentez considérablement le nombre d'entrées de renseignements sur la sécurité que vous bloquez, le déploiement peut prendre plus de temps.
- Modèle d'appareil et mémoire. Sur les appareils offrant moins de mémoire, le déploiement peut prendre plus de temps.

Ne dépassez pas la capacité de vos appareils. Si vous dépassez le nombre maximal de règles ou de politiques prises en charge par un périphérique cible, le système affiche un avertissement. Le maximum dépend de plusieurs facteurs, non seulement de la mémoire et du nombre de processeurs sur l'appareil, mais aussi de la complexité des règles et des politiques. Pour en savoir plus sur l'optimisation des politiques et des règles, consultez Bonnes pratiques pour les règles de contrôle d'accès.

Utilisez une fenêtre de maintenance pour réduire l'impact des interruptions de trafic.

Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où les interruptions auront le moins d'impact.

Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 9 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11.

Pour les appareils défense contre les menaces , la colonne **Inspect Interruption (inspecter l'interruption)** dans la boîte de dialogue Deploy (déployer) vous avertit lorsque le déploiement risque d'interrompre le flux de trafic ou l'inspection. Vous pouvez procéder au déploiement, l'annuler ou le retarder; consultez Redémarrer les avertissements pour les appareils, à la page 7 pour obtenir plus d'informations.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 7

Déployer la configuration

Après avoir configuré votre déploiement, et chaque fois que vous modifiez cette configuration, vous devez déployer les modifications sur les périphériques concernés. Vous pouvez afficher l'état du déploiement dans le centre de messages.

Le déploiement met à jour les composants suivants :

- Les configurations des périphériques et des interfaces
- Les politiques liées au périphérique : NAT, VPN, QoS, les paramètres de la plateforme
- Le contrôle d'accès et politiques connexes : DNS, fichier, identité, intrusion, analyse de réseau, préfiltre, SSL
- Politique de découverte du réseau
- Mises à jour des règles de prévention des intrusions
- Les configurations et les objets associés à l'un de ces éléments

Vous pouvez configurer le système pour qu'il se déploie automatiquement en programmant une tâche de déploiement ou en configurant le système pour qu'il se déploie lors de l'importation des mises à jour des règles de prévention des intrusions. L'automatisation du déploiement des politiques est particulièrement utile si vous autorisez les mises à jour des règles de prévention des intrusions à modifier les politiques de base fournies par le système pour l'analyse des intrusions et du réseau. Les mises à jour des règles de prévention des intrusions peuvent également modifier les valeurs par défaut des options de prétraitement et de performance avancé dans vos politiques de contrôle d'accès.

Dans un déploiement multidomaine, vous pouvez déployer des modifications pour n'importe quel domaine auquel votre compte d'utilisateur appartient :

- Passez à un domaine ascendant pour déployer les modifications sur tous les sous-domaines en même temps.
- Passez à un domaine descendant pour déployer les modifications uniquement sur ce domaine.

Déployer les modifications de configuration

Après avoir modifié les configurations, déployez-les sur les appareils ciblés. Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où une interruption du flux de trafic ou de l'inspection aura le moins d'impact.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 9 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11.

Avant de commencer

- Assurez-vous que tous les périphériques gérés utilisent la même révision de l'objet des zones de sécurité. Si vous avez modifié les objets de la zone de sécurité : Ne déployez les modifications de configuration sur aucun appareil avant d'avoir modifié le paramètre de zone pour les interfaces sur *tous* les appareils que vous souhaitez synchroniser. Vous devez déployer tous les appareils gérés en même temps.
- Pour consulter un aperçu des modifications de déploiement, activez l'accès API REST. Pour activer l'accès à l'API REST, suivez les étapes de la section *Enabling REST API Access (activer l'accès à l'API REST)* dans le Guide d'administration Cisco Secure Firewall Management Center.

Remarque Le processus de déploiement échoue si la configuration du périphérique est lue au niveau de l'interface de la ligne de commande du périphérique pendant le déploiement. N'exécutez pas de commandes telles que **show running-config** pendant le déploiement.

Procédure

Étape 1 Dans la barre de menus de centre de gestion, cliquez sur **Deploy** (déployer).

Étape 2 Pour un déploiement rapide, vérifiez des périphériques spécifiques, puis cliquez sur **Deploy**(déployer) ou sur **Deploy All** (Déployer tout) pour déployer sur tous les périphériques. Sinon, pour obtenir des options de déploiement supplémentaires, cliquez sur **Advanced Deploy**(déploiement avancé).

Le reste de la procédure s'applique à l'écran **Advanced Deploy** (déploiement avancé).

