Meilleures pratiques : scénarios d'utilisation pour FTD

Les rubriques suivantes expliquent certaines tâches courantes que vous pourriez vouloir accomplir à l'aide de Cisco Firepower Threat Defense en utilisant FDM. Ces scénarios d'utilisation sont fondés sur l'hypothèse voulant que vous ayez terminé la configuration du périphérique avec l'assistant et que vous ayez conservé cette configuration initiale. Même si vous avez modifié la configuration initiale, vous devriez être en mesure d'utiliser ces exemples pour comprendre comment utiliser le produit.

Comment configurer l'appareil en FDM

Après avoir terminé la configuration avec l'assistant, vous devriez avoir un périphérique qui fonctionne avec quelques règles de base en place :

- Interfaces interne et externe. Aucune autre interface de données n'est configurée.
- (Firepower 4100/9300) Les interfaces de données ne sont pas préconfigurées.
- (ISA 3000) Un groupe de ponts contient 2 interfaces internes et 2 interfaces externes. Vous devez définir manuellement l'adresse IP de BVI1 pour terminer votre configuration.
- (À l'exception de Firepower 4100/9300) Zones de sécurité pour les interfaces interne et externe.
- (À l'exception de Firepower 4100/9300) Une règle d'accès qui fait confiance au trafic interne vers externe. Pour l'ISA 3000, il existe des critères d'accès qui autorisent tout le trafic de l'intérieur vers l'extérieur et de l'extérieur vers l'intérieur.
- (À l'exception de Firepower 4100/9300 et ISA 3000) Une règle d'interface NAT qui traduit tout le trafic interne vers externe vers des ports uniques sur l'adresse IP de l'interface externe.

- (À l'exception de Firepower 4100/9300 et ISA 3000) Un serveur DHCP fonctionnant sur l'interface interne .

Les étapes suivantes donnent un aperçu des fonctionnalités supplémentaires que vous pourriez souhaiter configurer. Veuillez cliquer sur le bouton d'aide (**?**) dans une page pour obtenir des renseignements détaillés sur chaque étape.

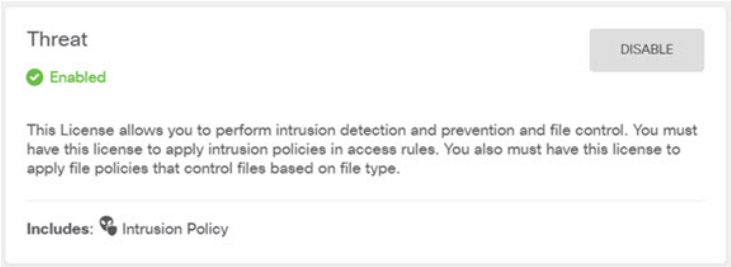
Procédure

Étape 1 Choisissez **Device (périphérique)**, cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Smart License** (Licence Smart).

Cliquez sur **Enable** (Activer) pour chacune des licences facultatives que vous souhaitez utiliser : Menace , Programme malveillant, URL. Si vous avez enregistré l'appareil pendant la configuration, vous pouvez également activer la licence VPN RA souhaitée. Lisez l'explication sur chaque licence si vous ne savez pas si vous en avez besoin.

Si vous n'êtes pas enregistré, vous pouvez le faire à partir de cette page. Cliquez sur **Register Device (enregistrer l'appareil)** et suivez les instructions. Veuillez vous inscrire avant l'expiration de la licence d'évaluation.

Par exemple, une licence (license Threat) activée devrait se présenter comme suit :



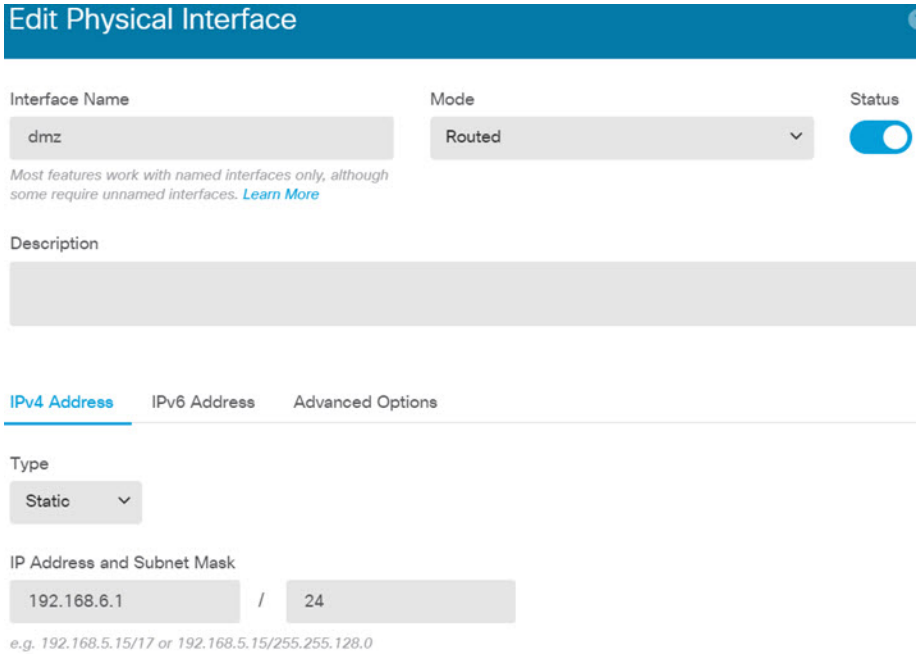
Étape 2 Si vous avez câblé d'autres interfaces, choisissez **Device (périphérique)**, puis cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur le type d'interface pour afficher la liste des interfaces.

- Pour le Firepower 4100/9300, aucune interface de données n'est préconfigurée avec des noms, des adresses IP ou des zones de sécurité, vous devez donc activer et configurer les interfaces que vous souhaitez utiliser.
- Comme l'l'ISA 3000 sont préconfigurés avec un groupe de ponts contenant toutes les interfaces de données , il n'est pas nécessaire de configurer ces interfaces. Cependant, vous devez configurer manuellement une adresse IP pour le BVI. Si vous souhaitez dissocier le groupe de ponts, vous pouvez le modifier pour supprimer les interfaces que vous souhaitez traiter séparément. Vous pouvez ensuite configurer ces interfaces comme hôtes de réseaux distincts.

  Pour les autres modèles, vous pouvez créer un groupe de ponts pour les autres interfaces, ou configurer des réseaux distincts, ou une combinaison des deux.
- Pour le Firepower 1010, toutes les interfaces, à l'exception d'Ethernet1/1 (externe), sont des ports de commutation en mode d'accès affectés à VLAN1 (interne). Vous pouvez modifier les ports de commutation en ports de pare-feu; ajouter de nouvelles interfaces VLAN et y affecter des ports de commutation; ou configurer les ports de commutation en mode de ligne principale.

Cliquez sur l'icône de modification ( ) pour chaque interface afin de définir le mode, l'adresse IP et d'autres paramètres.

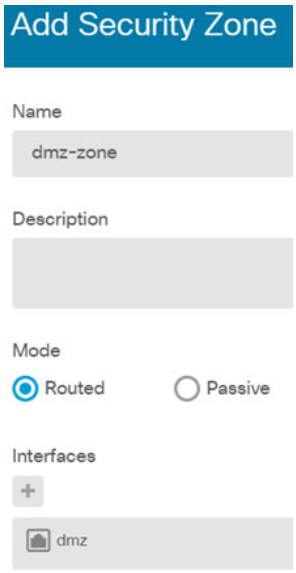
Dans l'exemple suivant, une interface est configurée pour être utilisée comme « zone démilitarisée » (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web. Lorsque vous avez terminé, cliquez sur **Save** (enregistrer).



Étape 3 Si vous avez configuré de nouvelles interfaces, sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

Modifiez ou créez de nouvelles zones, selon le cas. Chaque interface doit appartenir à une zone, car vous configurez les politiques en fonction des zones de sécurité et non des interfaces. Vous ne pouvez pas placer les interfaces dans des zones lors de leur configuration. Par conséquent, vous devez toujours modifier les objets des zones après avoir créé de nouvelles interfaces ou modifié le but des interfaces existantes.

L'exemple suivant montre comment créer une nouvelle zone dmz pour l'interface dmz.

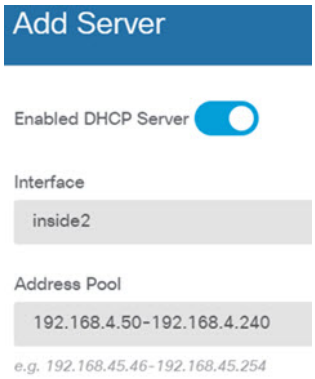


Étape 4 Si vous souhaitez que les clients internes utilisent le protocole DHCP pour obtenir une adresse IP du périphérique, sélectionnez **Device (périphérique)**, puis **System Settings (Paramètres système)** > **DHCP Server (Serveur DHCP)**. Sélectionnez l'onglet **DHCP Server** (Serveur DHCP).

Un serveur DHCP est déjà configuré pour l'interface interne, mais vous pouvez modifier l'ensemble des adresses ou même le supprimer. Si vous avez configuré d'autres interfaces internes, il est très courant de configurer un serveur DHCP pour ces interfaces. Cliquez sur **+** pour configurer le serveur et l'ensemble d'adresses pour chaque interface interne.

Vous pouvez également affiner la liste WINS et DNS fournie aux clients dans l'onglet **Configuration**.

L'exemple suivant montre comment configurer un serveur DHCP sur l'interface interne 2 avec l'ensemble d'adresses 192.168.4.50-192.168.4.240.



Étape 5 Choisissez **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Routing** (Routage) et configurez une route par défaut.

La voie de routage par défaut s'oriente normalement vers le routeur ISP (ou en amont) qui se trouve à côté de l'interface externe. Une voie de routage IPv4 par défaut est configuré sur any-ipv4 (0.0.0.0/0), alors qu'un routage IPv6 par défaut est configuré sur any-ipv6 (:: 0/0). Créez le routage pour chaque version IP que vous utilisez. Si vous utilisez le protocole DHCP pour obtenir une adresse pour l'interface externe, vous avez peut-être déjà accès au routage par défaut dont vous avez besoin.

Les voies de routage que vous définissez sur cette page concernent uniquement les interfaces de données. Elles n'ont aucun impact sur l'interface de gestion. Définissez la passerelle de gestion sous **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)**.

L'exemple suivant montre une voie de routage par défaut pour IPv4. Dans cet exemple, la passerelle isp-gateway est un objet réseau qui identifie l'adresse IP de la passerelle du fournisseur de services Internet (vous devez obtenir l'adresse de votre fournisseur de services Internet). Vous pouvez créer cet objet en cliquant sur **Create New Network** (créer un nouveau réseau) au bas du menu déroulant **Gateway** (passerelle).

Étape 6 Sélectionnez les politiques sous **Policies** et configurez les politiques de sécurité pour le réseau.

L'assistant de configuration de périphérique active le flux du trafic entre la zone interne et la zone externe ainsi que la NAT d'interface pour toutes les interfaces vers l'interface externe. Même si vous configurez de nouvelles interfaces, si vous les ajoutez à l'objet dans la zone interne, la règle de contrôle d'accès s'applique automatiquement à celles-ci.

Cependant, si vous avez plusieurs interfaces internes, vous avez besoin d'une règle de contrôle d'accès pour permettre la circulation du trafic d'une zone interne à une autre. Si vous ajoutez d'autres zones de sécurité, vous avez besoin de règles pour autoriser le trafic en provenance et à destination de ces zones. Il s'agit de vos modifications minimales.