Illustration 1 : Déploiement rapide

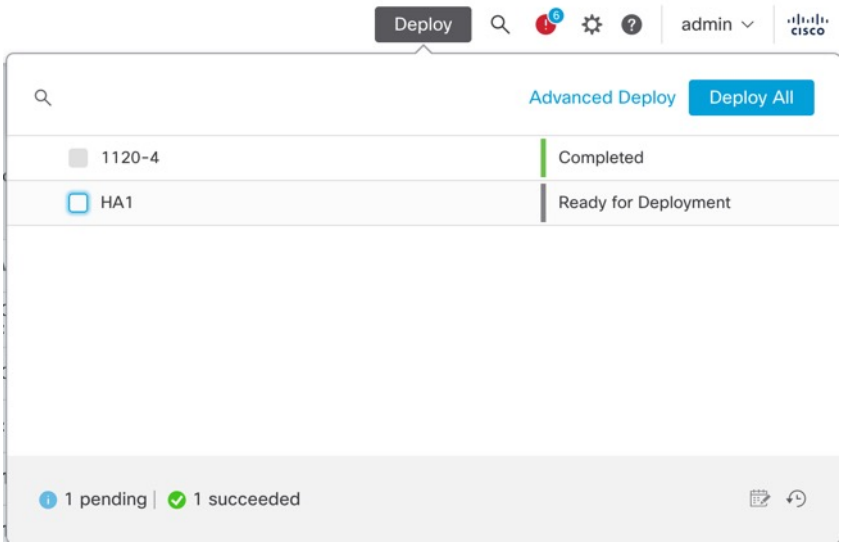
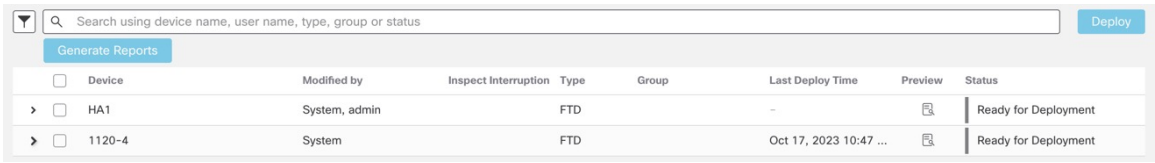
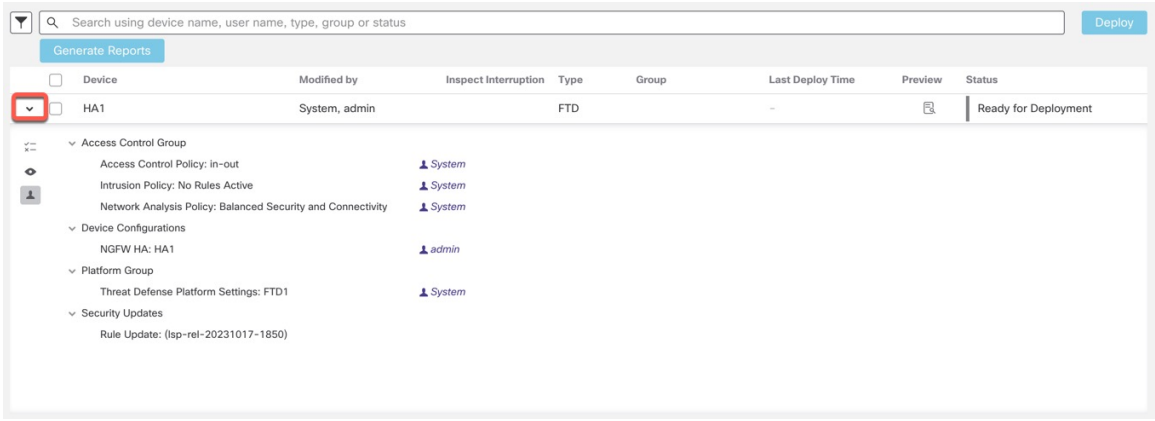


Illustration 2 : Déploiement avancé



Étape 3 Cliquez sur **Flèche développer** (›) pour afficher les modifications de configuration propres au périphérique à déployer.

Illustration 3 : Diversification



- La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets. En développant la liste des appareils, vous pouvez afficher les utilisateurs qui ont modifié les politiques par rapport à chaque liste de politiques. Pour savoir quand l'utilisateur **système** s'affiche (au lieu de l'utilisateur connecté), consultez Nom d'utilisateur du système, à la page 6.

  Remarque Les noms d'utilisateur ne sont pas fournis pour les politiques et objets supprimés.

- La colonne **Inspect Interruption** (inspecter l'interruption) indique si une interruption de l'inspection du trafic peut être entraînée dans l'appareil pendant le déploiement.

  Lorsque l'état indique (Oui) que le déploiement interrompra l'inspection, et peut-être le trafic, sur le périphérique défense contre les menaces , la liste étendue indique les configurations spécifiques causant l'interruption avec le **Inspecter interruption** ( ).

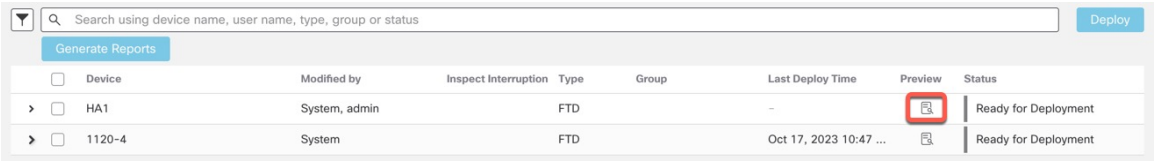
  Si l'entrée est vide dans cette colonne pour un périphérique, cela indique qu'il n'y aura aucune interruption de l'inspection du trafic sur ce périphérique pendant le déploiement.

  Voir Redémarrer les avertissements pour les appareils, à la page 7 pour des informations qui vous aideront à déterminer les configurations qui interrompent l'inspection du trafic et qui risquent d'interrompre le trafic lorsqu'elles sont déployées sur les appareilsdéfense contre les menaces .

- La colonne **Last Modified Time** (moment de la dernière modification) indique la dernière fois que vous avez modifié la configuration.
- La colonne **Preview** (aperçu) vous permet de prévisualiser les modifications pour le prochain déploiement.
- La colonne **Status** (état) indique l'état de chaque déploiement. Pour en savoir plus, consultez Afficher l'état du déploiement, à la page 23.

Étape 4 Dans la colonne **Aperçu**, cliquez sur **Aperçu** ( ) pour voir les modifications de configuration que vous pouvez déployer.

Illustration 4 : Prévisualiser

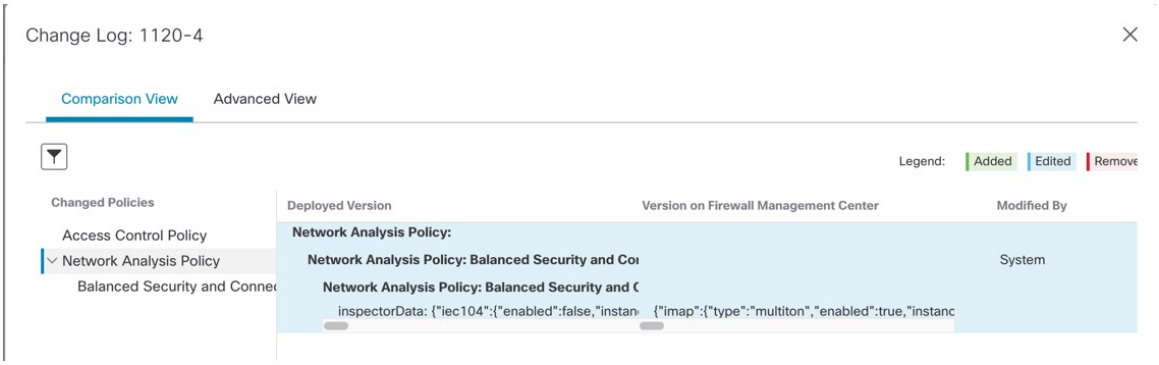


Remarque Si vous modifiez le nom de centre de gestion en **System** ( ) > **Configuration** > **Information**, l'aperçu de déploiement ne précise pas cette modification, mais nécessite un déploiement.

Pour les fonctionnalités non prises en charge pour l'aperçu, consultez Aperçu du déploiement, à la page 2.

L'onglet **Comparaison View** (Affichage de la comparaison) répertorie toutes les modifications apportées aux politiques et aux objets. Le volet gauche répertorie en arborescence tous les différents types de politique qui ont été modifiés sur le périphérique.

Illustration 5 : Affichage de la comparaison



L'icône de **filtre** ( ) vous permet de filtrer les politiques au niveau de l'utilisateur et au niveau des politiques.

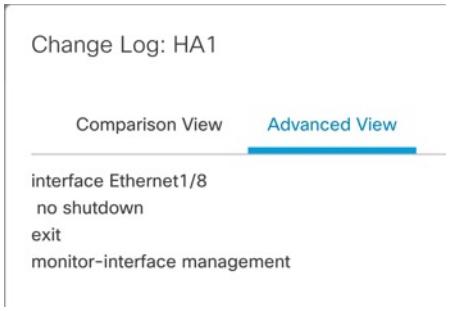
Le volet droit répertorie l'ensemble des ajouts, modifications ou suppressions dans la politique ou l'objet sélectionné dans le volet gauche. Les deux colonnes du volet de droite présentent les derniers paramètres de configuration déployés (dans la colonne **Deployed Version (version déployée)**) par rapport aux modifications qui doivent être déployées (dans la colonne **Version on Firewall Management Center (version sur le centre de gestion du pare-feu)**). Les derniers paramètres de configuration déployés sont dérivés d'un instantané du dernier déploiement sauvegardé dans centre de gestion et non du périphérique. Les couleurs d'arrière-plan des paramètres sont codées selon la légende disponible en haut à droite de la page.

La colonne **Modified By** répertorie les utilisateurs qui ont modifié ou ajouté les paramètres de configuration. Au niveau de la politique, le centre de gestion présente tous les utilisateurs qui ont modifié la politique, et au niveau de la règle, le centre de gestion présente seulement le dernier utilisateur qui a modifié la règle.

Vous pouvez télécharger une copie du journal des modifications en cliquant sur le bouton **Download Report** (télécharger le rapport).

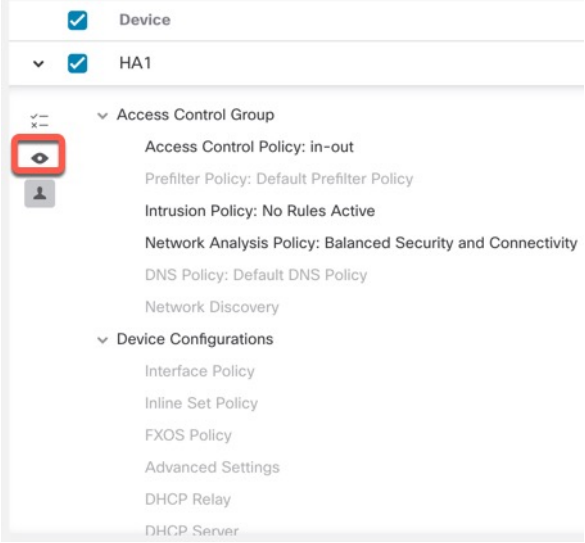
L'onglet **Advanced View** (affichage avancé) affiche les commandes CLI qui seront appliquées. Cet affichage est utile si vous connaissez bien l'interface de ligne de commande d'ASA, qui est utilisée pour le back-end de défense contre les menaces .

Illustration 6 : Affichage avancé



Étape 5 Utilisez **Afficher ou masquer la politique** ( ) pour afficher ou masquer sélectivement les politiques non modifiées connexes.

Illustration 7 : Afficher ou masquer la politique



Étape 6 Cochez la case en regard du nom du périphérique pour déployer toutes les modifications de configuration ou cliquez sur **Sélection de politique** ( ) pour sélectionner des politiques ou des configurations individuelles à déployer tout en retenant les modifications restantes sans les déployer.