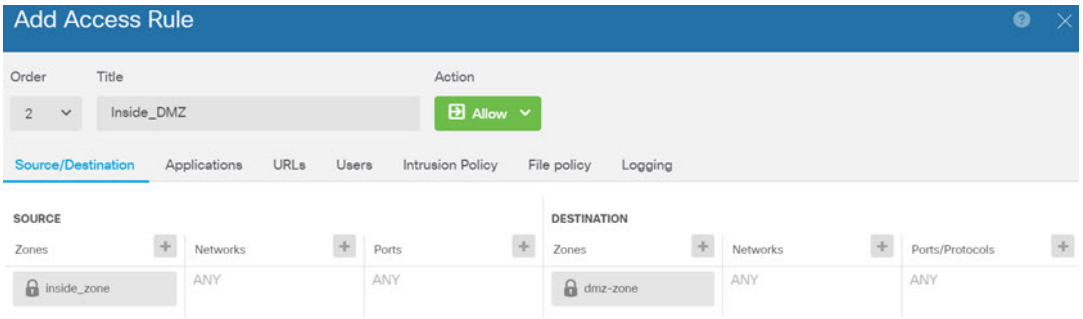
En outre, vous pouvez configurer d'autres politiques pour fournir des services supplémentaires et affiner la NAT et les règles d'accès afin d'obtenir les résultats requis par votre organisation. Vous pouvez configurer les politiques suivantes :

- **Déchiffrement SSL** : Si vous souhaitez inspecter les connexions chiffrées (comme HTTPS) pour détecter les intrusions, les logiciels malveillants, etc., vous devez déchiffrer les connexions. Utilisez la politique de déchiffrement SSL pour déterminer les connexions qui doivent être déchiffrées. Le système rechiffre la connexion après l'avoir inspectée.
- **Identité** : Si vous souhaitez corréler l'activité du réseau à des utilisateurs individuels ou contrôler l'accès au réseau en fonction de l'utilisateur ou de l'appartenance à un groupe d'utilisateurs, utilisez la politique d'identité pour déterminer l'utilisateur associé à une adresse IP source donnée.
- **Security Intelligence** (Renseignements de sécurité) : utilisez la politique sur les renseignements de sécurité pour supprimer rapidement les connexions en provenance des adresses IP ou des URL de la liste

de blocage ou vers celles-ci. En inscrivant sur la liste de blocage les mauvais sites connus, vous n'avez pas besoin de les prendre en compte dans votre stratégie de contrôle d'accès. Cisco fournit des flux régulièrement mis à jour d'adresses et d'adresses URL incorrectes afin que la liste de blocage issue des renseignements de sécurité se mette à jour de façon dynamique. En utilisant les flux, vous n'avez pas besoin de modifier la politique pour ajouter ou supprimer des éléments dans la liste de blocage.

- **NAT** (Network Address Translation, traduction d'adresses réseau) : utilisez la politique NAT pour convertir les adresses IP internes en adresses de routage externe.
- **Contrôle d'accès** : Utilisez la politique de contrôle d'accès pour déterminer les connexions autorisées sur le réseau. Vous pouvez procéder au filtrage selon la zone de sécurité, l'adresse IP, le protocole, le port, l'application, l'adresse URL, l'utilisateur ou le groupe d'utilisateurs. Vous pouvez aussi appliquer également des politiques en lien avec la prévention des intrusions et avec la présence de fichiers (logiciels malveillants) en utilisant des règles de contrôle d'accès. Utilisez cette politique pour mettre en œuvre le filtrage d'URL.
- **Intrusion** : Utilisez les politiques de prévention des intrusions pour rechercher les menaces connues. Bien que vous appliquiez des politiques de prévention des intrusions à l'aide de règles de contrôle d'accès, vous pouvez modifier lesdites politiques pour activer ou désactiver sélectivement des règles de prévention précises en lien avec les intrusions.

L'exemple suivant montre comment autoriser le trafic entre la zone interne et la zone dmz dans la politique de contrôle d'accès. Dans cet exemple, aucune option n'est définie sous les autres onglets, à l'exception de la journalisation (**Logging**), pour laquelle l'option **At End of Connection** (à la fin de la connexion) est sélectionnée.



Étape 7 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.

Comment mieux comprendre le trafic de votre réseau

Après avoir terminé la configuration initiale de l'appareil, vous disposerez d'une politique de contrôle d'accès qui permet à l'ensemble du trafic interne d'accéder à Internet ou à un autre réseau en amont, et d'une action par défaut pour bloquer tout autre trafic. Avant de créer des règles de contrôle d'accès supplémentaires, il peut être utile d'avoir accès à un aperçu du trafic qui se produit réellement sur votre réseau.

Vous pouvez utiliser les fonctionnalités de surveillance de FDM pour analyser le trafic réseau. La création de rapports FDM vous aide à répondre aux questions suivantes :

- À quoi sert mon réseau?
- Qui utilise le réseau le plus?
- Où vont mes utilisateurs?
- Quels appareils utilisent-ils?
- Quelles règles de contrôle d'accès (politiques) sont les plus touchées?

La règle d'accès initial peut donner un aperçu du trafic, y compris les politiques, les destinations et les zones de sécurité. Toutefois, pour obtenir des informations utilisateur, vous devez configurer une politique d'identité prévoyant une procédure d'authentification qui exige que les utilisateurs s'identifient eux-mêmes. Pour obtenir des informations sur les applications utilisées sur le réseau, vous devez effectuer quelques modifications supplémentaires.

La procédure suivante explique comment configurer l'appareil Cisco Firepower Threat Defense pour surveiller le trafic et donne un aperçu du processus de bout en bout de configuration et de surveillance des politiques.

Remarque Cette procédure ne donne pas un aperçu des catégories de sites Web et de la réputation des sites visités par les utilisateurs. Vous ne pouvez donc pas voir d'informations importantes dans le tableau de bord des catégories Web. Vous devez mettre en œuvre le filtrage d'URL par catégorie et activer la licence d'URL pour obtenir des données de catégorie et de réputation. Si vous souhaitez simplement obtenir ces informations, vous pouvez ajouter une nouvelle règle de contrôle d'accès qui autorise l'accès à une catégorie acceptable, comme Finance (finances) et en faire la première règle de la politique de contrôle d'accès. Pour en savoir plus sur la mise en œuvre du filtrage d'URL, consultez Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 23.

Procédure

Étape 1 Pour mieux comprendre le comportement des utilisateurs, vous devez configurer une politique d'identité pour vous assurer que l'utilisateur associé à une connexion est identifié.

En activant la politique d'identité, vous pouvez recueillir des informations au sujet des utilisateurs du réseau et des ressources qu'ils utilisent. Ces informations sont disponibles dans le tableau de bord de contrôle des utilisateurs. Les informations sur l'utilisateur sont également disponibles pour les événements de connexion affichés dans le visualiseur d'événements.

Dans cet exemple, nous mettrons en œuvre l'authentification active pour obtenir de l'information sur l'identité de l'utilisateur. Grâce à une authentification active, l'appareil demande à l'utilisateur de fournir son nom d'utilisateur et son mot de passe. Les utilisateurs ne sont authentifiés que lorsqu'ils utilisent un navigateur Web pour les connexions HTTP.

Si un utilisateur ne parvient pas à s'authentifier, il peut néanmoins se connecter au Web. Toutefois, vous n'aurez pas accès à de l'information sur l'identité de l'utilisateur pour les connexions. Si vous le souhaitez, vous pouvez créer une règle de contrôle d'accès pour supprimer le trafic des utilisateurs ayant échoué à l'authentification.

a) Cliquez sur **Policies** (politiques) dans le menu principal, puis cliquez sur **Identity** (identité).

   La politique d'identité est initialement désactivée. Lorsque vous faites appel à l'authentification active, la politique d'identité utilise votre serveur Active Directory pour authentifier les utilisateurs et les associer à l'adresse IP du poste de travail qu'ils utilisent. Par la suite, le système identifiera le trafic pour cette adresse IP comme étant le trafic de l'utilisateur.

b) Cliquez sur **Enable Identity Policy** (activer la politique d'identité).

c) Cliquez sur le bouton **Create Identity Rule** (créer une règle d'identité) ou sur le bouton **+** pour créer la règle nécessitant une authentification active.

   Dans cet exemple, nous supposerons que vous souhaitez exiger l'authentification pour tout le monde.

d) Entrez un nom (**Name**) pour la règle, qui peut être tout ce que vous choisissez, par exemple, Require_Authentication.

e) Sous l'onglet **Source/Destination**, laissez les valeurs par défaut, qui s'appliquent à tout critère (Any).

   Vous pouvez appliquer à la politique les limites de votre choix pour établir un ensemble de trafic plus limité. Cependant, l'authentification active ne sera tentée que pour le trafic HTTP, donc c'est sans importance que le trafic non-HTTP corresponde (ou non) aux critères en lien avec la source/destination. Pour en savoir plus sur les propriétés de la politique d'identité, consultez Configurer les règles d'identité.

f) Sous **Action**, sélectionnez **Active Auth**.

   En supposant que vous n'ayez pas configuré les paramètres de politique d'identité, la boîte de dialogue Identity Policy Configuration (configuration de politique d'identité) s'ouvrira car il y a des paramètres non définis.

g) Configurez le portail captif et les paramètres de déchiffrement SSL requis pour l'authentification active.

   Lorsqu'une règle d'identité requiert une authentification active pour un utilisateur, l'utilisateur est redirigé vers le port portail captif, puis il est invité à s'authentifier. Le portail captif requiert des règles de déchiffrement SSL, que le système générera automatiquement, mais vous devez sélectionner le certificat à utiliser pour les règles de déchiffrement SSL.

   - **Server Certificate** (certificat de serveur) : Sélectionnez le certificat interne à présenter aux utilisateurs lors de l'authentification active. Vous pouvez sélectionner le certificat DefaultInternalCertificate autosigné prédéfini ou cliquer sur **Create New Internal Certificate** (créer un nouveau certificat interne) et télécharger un certificat déjà réputé fiable pour vos navigateurs.

     Les utilisateurs devront accepter le certificat si vous ne téléchargez pas un certificat déjà réputé fiable pour leurs navigateurs.

   - **Redirect to Host Name** (rediriger vers le nom d'hôte) : Sélectionnez l'objet réseau qui définit le nom d'hôte qualifié complet de l'interface à utiliser comme portail captif pour les demandes

d'authentification active. Cliquez sur **Create New Network** (créer un nouveau réseau) si l'objet n'existe pas.

Le nom de domaine complet doit mener à l'adresse IP de l'une des interfaces du périphérique. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP. Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat.