Vous pouvez également afficher les modifications interdépendantes pour une politique ou une configuration donnée en utilisant cette option. Le centre de gestion détecte dynamiquement les dépendances entre les politiques (par exemple, entre une politique de contrôle d'accès et une politique d'intrusion), et entre les objets partagés et les politiques. Les modifications interdépendantes sont indiquées à l'aide de balises de couleur pour identifier un ensemble de modifications de déploiement interdépendantes. Lorsqu'une des modifications de déploiement est sélectionnée, les modifications interdépendantes sont automatiquement sélectionnées.

Pour en savoir plus, consultez Déploiement sélectif des politiques, à la page 3.

Remarque

- Lorsque les modifications apportées aux objets partagés sont déployées, les politiques concernées doivent également être déployées avec elles. Lorsque vous sélectionnez un objet partagé pendant le déploiement, les politiques touchées sont automatiquement sélectionnées.
- Le déploiement sélectif n'est pas pris en charge pour les déploiements planifiés et les déploiements utilisant des API REST. Vous ne pouvez opter que pour le déploiement complet de toutes les modifications dans ces cas.
- Les vérifications de pré-déploiement pour les avertissements et les erreurs sont effectuées non seulement sur les politiques sélectionnées, mais sur toutes les politiques qui sont obsolètes. Par conséquent, la liste des avertissements ou des erreurs affiche également les politiques désélectionnées.
- De même, l'indication de la colonne **Inspect Interruption** (inspecter l'interruption) dans la page de déploiement prend en compte toutes les politiques obsolètes et pas seulement les politiques sélectionnées. Pour en savoir plus sur la colonne**Inspect Interruption**, consultez Redémarrer les avertissements pour les appareils, à la page 7.

Étape 7 Après avoir sélectionné les périphériques ou les politiques à déployer, cliquez sur **Estimate** (estimation) pour obtenir une estimation approximative de la durée de déploiement.

Illustration 8 : Estimation

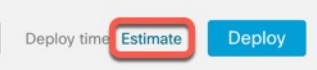
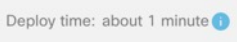


Illustration 9 : Durée de déploiement



La durée est une estimation approximative (avec un degré de précision d'environ 70 %). Le temps réel nécessaire pour le déploiement peut varier dans quelques scénarios. L'estimation est fiable pour des déploiements allant jusqu'à 20 appareils

Lorsqu'une estimation n'est pas disponible, il sera indiqué que les données ne sont pas disponibles, car le premier déploiement réussi sur le périphérique sélectionné est en attente. Cette situation peut se produire après une recréation d'image de centre de gestion, une mise à niveau de version ou un basculement à haute disponibilité.

Remarque L'estimation est incorrecte et peu fiable pour les changements groupés au niveau des politiques (dans le cas de migrations de politiques en bloc) et pour les déploiements sélectifs, car elle est basée sur la technique heuristique.

Étape 8 Cliquez sur **Déployer**.

Étape 9 Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs.

Vous avez les choix suivants :

- Deploy (déployer) : Continuer le déploiement sans résoudre les conditions de mise en garde. Vous ne pouvez pas continuer si le système détecte des erreurs.
- Close (fermer) : Quitter sans déployer. Vous devrez résoudre les conditions d'erreur et de mise en garde, puis réessayer de déployer la configuration.

Prochaine étape

- (Facultatif) Surveillez l'état du déploiement ; voir *Viewing Deployment Messages (affichage des messages de déploiement)*dans Guide d'administration Cisco Secure Firewall Management Center.
- Si le déploiement échoue, consultez Bonnes pratiques pour le déploiement des modifications de configuration, à la page 14.
- Durant le déploiement, s'il y a certains changements de configuration dans le déploiement, l'échec du déploiement peut entraîner une interruption du trafic. Par exemple, dans un environnement de grappe, une configuration erronée d'une adresse IP qui ne se trouve pas dans le même sous-réseau que les adresses IP de site est configurée sur l'interface. En raison de cette erreur, le déploiement échoue et le périphérique tente d'effacer la configuration pendant le traitement de l'opération de restauration. Ensemble, ces événements entraînent un échec du déploiement qui interrompt le trafic.

  Consultez le tableau suivant pour savoir quelles modifications de configuration peuvent entraîner une interruption du trafic en cas d'échec du déploiement.

Changements de configuration	Existe?	Effet sur le trafic?
Modifications apportées au **service de défense contre les menaces** dans une politique de contrôle d'accès	Oui	Oui
VRF	Oui	Oui
Interface	Oui	Oui
Qualité de service	Oui	Oui

Remarque Les changements de configuration interrompant le trafic pendant le déploiement ne sont valables que si le centre de gestion et le défense contre les menaces sont tous deux de version 6.2.3 ou supérieure.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 7

Redéployer les configurations existantes sur un périphérique

Vous pouvez forcer le déploiement de configurations existantes (non modifiées) sur un seul périphérique géré. Nous vous recommandons *fortement* de procéder au déploiement lors d'une période de maintenance ou à un moment où une interruption du flux de trafic ou de l'inspection aura le moins d'impact.

Mise en garde Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Voir Comportement du trafic au redémarrage de Snort, à la page 9 et Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation, à la page 11.

Avant de commencer

Passez en revue les consignes décrites dans Bonnes pratiques pour le déploiement des modifications de configuration, à la page 14.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**.

Étape 2 Cliquez sur **Edit** (✎) à côté du périphérique sur lequel vous souhaitez forcer le déploiement.

Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.

Étape 3 Cliquez sur **Device (périphérique)**.

Étape 4 Cliquez sur **Edit** (✎) à côté de l'en-tête de section **Général**.

Étape 5 Cliquez sur **Forcer le déploiement** (→).

Remarque Le déploiement forcé prend plus de temps que le déploiement normal, car il implique la génération complète des règles de politique à déployer sur FTD.

Étape 6 Cliquez sur **Deploy** (déployer).

Le système détecte les erreurs ou les avertissements relatifs aux configurations que vous déployez. Vous pouvez cliquer sur **Proceed** (Continuer) pour poursuivre sans résoudre les conditions d'avertissement. Cependant, vous ne pouvez pas continuer si le système détecte des erreurs.

Prochaine étape

- (Facultatif) Surveillez l'état du déploiement ; voir *Viewing Deployment Messages (affichage des messages de déploiement)*dans Guide d'administration Cisco Secure Firewall Management Center.
- Si le déploiement échoue, consultez Bonnes pratiques pour le déploiement des modifications de configuration, à la page 14.

Sujets connexes

Scénarios de redémarrage de Snort, à la page 7

Gérer les déploiements

Afficher l'état du déploiement

Dans la page Déploiement, la colonne **Status** (état) indique l'état du déploiement de chaque appareil. Si un déploiement est en cours, l'état actuel de la progression du déploiement s'affiche, sinon l'un des états suivants s'affiche :

- Pending (en attente) : Indique que des modifications doivent être apportées au périphérique.
- Warnings or errors (avertissements ou erreurs) : Indique que les vérifications préalables au déploiement ont détecté des avertissements ou des erreurs pour le déploiement et que vous n'avez pas effectué le déploiement. Vous pouvez poursuivre le déploiement en cas d'avertissements, mais pas en cas d'erreurs.

Remarque La colonne d'état (Status) précise l'état d'avertissement ou d'erreur uniquement pour une session utilisateur unique dans la page de déploiement. Si vous quittez la page ou actualisez la page, l'état passe à « pending » (en attente).

- Failed (échec) : Indique que la tentative de déploiement précédente a échoué. Cliquez sur l'état (Status) pour afficher les détails.

- In queue (en file d'attente) : Indique que le déploiement est lancé et que le système n'a pas encore commencé le processus de déploiement.
- Completed (terminé) : Indique que le déploiement a été effectué avec succès.

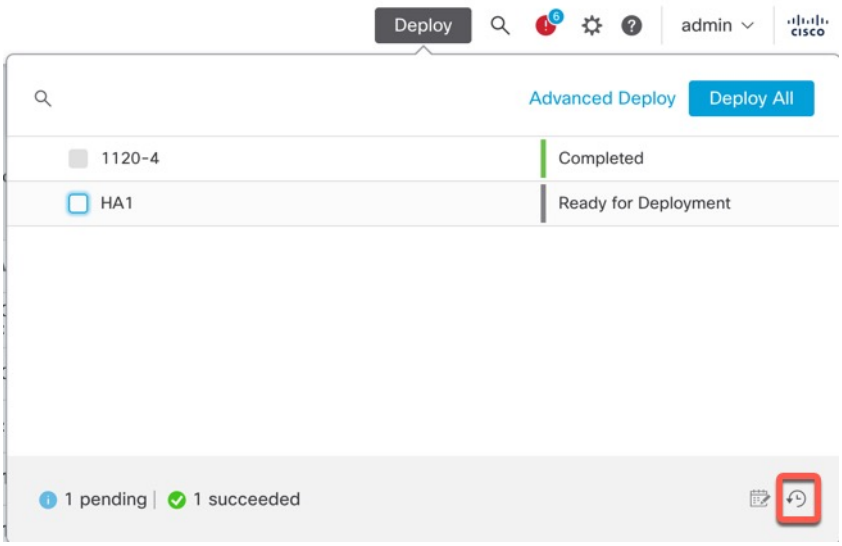
Afficher l'historique des déploiements

Dans l'historique de déploiement, les 10 derniers déploiements réussis, les 5 derniers déploiements ayant échoué et les 5 derniers déploiements de restauration sont capturés.

Procédure

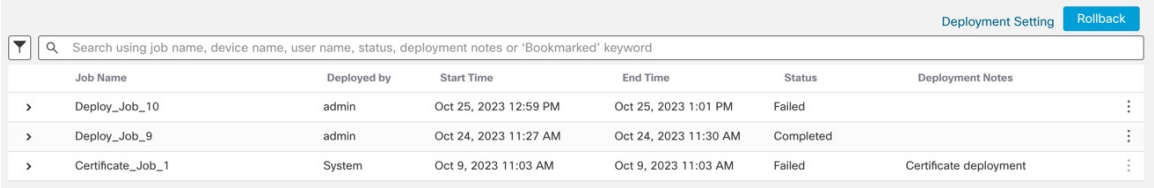
Étape 1 Dans la barre de menu centre de gestion, cliquez sur **Déployer**, puis sur **Deployment History** ( ).

Illustration 10 : Icône de l'historique de déploiement



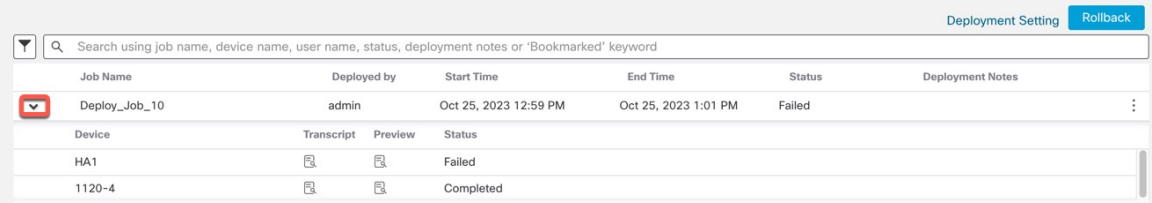
Une liste de toutes les tâches de déploiement et de restauration précédentes s'affiche dans l'ordre chronologique inverse.