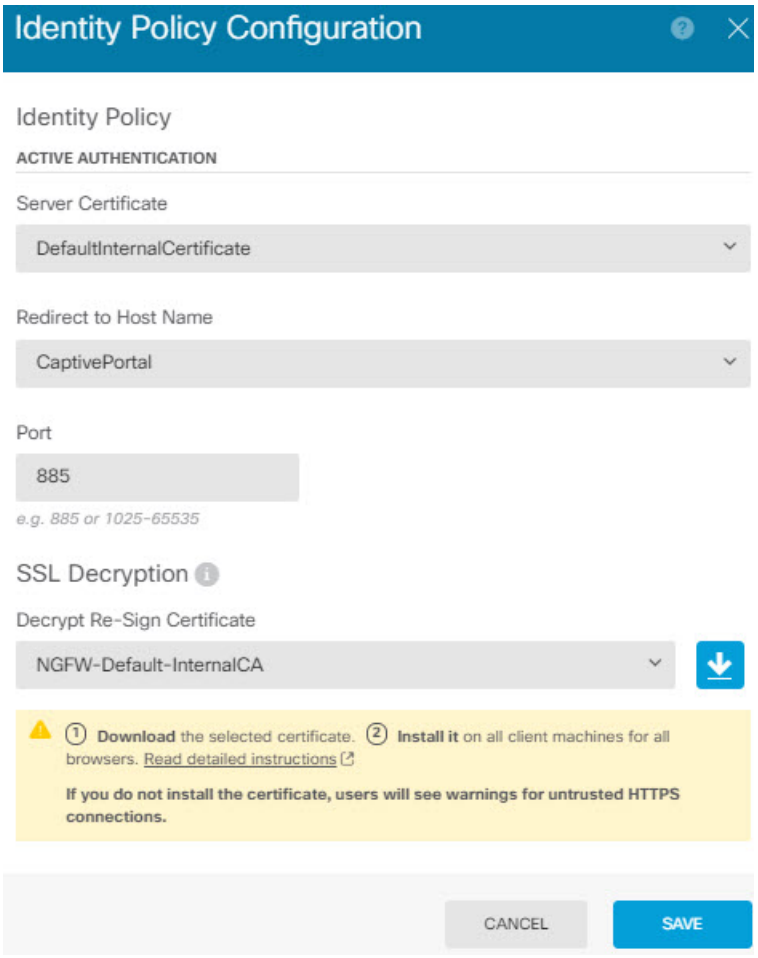
Si une règle d'identité requiert une authentification active pour un utilisateur, mais que vous ne précisez pas de nom de domaine complet de redirection, l'utilisateur sera redirigé vers le port du portail captif de l'interface de connexion.

- **Port** : le port du portail captif. La valeur par défaut est 885 (TCP). Si vous configurez un autre port, il doit être compris entre 1025 et 65535.
- **Decrypt Re-Sign Certificate** (déchiffrer le certificat resigné) : Sélectionnez le certificat d'autorité de certification interne à utiliser pour les règles qui mettent en application le déchiffrement avec les certificats resignés. Vous pouvez utiliser le certificat NGFW-Default-InternalCA prédéfini (par défaut) ou celui que vous avez créé ou téléchargé. Si le certificat n'existe pas encore, cliquez sur **Create Internal CA** (créer une autorité de certification interne) pour le créer. (Vous êtes invité à déchiffrer le certificat de re-signature seulement si vous n'avez pas encore activé la politique de déchiffrement SSL.)

  Si vous n'avez pas encore installé le certificat dans les navigateurs clients, cliquez sur le bouton de téléchargement () pour en obtenir une copie. Consultez la documentation de chaque navigateur afin de savoir comment installer le certificat. Voir aussi Téléchargement du certificat d'autorité de certification pour déchiffrer les règles de nouvelle signature.

Exemple :

La boîte de dialogue Identity Policy Configuration (configuration de la politique d'identité) devrait maintenant ressembler à ce qui suit.



h) Cliquez sur **Save** pour enregistrer les paramètres d'authentification active.

L'onglet Active Authentication (authentification active) apparaît maintenant sous le paramètre Action.

i) Sous l'onglet **Authentification active** (authentification active), sélectionnez **HTTP Negotiate**.

Cela permet au navigateur et au serveur d'annuaire de négocier le protocole d'authentification le plus puissant, dans l'ordre, NTLM, puis HTTP de base.

Remarque
Si vous ne pouvez pas fournir un nom de domaine complet **Redirect to Host Name** (Redirection vers le nom d'hôte), les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM redirigent l'utilisateur vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.AD-domain-name*. Si vous souhaitez utiliser la négociation HTTP sans nom de domaine complet de redirection vers l'hôte (**Redirect to Host Name**), vous devez également mettre à jour votre serveur DNS pour mapper ce nom avec les adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier. Nous vous recommandons de toujours fournir un nom de domaine complet de redirection vers le nom d'hôte (**Redirect to Host Name**) pour assurer un comportement cohérent, quelle que soit la méthode d'authentification. Si vous ne pouvez pas ou ne voulez pas mettre à jour le serveur DNS, sélectionnez l'une des autres méthodes d'authentification.

j) En ce qui concerne la source d'identité AD (**AD Identity Source**), cliquez sur **Create New Identity Realm** (créer un domaine d'identité).

Si vous avez déjà créé votre objet serveur de domaine, sélectionnez-le et ignorez les étapes de configuration du serveur.

Remplissez les champs suivants, puis cliquez sur **OK**.

- **Name** (nom) : Nom du domaine de répertoire.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

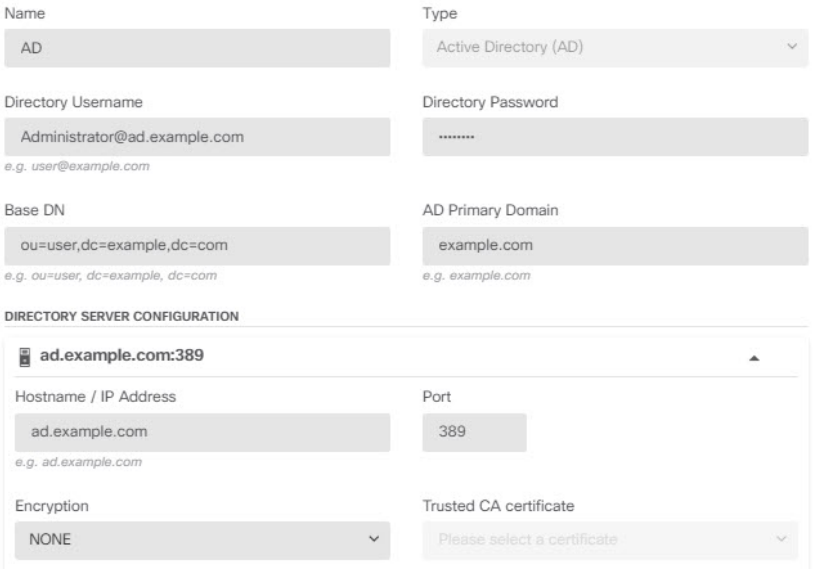
  Remarque
  Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=adminisntrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.
- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP.
- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement.
- **Encryption** (chiffrement) : Pour utiliser une connexion chiffrée pour le téléchargement des informations sur les utilisateurs et les groupes, sélectionnez la méthode souhaitée, **STARTTLS** ou **LDAPS**. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair.
  - **STARTTLS** négocie la méthode de chiffrement et utilise la méthode la plus efficace prise en charge par le serveur d'annuaire. Utilisez le port 389. Cette option n'est pas prise en charge si vous utilisez le domaine pour le VPN d'accès à distance.
  - **LDAPS** nécessite LDAP sur SSL. Utilisez le port 636.
- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP

du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

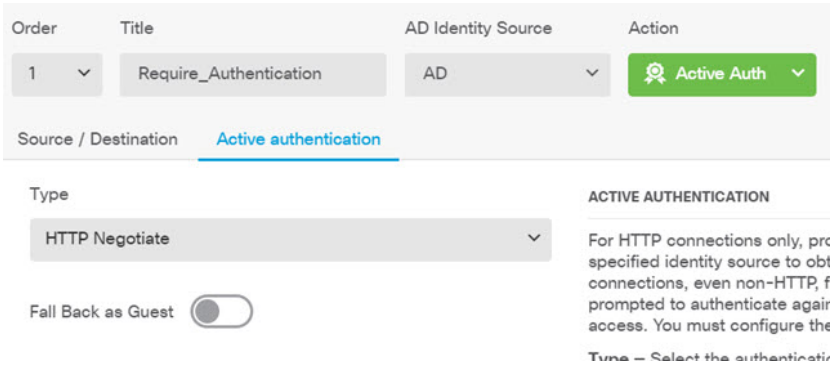
Exemple :

Par exemple, l'image suivante montre comment créer une connexion non chiffrée pour le serveur ad.exemple.com. Le domaine principal est exemple.com et le nom d'utilisateur du répertoire est Administrateur@ad.exemple.com. Toutes les informations relatives aux utilisateurs et aux groupes se trouvent sous le nom distinctif (DN) ou=user,dc=example,dc=com.



k) Pour la **source d'identité AD**, sélectionnez l'objet que vous venez de créer.

La règle devrait ressembler à ce qui suit.



l) Cliquez sur **OK** pour ajouter la règle.

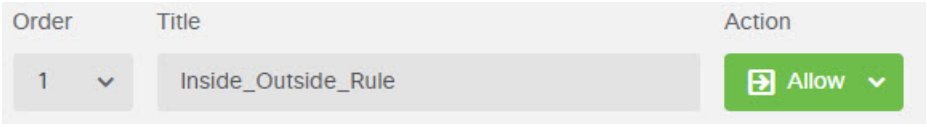
Si vous regardez dans le coin supérieur droit de la fenêtre, vous pouvez voir que le bouton d'icône **Deploy** (déployer) a maintenant un point, ce qui indique qu'il y a des changements non déployés. Apporter des modifications à l'interface utilisateur n'est pas suffisant pour configurer les modifications sur l'appareil. Vous devez déployer les modifications. Ainsi, vous pouvez apporter un ensemble de modifications connexes avant de les déployer, afin d'éviter les problèmes susceptibles de découler de l'exécution sur le périphérique d'un ensemble de modifications partiellement configuré. Vous déploierez les modifications plus tard dans cette procédure.

Étape 2 Modifiez l'action de la règle de contrôle d'accès Inside_Outside_Rule afin de l'autoriser (**Allow**).

La règle d'accès Inside_Outside_Rule est créée en tant que règle de confiance. Cependant, le trafic considéré comme digne de confiance n'est pas inspecté, de sorte que le système ne peut pas connaître certaines de ses caractéristiques, comme l'application, lorsque les critères de correspondance du trafic n'incluent pas l'application ou d'autres conditions que la zone, l'adresse IP et le port. Si vous modifiez la règle pour autoriser le trafic plutôt que de lui accorder votre confiance, le système inspectera entièrement le trafic.

Remarque
(ISA 3000.) Vous pouvez également envisager de modifier les paramètres de Outside_Inside_Rule, Inside_Inside_Rule et Outside_Outside_Rule de « Trust » (faire confiance) à « Allow » (autoriser).

a) Cliquez sur **Access Control** (contrôle d'accès) dans la page des politiques (**Policies**).
b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.
c) Sélectionnez **Allow** (autoriser) sous **Action**.

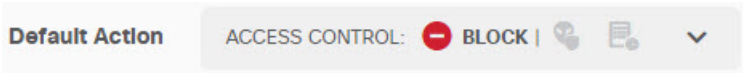


d) Cliquez sur **OK** pour enregistrer la modification

Étape 3 Activez la journalisation de l'action par défaut de la politique de contrôle d'accès.

Les tableaux de bord contiennent des informations sur les connexions uniquement dans les cas où la connexion correspond à une règle de contrôle d'accès qui permet la journalisation des connexions. La règle Inside_Outside_Rule permet la journalisation, mais l'action par défaut désactive la journalisation. Ainsi, les tableaux de bord affichent uniquement des informations sur la règle Inside_Outside_Rule et ne reflètent pas les connexions qui ne correspondent à aucune règle.

a) Cliquez n'importe où dans l'action par défaut au bas de la page de politique de contrôle d'accès.