Illustration 11 : Page d'historique des déploiements



Étape 2 Cliquez sur **Flèche développer** ( ) en regard de la tâche de déploiement requise pour afficher les appareils inclus dans la tâche et leurs états de déploiement.

Illustration 12 : Diversification



- Affichez les remarques dans la colonne **Notes de déploiement**.

  Les notes de déploiement sont des notes personnalisées qu'un utilisateur peut ajouter dans le cadre du déploiement. Ces notes sont facultatives.

Étape 3 (Facultatif) Cliquez sur **Détails de la transcription** ( ) pour afficher les commandes envoyées au périphérique et les réponses reçues.

Illustration 13 : Icône des détails de la transcription

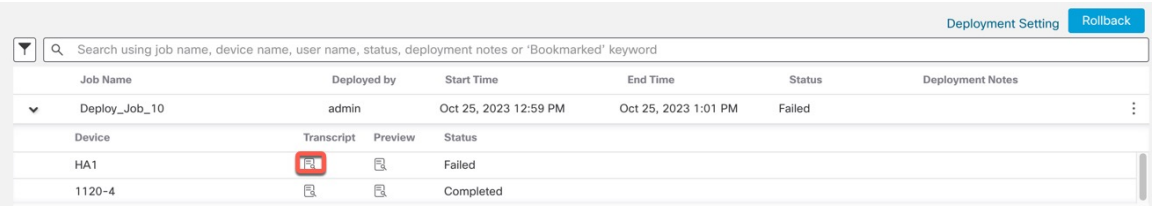
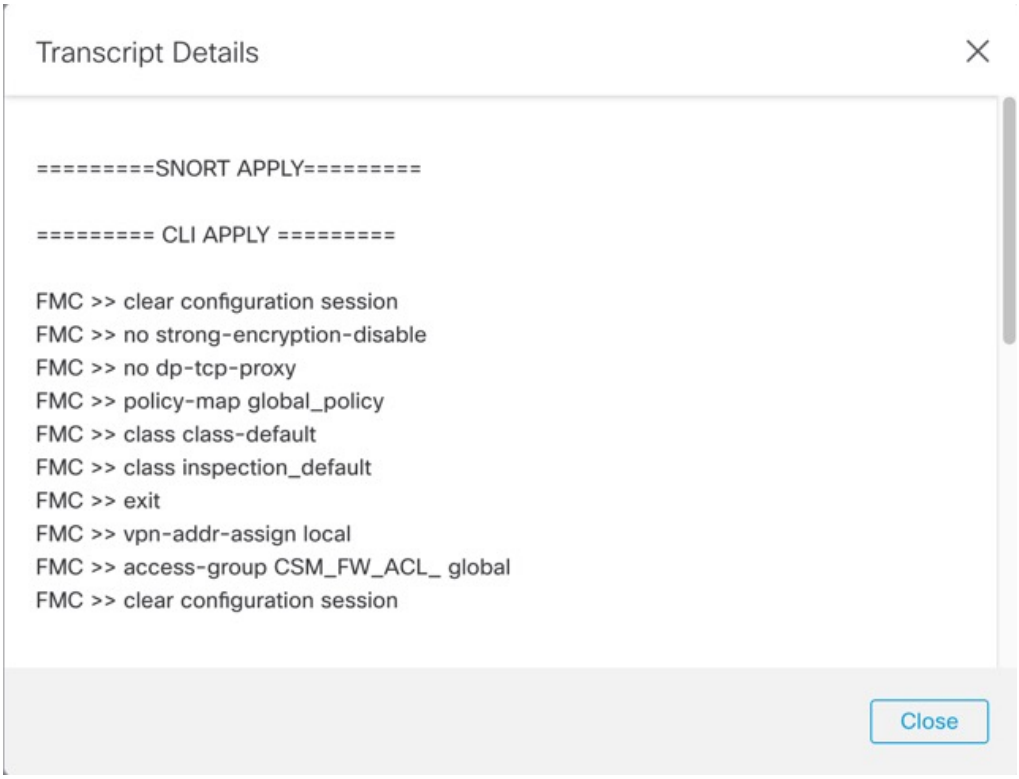


Illustration 14 : Détails de la transcription



Elle comprend les sections suivantes :

- **Snort Apply** (Appliquer Snort) : en cas d'échec ou de réponse des politiques liées à Snort, les messages sont affichés dans cette section. Normalement, la section est vide.
- **CLI Apply** (Appliquer la CLI) : cette section traite des fonctions qui sont configurées à l'aide de commandes envoyées au périphérique.
- **Infrastructure Messages** : Cette section affiche l'état des différents modules de déploiement.

Dans la section **CLI Apply**, la transcription de déploiement comprend les commandes envoyées à l'appareil et toutes les réponses renvoyées par l'appareil. Ces réponses peuvent être des messages informatifs ou des messages d'erreur. En cas d'échec des déploiements, recherchez les messages indiquant des erreurs dans les commandes. L'examen de ces erreurs peut être particulièrement utile si vous utilisez des règles FlexConfig pour configurer des fonctionnalités personnalisées. Ces erreurs peuvent vous aider à corriger le script dans l'objet FlexConfig qui tente de configurer les commandes.

Remarque Il n'y a aucune distinction faite dans la transcription entre les commandes envoyées pour les fonctionnalités gérées et celles générées par les politiques FlexConfig.