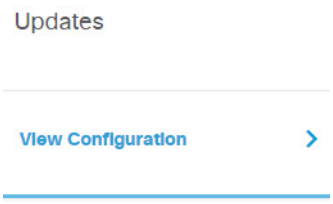


b) Sélectionnez la journalisation au début et à la fin de la connexion (**Select Log Action** > **At Beginning and End of Connection**).
c) Cliquez sur **OK**.

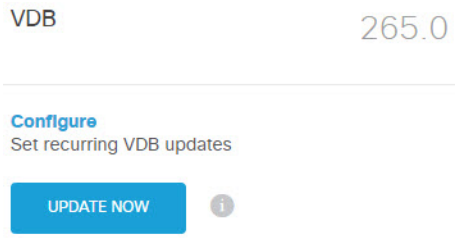
Étape 4 Définissez un calendrier de mises à jour pour la base de données sur les vulnérabilités (VDB).

Cisco diffuse régulièrement des mises à jour de la VDB, qui comprend les détecteurs d'applications pouvant reconnaître l'application utilisée dans une connexion. Vous devez mettre à jour la VDB régulièrement. Vous pouvez soit télécharger manuellement les mises à jour, soit configurer un calendrier de mises à jour régulières. La procédure suivante montre comment configurer un calendrier. Par défaut, les mises à jour de la base de données sur les vulnérabilités sont désactivées. Vous devez donc les activer pour mettre à jour la VDB.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe Updates (mises à jour).



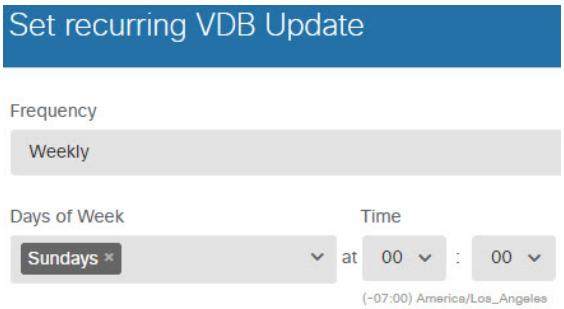
c) Cliquez sur **Configure** (configurer) dans le groupe VDB.



d) Définir le calendrier de mises à jour.

Choisissez une heure et une fréquence qui ne perturberont pas votre réseau. Il faut comprendre que le système effectuera un déploiement automatique après le téléchargement de la mise à jour. C'est nécessaire pour activer les nouveaux détecteurs. Ainsi, toutes les modifications de configuration que vous avez apportées et enregistrées, mais que vous n'avez pas encore déployées, seront également déployées.

Par exemple, voici l'horaire de la mise à jour de la VDB une fois par semaine, le dimanche, à minuit.



e) 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.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les utilisateurs et les applications. Vous pouvez évaluer ces informations pour rechercher des tendances indésirables et élaborer de nouvelles règles d'accès pour limiter les utilisations inacceptables.

Si vous souhaitez commencer à recueillir des informations sur les intrusions et les logiciels malveillants, vous devez activer les politiques de prévention des intrusions et des politiques de fichiers sur l'une ou plusieurs des règles d'accès. Vous devez également activer les licences pour ces fonctionnalités.

Si vous souhaitez commencer à recueillir des informations sur les catégories d'URL, vous devez mettre en œuvre le filtrage d'URL.

Comment bloquer les menaces

Vous pouvez mettre en œuvre le filtrage IPS (Intrusion Prevention System) de nouvelle génération en ajoutant des politiques de prévention des intrusions à vos règles de contrôle d'accès. Les politiques de prévention des intrusions analysent le trafic réseau et comparent le contenu du trafic aux menaces connues. Si une connexion correspond à une menace que vous surveillez, le système la coupe, empêchant ainsi l'attaque.

Tous les autres traitements de trafic ont lieu avant que le trafic réseau ne fasse l'objet d'un examen pour détecter les intrusions. En associant une politique de prévention des intrusions à une règle de contrôle d'accès, vous informez le système qu'avant que soit transmis le trafic correspondant aux conditions de la règle de contrôle d'accès, vous souhaitez inspecter le trafic au moyen d'une politique de prévention des intrusions.

Vous pouvez configurer des politiques de prévention des intrusions uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**). En outre, vous pouvez configurer une politique de prévention des intrusions dans le cadre de l'action par défaut si l'action par défaut est **allow** (autoriser).

Les politiques d'intrusion sont conçues par le Cisco Talos Intelligence Group (Talos), qui définit les états des règles d'intrusion et de préprocesseur et les paramètres avancés. Vous pouvez créer vos propres politiques personnalisées en fonction des politiques Talos si vous utilisez Snort 3 comme moteur d'inspection.

En plus d'inspecter le trafic que vous autorisez afin de détecter d'éventuelles intrusions, vous pouvez utiliser la politique de renseignement de sécurité pour bloquer de manière préventive tout le trafic en provenance ou à destination d'adresses IP ou d'adresses URL connues comme mauvaises.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez la licence Menace .

Vous devez activer la licence Menace pour utiliser les politiques de prévention des intrusions et les renseignements sur la sécurité. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation de la licence. Si vous avez enregistré l'appareil, vous devez acheter la licence requise et l'ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.

c) Cliquez sur **Enable** (activer) dans le groupe **Menace** .

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).

Étape 2 Sélectionnez une politique de prévention des intrusions pour l'une ou plusieurs des règles d'accès.

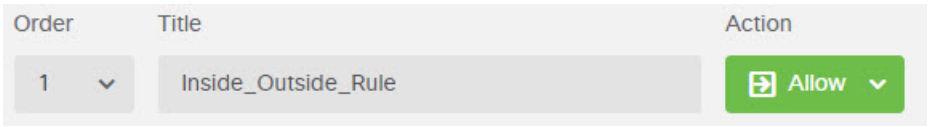
Déterminez les règles qui couvrent le trafic qui doit faire l'objet de l'analyse pour la recherche de menaces. Pour cet exemple, nous allons ajouter l'inspection en lien avec la prévention des intrusions à la règle Inside_Outside_Rule.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.

c) Si vous ne l'avez pas encore fait, sélectionnez **Allow**(autoriser) pour l'action (**Action**).

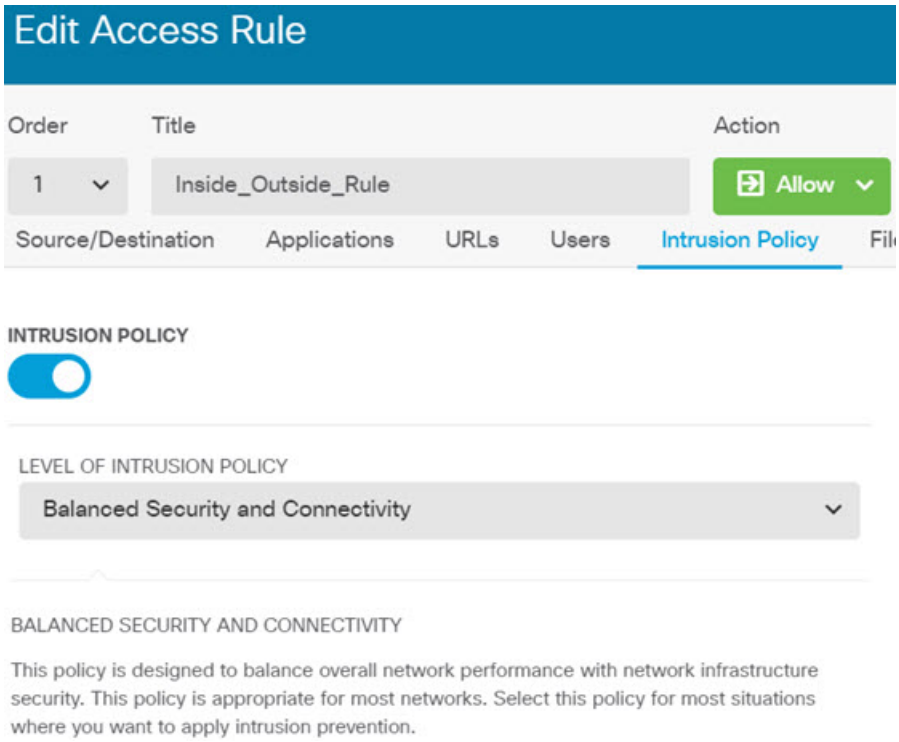


d) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions).

e) Cliquez sur le bouton **Intrusion Policy** (politique de prévention des intrusions) pour l'activer, puis sélectionnez la politique.

La politique **Balanced Security and Connectivity**(sécurité et connectivité équilibrées) convient à la plupart des réseaux. Elle offre une bonne protection contre les intrusions sans être trop agressive, ce qui peut entraîner l'abandon d'un trafic que vous pourriez ne pas vouloir supprimer. Si vous déterminez que vous perdez trop de trafic, vous pouvez simplifier l'inspection en lien avec la prévention des intrusions en sélectionnant la politique **Connectivity over Security** (connectivité avant sécurité).

Si vous avez besoin de plus d'agressivité en matière de sécurité, essayez la politique **Security over Connectivity** (sécurité avant connectivité). La politique de détection maximale (**Maximum Detection**) accorde encore plus d'importance à la sécurité de l'infrastructure réseau, ce qui peut avoir un impact opérationnel encore plus important.



f) Cliquez sur **OK** pour enregistrer la modification

Étape 3 (Facultatif) Rendez-vous sur **Policies (politiques)** > **Intrusion**, cliquez sur l'icône en forme de roue et configurez un serveur syslog pour la politique de prévention des intrusions.

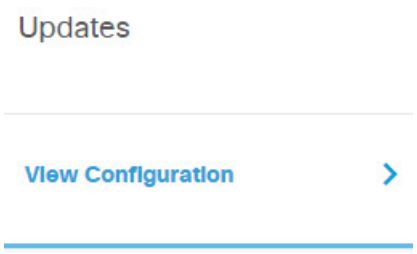
Les incidents d'intrusion n'utilisent pas le serveur syslog configuré pour la règle de contrôle d'accès.

Étape 4 Définir un calendrier de mise à jour pour la base de données des règles de prévention des intrusions.

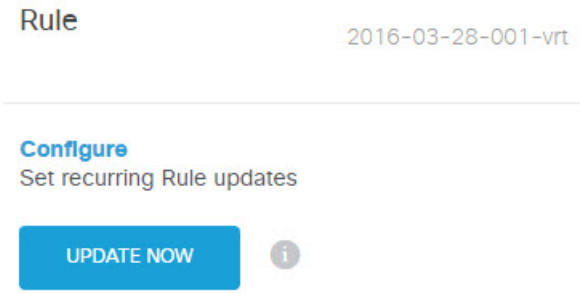
Cisco publie régulièrement des mises à jour de la base de données des règles de prévention des intrusions, qui est utilisée par les politiques d'intrusion pour déterminer si les connexions doivent être abandonnées. Vous devez mettre à jour la base de données des règles régulièrement. Vous pouvez soit télécharger manuellement les mises à jour, soit configurer un calendrier de mises à jour régulières. La procédure suivante montre comment configurer un calendrier. Par défaut, les mises à jour de la base de données sont désactivées. Vous devez donc prendre des mesures pour obtenir des règles mises à jour.

a) Cliquez sur **Device (périphérique)**.

b) Cliquez sur **View Configuration** dans le groupe Updates (mises à jour).



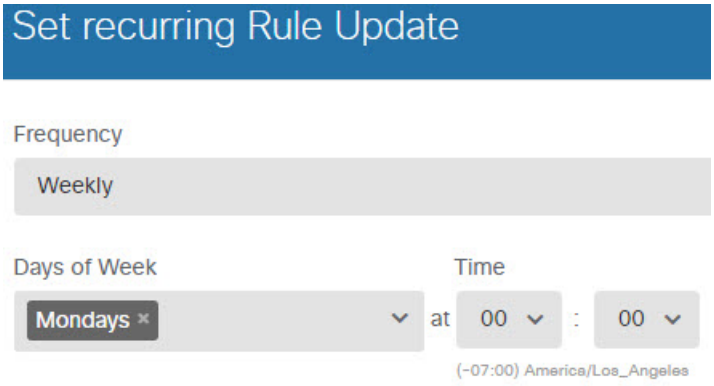
c) Cliquez sur **Configure** (configurer) dans le groupe des règles (Rule).



d) Définir le calendrier de mises à jour.

Choisissez une heure et une fréquence qui ne perturberont pas votre réseau. Il faut comprendre que le système effectuera un déploiement automatique après le téléchargement de la mise à jour. C'est nécessaire pour activer les nouvelles règles. Ainsi, toutes les modifications de configuration que vous avez apportées et enregistrées, mais que vous n'avez pas encore déployées, seront également déployées.

Par exemple, voici l'horaire de la mise à jour de la base de données sur les règles une fois par semaine, le lundi, à minuit.



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

Étape 5 Configurez la politique de renseignement de sécurité pour supprimer de manière préventive les connexions avec des sites et des hôtes connus comme mauvais.

En utilisant les renseignements de sécurité pour bloquer les connexions avec les hôtes ou les sites qui sont connus pour être des menaces, vous évitez à votre système le temps nécessaire pour effectuer une inspection approfondie des paquets afin de repérer les menaces dans chaque connexion. Les renseignements de sécurité permettent de bloquer rapidement le trafic indésirable, laissant plus de temps au système pour gérer le trafic important pour vous.

a) Cliquez sur **Device** (périphérique), puis sur **View Configuration** (afficher la configuration) dans le groupe **Updates** (mises à jour).
b) Cliquez sur **Update Now** (mettre à jour maintenant) dans le groupe Security Intelligence Feeds (flux de renseignements de sécurité).
c) Cliquez également sur **Configure** (configurer) et définissez une mise à jour périodique pour les flux. La valeur par défaut, **Hourly** (mise à jour toutes les heures), convient à la plupart des réseaux, mais vous pouvez réduire la fréquence si nécessaire.
d) Cliquez sur **Policies** (politiques), puis sur la politique **Security Intelligence** (renseignements de sécurité).
e) Cliquez sur **Enable Security Intelligence** si vous n'avez pas encore activé la politique.

f) Dans l'onglet **Network** (réseau), cliquez sur **+** dans la liste bloquer/abandonner (block/drop), puis sélectionnez tous les flux dans l'onglet **Network Feeds** (flux réseau). Vous pouvez cliquer sur le bouton **i** à côté d'un flux pour lire sa description.

Si vous voyez un message indiquant qu'il n'y a pas encore de flux, réessayez plus tard. Le téléchargement des flux n'est pas encore terminé. Si ce problème persiste, assurez-vous qu'il y a un chemin entre l'adresse IP de gestion et Internet.

g) Cliquez sur **OK** pour ajouter les flux sélectionnés.

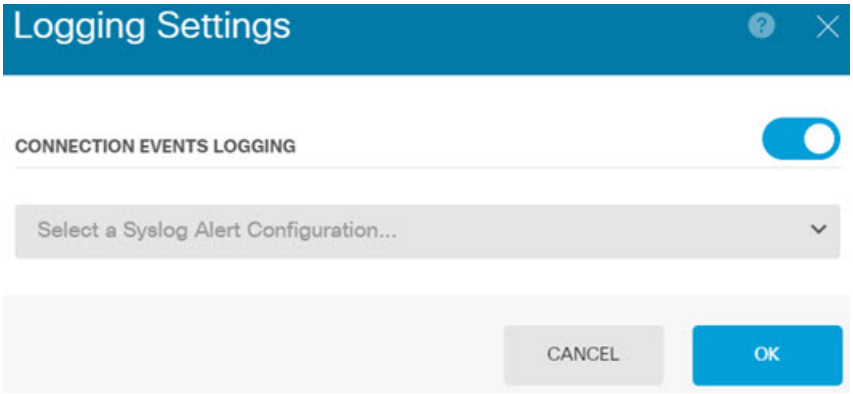
Si vous connaissez d'autres adresses IP incorrectes, vous pouvez cliquer sur **+** > **Network Objects** et ajouter les objets qui contiennent les adresses. Vous pouvez cliquer sur **Create New Network Object** (créer un nouvel objet réseau) au bas de la liste pour les ajouter immédiatement.

h) Cliquez sur l'onglet **URL**, puis sur **+** > **URL Feeds** dans la liste block/drop, enfin, sélectionnez tous les flux URL. Cliquez sur **OK** pour les ajouter à la liste.

Comme pour la liste de réseaux, vous pouvez ajouter vos propres objets URL à la liste pour bloquer d'autres sites qui ne sont pas dans les flux. Cliquez sur **+** > **URL Objects (objets URL)**. Vous pouvez ajouter de nouveaux objets en cliquant sur **Create New URL Object** (créer un nouvel objet URL) à la fin de la liste.

i) Cliquez sur l'icône en forme de roue et activez la journalisation des événements de connexion (**Connection Events Logging**) pour permettre à la politique de générer des événements de renseignements de sécurité pour les connexions correspondantes. Cliquez sur **OK** pour enregistrer les modifications.

Si vous n'activez pas la journalisation des connexions, vous n'aurez aucune donnée à utiliser pour déterminer si la politique répond aux attentes. Si un serveur syslog externe est défini, vous pouvez le sélectionner maintenant afin que les événements soient également envoyés à ce serveur.



j) Au besoin, vous pouvez ajouter des objets réseau ou URL à la liste **Do Not Block** (ne pas bloquer) dans chaque onglet pour créer des exceptions à la liste de contacts bloqués.

Les listes **Do Not Block** ne sont pas vraiment des listes encadrant les autorisations. Ce sont plutôt des listes d'exceptions. Si une adresse ou une URL dans la liste d'exceptions apparaît également dans la liste des contacts bloqués, la connexion pour l'adresse ou l'URL est transmise à la politique de contrôle d'accès. De cette façon, vous pouvez bloquer un flux, mais si vous constatez plus tard qu'une adresse ou un site souhaitable est bloqué, vous pouvez utiliser la liste des exceptions pour remplacer ce blocage sans devoir supprimer complètement le flux. Gardez à l'esprit que ces connexions sont ensuite évaluées par le contrôle d'accès et, si elles sont configurées, par des politiques de prévention des intrusions. Ainsi, si des connexions contiennent des menaces, elles peuvent être identifiées et bloquées lors d'une inspection de prévention des intrusions.

Consultez le tableau de bord de règles d'accès et de règles SI, ainsi que l'écran des renseignements sur la sécurité (Security Intelligence) dans le visualiseur d'événements, pour déterminer le trafic qui est réellement abandonné par la politique et établir si vous devez ajouter des adresses ou des URL aux listes **Do Not Block**.

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.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les auteurs des attaques, les cibles et les menaces, si des intrusions sont détectées. Vous pouvez évaluer ces informations pour déterminer si votre réseau a besoin de précautions de sécurité renforcées, ou si vous devez réduire le niveau des politiques de prévention des intrusions que vous utilisez.

Pour les renseignements de sécurité, vous pouvez voir les occurrences des politiques sur le tableau de bord des règles d'accès et de SI. Vous pouvez également voir les événements en lien avec les renseignement de sécurité dans le visualiseur d'événements. Les blocs fondés sur les renseignements de sécurité ne sont pas reflétés dans les renseignements sur les menaces d'intrusion, car le trafic est bloqué avant de pouvoir être inspecté.

Comment bloquer les logiciels malveillants

Les utilisateurs risquent continuellement d'obtenir des logiciels malveillants, ou *maliciels*, à partir de sites Internet ou d'autres méthodes de communication, comme le courrier électronique. Même des sites Web de confiance peuvent être piratés pour transmettre des logiciels malveillants à des utilisateurs peu méfiants. Les pages Web peuvent contenir des objets provenant de différentes sources. Ces objets peuvent inclure des images, des exécutables, du Javascript, des publicités, etc. Les sites Web compromis comprennent souvent des objets hébergés sur des sources externes. Une véritable solution de sécurité signifie regarder chaque objet individuellement, pas seulement la demande initiale.

Utilisez des politiques de fichiers pour détecter les programmes malveillants à l'aide du logiciel de défense contre les programmes malveillants. Vous pouvez également utiliser les politiques de fichiers pour effectuer le contrôle de fichier, ce qui permet de contrôler tous les fichiers d'un type spécifique, qu'ils contiennent ou non des logiciels malveillants.

Le logiciel de défense contre les programmes malveillants utilise Cisco AMP Cloud pour récupérer les dispositions relatives aux éventuels programmes malveillants détectés dans le trafic réseau. L'interface de gestion doit disposer d'un chemin vers Internet pour atteindre Cisco AMP Cloud et effectuer des recherches de programmes malveillants. Lorsque l'appareil détecte un fichier admissible, il utilise la valeur de hachage SHA-256 du fichier pour demander la Cisco AMP Cloud disposition du fichier. Voici les dispositions possibles

d'un fichier : inoffensif (**clean**), malveillant (**malware**) ou inconnu (**unknown**; aucun verdict clair). Si le Cisco AMP Cloud n'est pas accessible, la disposition est **inconnue**.

En associant une politique de fichiers à une règle de contrôle d'accès, vous informez le système qu'avant de transmettre le trafic correspondant aux conditions de la règle de contrôle d'accès, vous devez d'abord inspecter tous les fichiers de la connexion.

Vous pouvez configurer des politiques de fichiers uniquement sur des règles qui autorisent (**allow**) le trafic. Aucune inspection n'est effectuée sur les règles définies pour attribuer la confiance (**trust**) à un trafic ou le bloquer (**block**).

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez les licences Programme malveillant et Menace .

Vous devez activer la licence Programme malveillant pour utiliser les politiques de fichiers en plus de la licence Menace , qui est requise pour les politiques de détection des intrusions.. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation des licences. Si vous avez enregistré l'appareil, vous devez acheter les licences requises et les ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.

c) Cliquez sur **Enable** (activer) dans le groupe **Programme malveillant** et, si ce n'est déjà fait, dans le groupe **Menace** .

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).

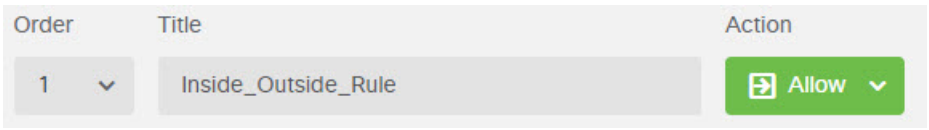
Étape 2 Sélectionnez une politique de fichiers pour l'une ou plusieurs des règles d'accès.