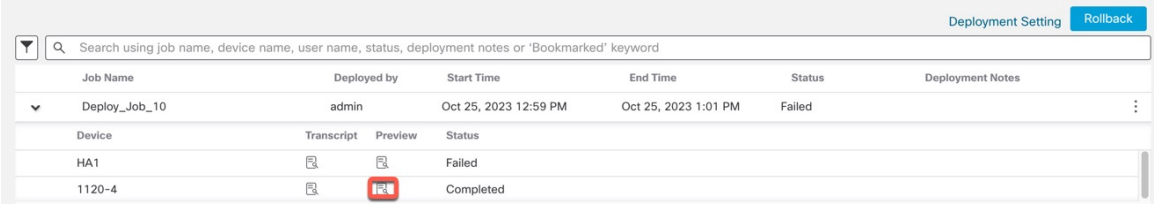
Par exemple, la séquence suivante montre que a centre de gestion envoyé des commandes pour configurer GigabitEthernet0/0 avec le nom logique **extérieur**. L'appareil a répondu qu'il réglait automatiquement le niveau de sécurité sur 0.Défense contre les menaces n'utilise le niveau de sécurité pour rien.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

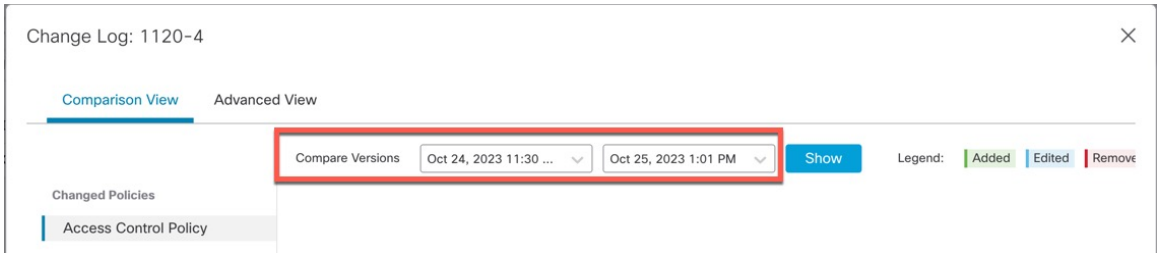
Étape 4 (Facultatif) Cliquez sur **Aperçu** ( ) pour afficher les modifications de politique et d'objet déployées sur le périphérique par rapport à la version précédemment déployée.

Illustration 15 : icône Aperçu



1. Pour comparer deux versions et afficher le journal des modifications, sélectionnez les versions requises dans les listes déroulantes et cliquez sur le bouton **Show (afficher)**. Les zones déroulantes affichent le nom de la tâche de déploiement et l'heure de fin du déploiement.

Illustration 16 : Comparer les versions



Remarque Les zones de liste déroulante affichent également les échecs de déploiement.

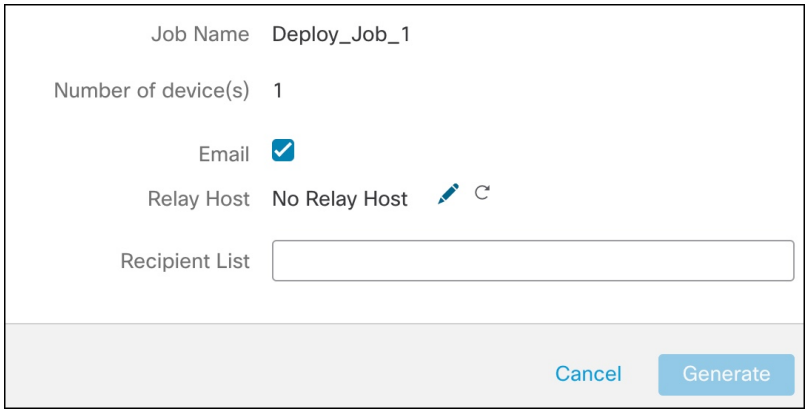
2. La colonne **Modified By** (modifié par) répertorie les utilisateurs qui ont modifié les politiques ou les objets.
    1. Au niveau de la politique, centre de gestion affiche tous les noms d'utilisateurs qui ont modifié la politique.
    2. Au niveau de la règle, centre de gestion affiche le dernier utilisateur qui a modifié la règle.
3. Vous pouvez télécharger une copie du journal des modifications en cliquant sur le bouton **Download Report** (télécharger le rapport).

Remarque
- L'aperçu de l'historique de déploiement n'est pas pris en charge pour les inscriptions de certificats, les opérations haute disponibilité et les échecs de déploiement.
- Lorsqu'un périphérique est enregistré, l'aperçu n'est pas pris en charge pour l'enregistrement de l'historique des tâches créé.

Étape 5 (Facultatif) En regard de chaque tâche de déploiement, cliquez sur l'icône **Plus** (⋮) et exécutez d'autres actions :

- **Marque-page** : pour mettre la tâche de déploiement en signet.
- **Edit Deployment Notes**(modifier les notes de déploiement) : pour modifier vos notes de déploiement personnalisées que vous avez ajoutées pour une tâche de déploiement.
- **Generate Report**(générer un rapport) : pour générer un rapport sur le déploiement, qui peut être utilisé à des fins d'audit. Ce rapport comprend les propriétés de la tâche avec des informations d'aperçu et de transcription. Le rapport peut être téléchargé en tant que fichier PDF.
    1. Cliquez sur **Generate Report (** générer un rapport) pour générer un rapport de déploiement.