Déterminez les règles qui couvrent le trafic qui doit faire l'objet de l'analyse pour la recherche de logiciels malveillants. Pour cet exemple, nous allons ajouter l'inspection des fichiers à la règle Inside_Outside_Rule.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

b) Passez la souris sur la cellule **Actions** sur le côté droit de la rangée Inside_Outside_Rule pour exposer les icônes de modification et de suppression, puis cliquez sur l'icône de modification ( ) pour ouvrir la règle.
c) Si vous ne l'avez pas encore fait, sélectionnez **Allow**(autoriser) pour l'action (**Action**).

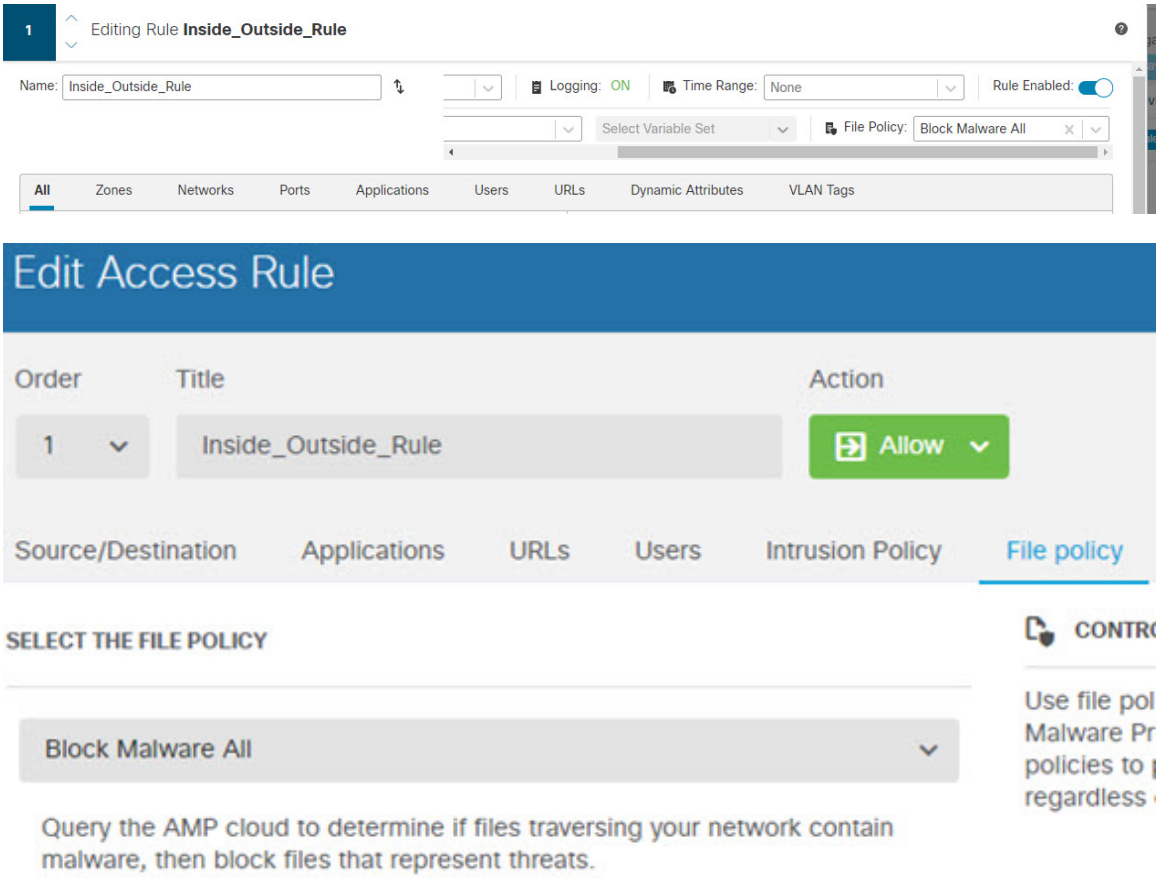


d) Cliquez sur l'onglet **File Policy** (politique de fichiers).
e) Cliquez sur la politique de fichiers que vous souhaitez utiliser.

Vous avez principalement le choix entre **bloquer tous les programmes malveillants**, qui supprime tous les fichiers considérés comme des programmes malveillants, et la fonction **tous les chercher sur le Cloud** , qui interroge le Cisco AMP Cloud pour déterminer la disposition du fichier, mais qui n'en bloque aucun. Si vous souhaitez d'abord voir comment les fichiers sont évalués, utilisez la recherche dans le nuage. Vous pourrez passer à la politique de blocage ultérieurement si vous êtes satisfait de l'évaluation des fichiers.

Il existe d'autres politiques qui bloquent les logiciels malveillants. Ces politiques sont associées au contrôle des fichiers, ce qui bloque le téléchargement de documents Microsoft Office, Office ou PDF. Autrement dit, ces politiques empêchent les utilisateurs d'envoyer ces types de fichiers à d'autres réseaux en plus de bloquer les logiciels malveillants. Vous pouvez sélectionner ces politiques si elles répondent à vos besoins.

Pour cet exemple, sélectionnez **Block Malware All**.



f) Cliquez sur l'onglet **Logging** (journalisation) et vérifiez que **Log Files** (fichiers journaux) est sélectionné sous File Events (événements de fichiers).

Par défaut, la journalisation des fichiers est activée lorsque vous sélectionnez une politique de fichiers. Vous devez activer la journalisation des fichiers pour obtenir des informations sur les fichiers et les logiciels malveillants dans les événements et les tableaux de bord.

g) Cliquez sur **OK** pour enregistrer la modification

Étape 3 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.

Prochaine étape

À ce stade, si des fichiers ou des logiciels malveillants sont transmis, les événements et les tableaux de bord de surveillance devraient commencer à afficher des informations sur les types de fichiers et les événements de fichiers et de logiciels malveillants. Vous pouvez évaluer ces informations pour déterminer si votre réseau a besoin de faire l'objet de plus de précautions de sécurité liées aux transmissions de fichiers.

Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL)

Vous pouvez avoir une politique d'utilisation acceptable pour votre réseau. Les politiques d'utilisation acceptable établissent une distinction entre l'activité réseau appropriée dans votre organisation et l'activité jugée inappropriée. Ces politiques sont généralement axées sur l'utilisation d'Internet et visent à maintenir la productivité, à éviter les responsabilités légales (par exemple, à maintenir un lieu de travail non hostile) et, en général, à contrôler le trafic Web.

Vous pouvez utiliser le filtrage d'URL pour définir une politique d'utilisation acceptable avec des politiques d'accès. Vous pouvez filtrer les grandes catégories, comme les jeux de hasard (Gambling), afin de ne pas avoir à identifier chaque site Web qui doit être bloqué. Pour les correspondances de catégorie, vous pouvez également spécifier la réputation relative des sites à autoriser ou à bloquer. Si un utilisateur tente de rechercher une URL avec cette catégorie et cette combinaison de réputation, la session est bloquée.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Cela assure que le système contrôlera le trafic Web comme prévu. Enfin, comme les renseignements sur les menaces de Cisco sont continuellement mis à jour à la lumière de nouvelles URL, ainsi que de nouvelles catégories et risques pour les URL existantes, vous pouvez vous assurer que le système utilise des informations à jour pour filtrer les URL demandées. Les sites malveillants qui représentent des menaces de sécurité, comme

les logiciels malveillants, les pourriels, les réseaux de zombies et l'hameçonnage peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques.

La procédure suivante explique comment mettre en œuvre une politique d'utilisation acceptable en utilisant le filtrage d'URL. Pour les besoins de cet exemple, nous bloquerons les sites de toute réputation dans plusieurs catégories, les sites de réseaux sociaux à risque et un site non classé, badsite.example.com.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, activez la licence **URL**.

Vous devez activer la licence URL pour utiliser la catégorie URL et les informations de réputation, ou pour voir les informations dans les tableaux de bord et les événements. Si vous utilisez actuellement la licence d'évaluation, vous activez une version d'évaluation de la licence. Si vous avez enregistré l'appareil, vous devez acheter la licence requise et l'ajouter à votre compte Smart Software Manager sur Cisco.com.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **View Configuration** dans le groupe des licences Smart.

c) Cliquez sur **Enable** (activer) dans le groupe **URL** (licence URL).

Le système enregistre la licence avec votre compte ou active la licence d'évaluation, selon le cas. Le groupe doit indiquer que la licence est activée, et le bouton indique Disable (désactivé).

Étape 2 Créez une règle de contrôle d'accès de filtrage d'URL.

Vous voudrez peut-être d'abord voir les catégories des sites visités par vos utilisateurs avant de définir une règle de blocage. Si tel est le cas, vous pouvez créer une règle avec l'action d'autorisation (Allow) pour une catégorie acceptable, comme la catégorie des services financiers (Finance). Étant donné que toutes les connexions Web doivent être inspectées pour déterminer si l'URL appartient à cette catégorie, vous obtiendrez des renseignements sur la catégorie même pour les sites des services non financiers (non-Finance).

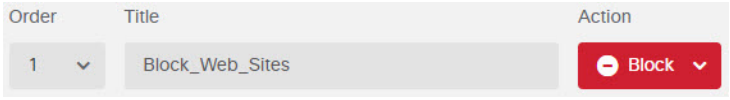
Mais il y a probablement des catégories d'URL dont vous savez déjà que vous souhaitez les bloquer. Une politique de blocage oblige également l'inspection, de sorte que vous obtenez des informations sur les catégories de connexions aux catégories non bloquées, et pas seulement au sujet des catégories bloquées.

a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

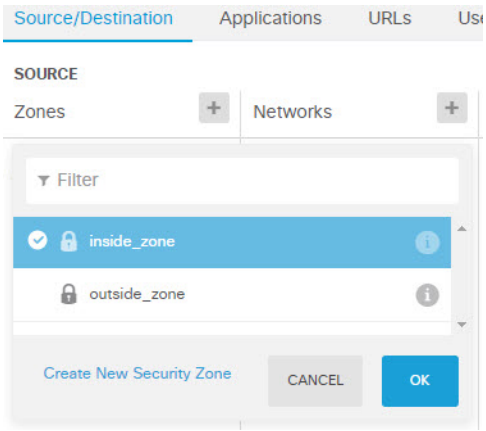
b) Cliquez sur + pour ajouter une nouvelle règle.
c) Configurez l'ordre, le titre et l'action.

- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons la même source/destination que la règle Inside_Outside_Rule créée lors de la configuration initiale de l'appareil. Vous avez peut-être également créé d'autres règles également. Pour maximiser l'efficacité du contrôle d'accès, il est préférable d'établir des règles précises dès le début, afin de déterminer rapidement si une connexion est autorisée ou interrompue. Dans cet exemple, sélectionnez **1** comme ordre des règles.
- **Title** (titre) : Donnez un nom significatif à la règle, par exemple Block_Web_Sites.
- **Action** : Sélectionnez **Block**.

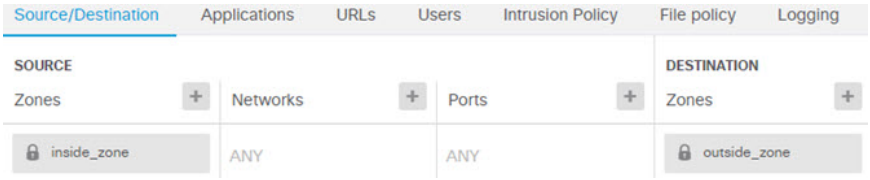


d) Dans l'onglet **Source/Destination**, cliquez sur **+** pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.

L'ajout de l'un des critères fonctionne de la même manière. Cliquez sur **+** pour ouvrir une petite boîte de dialogue où vous cliquez sur les éléments que vous souhaitez ajouter. Vous pouvez cliquer sur plusieurs éléments, puis cliquer sur un élément sélectionné le désélectionne; les cases à cocher indiquent les éléments sélectionnés. Mais rien n'est ajouté à la politique jusqu'à ce que vous cliquiez sur le bouton **OK**; la simple sélection des éléments ne suffit pas.



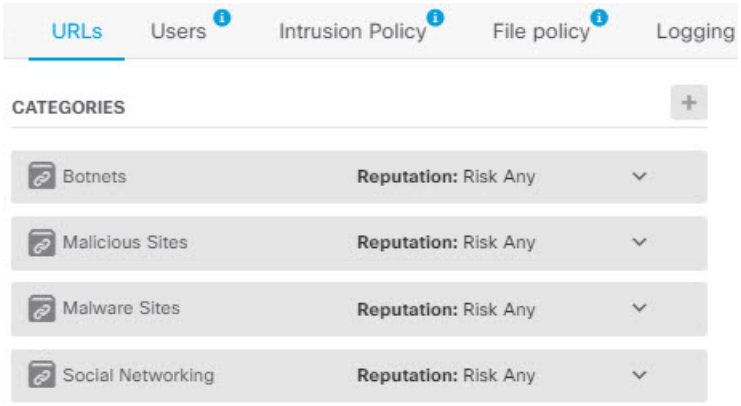
e) En utilisant la même technique, sélectionnez **outside_zone** pour les zones de destination (**Destination** > **Zones**).



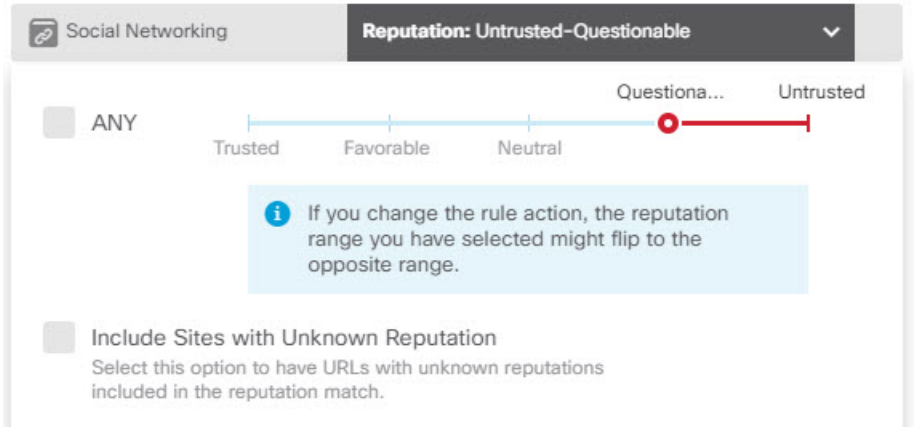
f) Cliquez sur l'onglet **URLs**.

g) Cliquez sur le signe + pour les catégories (**Categories**), puis sélectionnez les catégories que vous souhaitez bloquer complètement ou partiellement.

Pour les besoins de cet exemple, sélectionnez réseaux de zombies, sites malveillants, programmes malveillants et réseaux sociaux (Botnets, Malicious Sites, Malware Sites et Social Networking). Il y a d'autres catégories que vous voudrez probablement bloquer. Si vous connaissez un site que vous souhaitez bloquer, mais que vous n'êtes pas sûr de la catégorie, entrez l'URL dans le champ **URL to Check** (URL à vérifier) et cliquez sur **Go** pour lancer la vérification. Vous serez redirigé vers un site Web qui affiche les résultats de la recherche.



h) Pour mettre en œuvre le blocage sensible à la réputation de la catégorie des réseaux sociaux, cliquez sur **Reputation: Risk Any** dans cette catégorie, puis décocher **Any**, avant de sélectionner **Questionable**. Cliquez en dehors de la case du curseur pour le fermer.



À la gauche du curseur de réputation, vous trouverez de l'information sur les sites qui seront autorisés, tandis que les sites qui sont bloqués sont présentés du côté droit. Dans ce cas, seuls les sites de réseaux sociaux ayant une réputation considérée comme douteuse (Questionable) et non fiable (Untrusted) seront bloqués. Ainsi, vos utilisateurs devraient pouvoir accéder aux sites de réseaux sociaux les plus utilisés, où les risques sont moindres.

Sélectionnez l'option **Include Sites with Unknown Reputation** (inclure les sites avec une réputation inconnue) pour inclure les URL de réputation inconnue dans la correspondance de réputation. Les nouveaux sites ne sont généralement pas classés, et il peut y avoir d'autres raisons pour lesquelles la réputation d'un site est inconnue ou ne peut être déterminée.

Grâce à l'information sur la réputation, vous pouvez bloquer sélectivement les sites dans une catégorie que vous souhaitez autoriser autrement.

i) Cliquez sur le **+** à côté de la liste des **URL** à gauche de la liste des catégories.

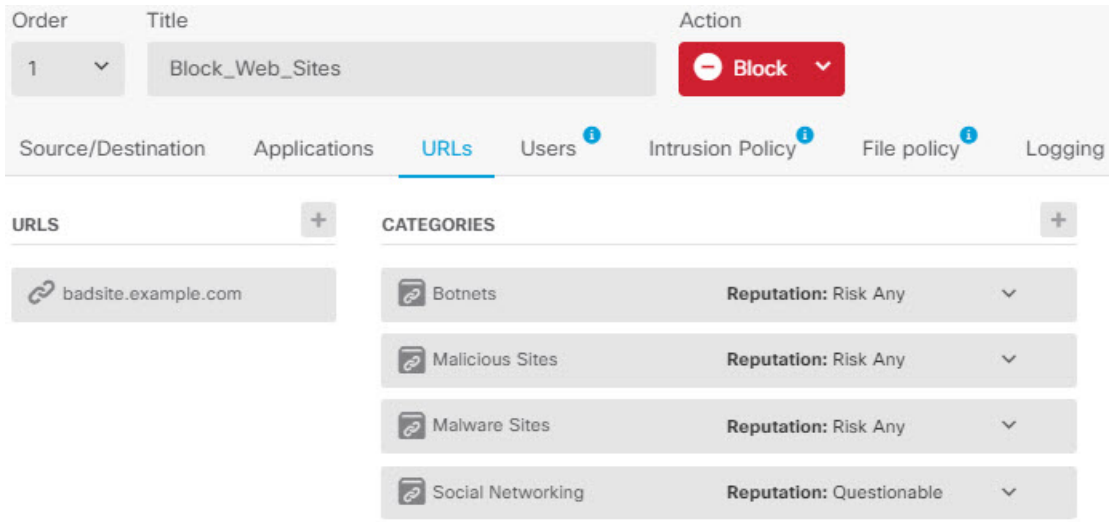
j) Au bas de la boîte de dialogue contextuelle, cliquez sur le lien **Create New URL** (créer une URL).

k) Entrez **badsite.exemple.com** pour le nom et l'URL, puis cliquez sur **OK** pour créer l'objet.

Vous pouvez nommer l'objet comme l'URL ou donner un nom différent à l'objet. Pour l'URL, n'incluez pas la partie protocole de l'URL, ajoutez simplement le nom du serveur.

l) Sélectionnez le nouvel objet, puis cliquez sur **OK**.

L'ajout de nouveaux objets lors de la modification des politiques ajoute simplement l'objet à la liste. Le nouvel objet n'est pas automatiquement sélectionné.



m) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations de catégorie et de réputation dans le tableau de bord de catégorie Web et les événements de connexion.

n) Cliquez sur **OK** pour enregistrer la règle.

Étape 3 (Facultatif) Définissez les préférences de filtrage d'URL.

Lorsque vous activez la licence URL, le système active automatiquement les mises à jour de la base de données de catégories Web. Le système recherche les mises à jour toutes les 30 minutes, bien que les données soient généralement mises à jour une fois par jour. Vous pouvez désactiver ces mises à jour si, pour une raison quelconque, vous ne souhaitez pas les mettre en œuvre.

Vous pouvez également choisir d'envoyer à Cisco des URL qui ne sont pas catégorisées pour analyse. Ainsi, si la base de données URL installée ne dispose pas d'une catégorisation pour un établissement, le Cisco Cloud peut en avoir une. Le nuage renvoie la catégorie et la réputation, et vos règles basées sur la catégorie peuvent alors être appliquées correctement à la requête URL. La sélection de cette option est importante pour les systèmes bas de gamme, qui installent une base de données d'URL plus petite en raison de contraintes de mémoire. Vous pouvez définir une durée de vie pour les résultats de la recherche : la valeur par défaut est Never (jamais), ce qui signifie que les résultats de la recherche ne sont jamais actualisés.

a) Cliquez sur **Device (périphérique)**.
b) Cliquez sur **System Settings** > **Traffic Settings** > **URL Filtering Preferences**.
c) Sélectionnez **Query Cisco CSI for Unknown URLs** (interroger Cisco CSI pour les URL inconnues).
d) Sélectionnez une durée de vie URL raisonnable (**URL Time to Live**), par exemple 24 heures.
e) Cliquez sur **Save** (enregistrer).

Étape 4 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.

Prochaine étape

À ce stade, les tableaux de bord et les événements de surveillance devraient commencer à afficher des informations sur les réputations et les catégories web et sur les connexions abandonnées. Vous pouvez évaluer ces informations pour déterminer si votre filtrage d'URL abandonne uniquement les sites qui sont répréhensibles, ou si vous avez besoin d'assouplir les paramètres de réputation pour certaines catégories.

Pensez à informer les utilisateurs au préalable que vous allez bloquer l'accès aux sites Web en fonction de leur catégorie et de leur réputation.

Comment contrôler l'utilisation des applications

Le Web est une plateforme désormais omniprésente pour la distribution des applications dans l'entreprise, qu'il s'agisse de plateformes d'applications basées sur un navigateur Web ou d'applications multimédias qui utilisent des protocoles Web pour l'entrée et la sortie des réseaux d'entreprise.

FTD inspecte les connexions pour déterminer l'application utilisée. Cela permet d'établir des règles de contrôle d'accès ciblées sur les applications, plutôt que de cibler des ports TCP/UDP spécifiques. Ainsi, vous pouvez bloquer ou autoriser sélectivement les applications Web même si elles utilisent le même port.

Bien que vous puissiez sélectionner des applications spécifiques à autoriser ou à bloquer, vous pouvez également rédiger des règles en fonction du type, de la catégorie, de l'étiquette, du risque ou de la pertinence de l'entreprise. Par exemple, vous pouvez créer une règle de contrôle d'accès qui identifie et bloque toutes les applications à haut risque et à faible pertinence commerciale. Si un utilisateur tente d'utiliser l'une de ces applications, la session est bloquée.

Cisco procède fréquemment à la mise à jour ou à l'ajout de détecteurs d'applications supplémentaires au moyen des mises à jour du système et de la base de données sur les vulnérabilités (VDB). Ainsi, une règle bloquant les applications à risque élevé peut s'appliquer automatiquement aux nouvelles applications sans que vous ayez à mettre à jour la règle manuellement.

Dans ce scénario, nous bloquerons toute application appartenant à la catégorie **anonymizer/proxy** (anonymiseur/serveur mandataire).