Illustration 17 : Produire un rapport



2. Dans la fenêtre contextuelle **Generate Report**, cochez la case **Email** (courriel).
3. Le rapport peut également être envoyé par courriel si l'hôte de relais de messagerie est configuré. Si l'hôte de relais de messagerie n'est pas configuré, utiliser l'icône **Modifier** ( ) pour configurer ou modifier l'hôte de relais de messagerie. *Configurer un hôte de relais de messagerie et une adresse de notification* dans Guide d'administration Cisco Secure Firewall Management Center.
4. Dans la **liste de destinataires**, vous pouvez saisir plusieurs adresses courriel, séparées par des points-virgules.
5. Cliquez sur **Generate** pour générer le rapport. Ce rapport est envoyé par courriel aux destinataires.
6. Dans l'onglet de tâches Notifications, vous pouvez suivre la progression. Une fois la génération du rapport terminée, cliquez sur le lien dans l'onglet des tâches de notification pour télécharger le rapport au format PDF.

Comparer les stratégies

Pour passer en revue les modifications apportées aux politiques en matière de conformité avec les normes de votre entreprise ou pour optimiser les performances du système, vous pouvez examiner les différences entre deux politiques ou entre une politique enregistrée et la configuration en cours.

Vous pouvez comparer les types de politiques suivants :

- DNS
- Fichier
- Santé
- Identité
- Prévention des intrusions (uniquement les politiques Snort 2)
- Analyse du réseau
- SSL

La vue de comparaison affiche les deux politiques côte à côte. Les différences entre les deux politiques sont mises en évidence :

- Le bleu indique que le paramètre en surbrillance est différent dans les deux politiques et que la différence est indiquée en rouge.
- Le vert indique que le paramètre en surbrillance apparaît dans une politique mais pas dans l'autre.

Avant de commencer

Vous ne pouvez comparer les politiques que si vous disposez des droits d'accès et des licences requises pour une politique donnée et que vous êtes dans le bon domaine pour configurer la politique.

Procédure

Étape 1 Accédez à la page de gestion de la politique que vous souhaitez comparer :

- DNS—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**
- File (fichier)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)**
- Health (intégrité)—**System** (⚙) > **Politique** > **d'intégrité**
- Identity (identité)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)**
- Intrusion—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**

  Remarque Vous pouvez comparer uniquement les politiques de Snort 2.

- Network Analysis (analyse du réseau)—**Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**

  Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

- SSL—**Politiques** > **Contrôle d'accès** > **Déchiffrement**

Étape 2 Cliquez sur **Compare Policies** (comparer les politiques).

Étape 3 Dans la liste déroulante **Compare Against**, choisissez le type de comparaison que vous souhaitez effectuer :

- Pour comparer deux politiques différentes, sélectionnez **Other Policy** (autre politique).
- Pour comparer deux révisions de la même politique, sélectionnez **Other Revision** (autre révision).
- Pour comparer une autre politique à la politique actuellement active, sélectionnez **Running Configuration** (configuration en cours).

Étape 4 Selon le type de comparaison que vous choisissez, vous avez les choix suivants :

- Si vous comparez deux politiques différentes, choisissez les politiques que vous souhaitez comparer dans les listes déroulantes **Policy A** et **Policy B**.
- Si vous comparez la configuration en cours à une autre politique, choisissez la deuxième politique dans la liste déroulante **Policy B**.

Étape 5 Cliquez sur **OK**.

Étape 6 Passez en revue les résultats de la comparaison :

- Comparison Viewer (visualiseur de comparaison) : Pour utiliser le visualiseur de comparaison de parcourir individuellement les différences de politique, cliquez sur **Previous** (précédent) ou **Next** (suivant) au-dessus de la barre de titre.
- Comparison Report (rapport de comparaison) : Pour générer un rapport PDF qui répertorie les différences entre les deux politiques, cliquez sur **Comparison Report** (rapport de comparaison).

Générer des rapports sur les politiques appliquées

Pour la plupart des politiques, vous pouvez générer deux types de rapports. Un rapport sur une seule politique fournit des détails sur la configuration enregistrée actuelle de la politique, tandis qu'un rapport de comparaison répertorie uniquement les différences entre deux politiques. Vous pouvez générer un rapport de politique unique pour tous les types de politiques, à l'exception de l'intégrité.

Remarque Les rapports sur les intrusions combinent les paramètres de la politique de base avec ceux des couches de politique et ne font aucune distinction entre les paramètres provenant de la politique de base ou de la couche de politique.

Avant de commencer

Vous pouvez générer des rapports sur des politiques uniquement si vous disposez des droits d'accès et des licences requises pour les politiques spécifiques et si vous êtes dans le bon domaine pour la configuration des politiques en cause.

Procédure

Étape 1 Accédez à la page de gestion de la politique pour laquelle vous souhaitez générer un rapport :

- Access Control (contrôle d'accès)—**Politiques** > **Contrôle d'accès**
- DNS—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **DNS**
- File (fichier)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Malware & File (programme malveillant et fichier)**
- Health (intégrité)—**System** (⚙) > **Politique** > **d'intégrité**
- Identity (identité)—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)**
- Intrusion—**Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**
- NAT— **Devices (appareils)** > **NAT**
- Network Analysis (analyse du réseau)—**Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**

  Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

- SSL—**Politiques** > **Contrôle d'accès** > **Déchiffrement**

Étape 2 Cliquez sur **Rapport** ( ) à côté de la politique pour laquelle vous souhaitez générer un rapport.

Historique des déploiements de la configuration

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Générer un rapport et envoyez-le par courriel lorsque vous déployez des modifications de configuration.	7.2	N'importe lequel	Vous pouvez désormais générer un rapport pour n'importe quel déploiement. Écrans nouveaux ou modifiés : **icônePlus ( )Déployer** > **Deployment History** ( ) > **Générer un rapport**

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.