Avant de commencer

Ce scénario se fonde sur l'hypothèse voulant que vous ayez terminé le scénario Comment mieux comprendre le trafic de votre réseau, à la page 7. Le scénario explique comment recueillir des informations sur l'utilisation des applications, que vous pouvez analyser dans le tableau de bord des applications. La compréhension des applications réellement utilisées peut vous aider à concevoir des règles efficaces basées sur les applications. Le scénario explique également comment planifier les mises à jour de la VDB, qui ne seront pas reproduites ici. Assurez-vous de mettre à jour la VDB régulièrement afin que les applications puissent être correctement identifiées.

Procédure

Étape 1 Créez la règle de contrôle d'accès basée sur l'application.

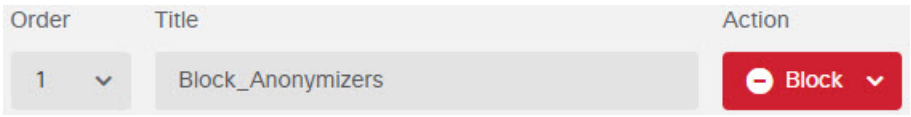
a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

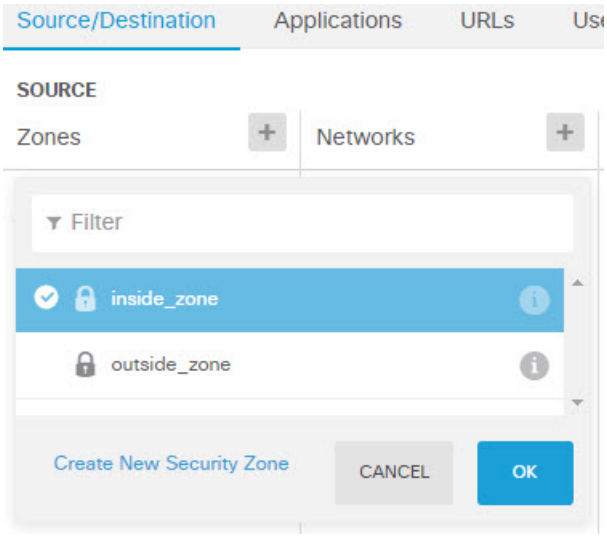
b) Cliquez sur **+** pour ajouter une nouvelle règle.

c) Configurez l'ordre, le titre et l'action.

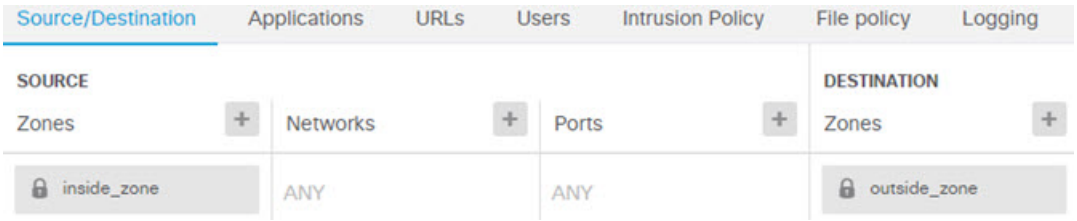
- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons la même source/destination que la règle Inside_Outside_Rule créée lors de la configuration initiale de l'appareil. Vous avez peut-être également créé d'autres règles également. Pour maximiser l'efficacité du contrôle d'accès, il est préférable d'établir des règles précises dès le début, afin de déterminer rapidement si une connexion est autorisée ou interrompue. Dans cet exemple, sélectionnez **1** comme ordre des règles.
- **Title** (titre) : Donnez un nom significatif à la règle, par exemple Block_Anonymizers.
- **Action** : Sélectionnez **Block**.



d) Dans l'onglet **Source/Destination**, cliquez sur **+** pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.



e) En utilisant la même technique, sélectionnez **outside_zone** pour les zones de destination (**Destination** > **Zones**).



f) Cliquez sur l'onglet **Applications**.

g) Cliquez sur le signe **+** pour les **Applications**, puis cliquez sur le lien **Advanced Filter** (filtre avancé) au bas de la boîte de dialogue contextuelle.

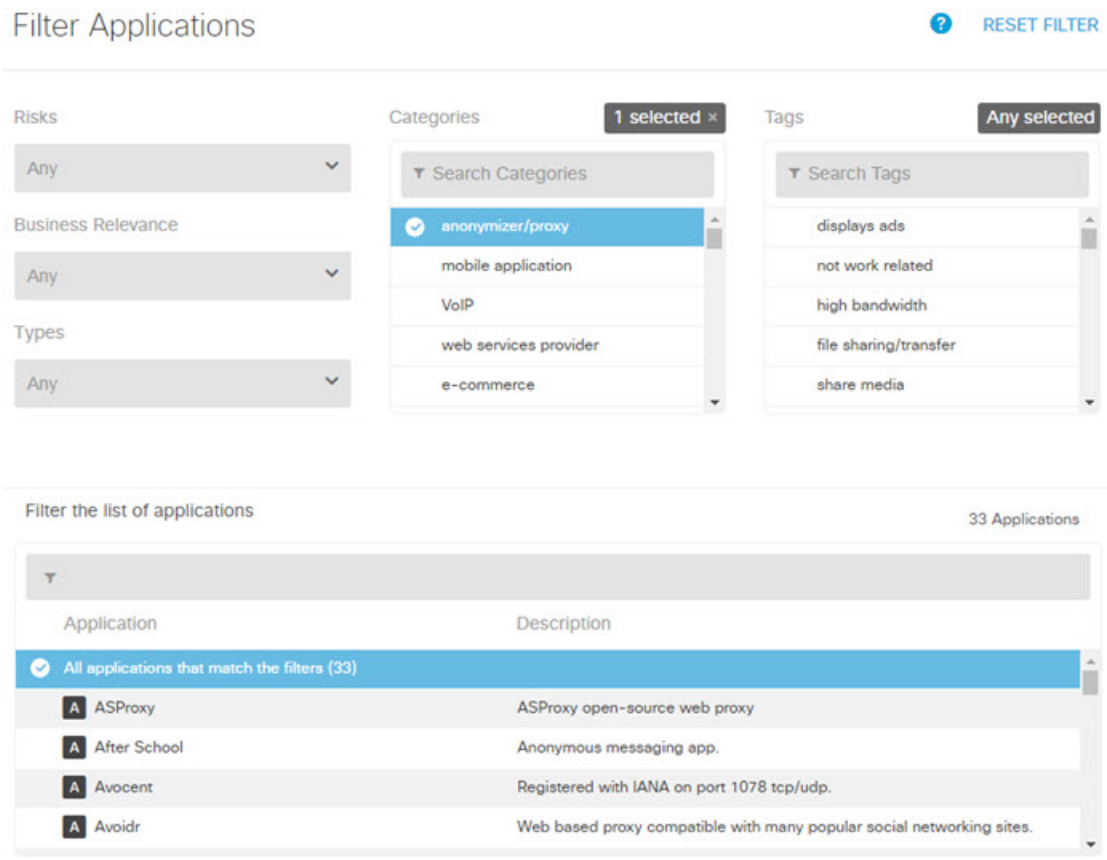
Bien que vous puissiez créer des objets de filtre d'application au préalable et les sélectionner dans la liste des filtres d'application ici, vous pouvez également spécifier des critères directement dans la règle de contrôle d'accès, et éventuellement enregistrer les critères en tant qu'objet de filtre. À moins d'écrire une règle pour une seule application, il est plus facile d'utiliser la boîte de dialogue de filtre avancé (Advanced Filter) pour trouver des applications et créer des critères appropriés.

À mesure que vous sélectionnez des critères, la liste des applications au bas de la boîte de dialogue est mise à jour pour afficher avec exactitude les applications qui correspondent aux critères. La règle que vous établissez s'applique à ces applications.

Examinez attentivement cette liste. Par exemple, vous pourriez être tenté de bloquer toutes les applications à très haut risque. Cependant, à ce jour, l'application TFPT est considérée comme à très haut risque. La plupart des entreprises ne veulent pas bloquer cette application. Prenez le temps

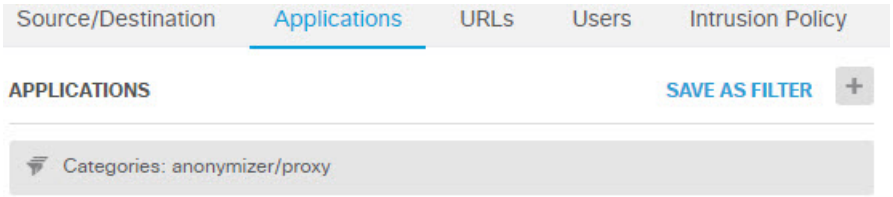
d'expérimenter en adoptant différents critères de filtrage pour voir quelles applications correspondent à vos sélections. Gardez à l'esprit que ces listes peuvent changer à chaque mise à jour de VDB.

Pour les besoins de cet exemple, sélectionnez les anonymiseurs et serveurs mandataires (anonymizers/proxies) dans la liste des catégories (Categories).



h) Cliquez sur **Add** (ajouter) dans la boîte de dialogue des filtres avancés (Advanced Filters).

Le filtre est ajouté et affiché sous l'onglet Applications.



i) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations sur les connexions bloquées par cette règle.

j) Cliquez sur **OK** pour enregistrer la règle.

Étape 2 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 3 Cliquez sur **Monitoring** (suivi) et évaluez les résultats.

Vous pouvez maintenant voir les connexions abandonnées sur le widget Applications du tableau de bord **Network Overview** (aperçu du réseau). Utilisez les options déroulantes **All/Denied/Allowed** pour vous concentrer uniquement sur les applications abandonnées.

Vous pouvez également trouver des informations sur les applications sur le tableau de bord des applications Web (**Web Applications**). Les tableaux de bord **Applications** affichent les résultats liés au protocole. Si une personne tente d'utiliser ces applications, en supposant que vous avez activé les politiques d'identité et exigez une authentification, vous devriez être en mesure d'établir un lien entre l'application et l'utilisateur qui tente la connexion.

Comment ajouter un sous-réseau

Si une interface est disponible sur votre appareil, vous pouvez la connecter à un commutateur (ou à un autre routeur) pour fournir des services à un autre sous-réseau.

Il y a plusieurs raisons pour lesquelles vous pourriez souhaiter ajouter un sous-réseau. Pour ce scénario d'utilisation, nous aborderons le scénario typique suivant.

- Le sous-réseau est un réseau interne qui utilise le réseau privé 192.168.2.0/24.
- L'interface du réseau a l'adresse statique 192.168.2.1. Dans cet exemple, l'interface physique est dédiée au réseau. Une autre option consiste à utiliser une interface déjà câblée et à créer une sous-interface pour le nouveau réseau.
- Le périphérique fournira des adresses aux postes de travail sur le réseau au moyen de DHCP, en utilisant 192.168.2.2-192.168.2.254 comme ensemble d'adresses.
- L'accès réseau aux autres réseaux internes et au réseau externe sera autorisé. Le trafic vers le réseau externe utilisera NAT pour obtenir une adresse publique.

Remarque Cet exemple suppose que l'interface inutilisée ne fait pas partie d'un groupe de ponts. S'il s'agit actuellement d'un membre du groupe de ponts, vous devez d'abord le retirer du groupe de ponts avant de suivre cette procédure.

Avant de commencer

Connectez physiquement le câble réseau à l'interface et au commutateur du nouveau sous-réseau.

Procédure

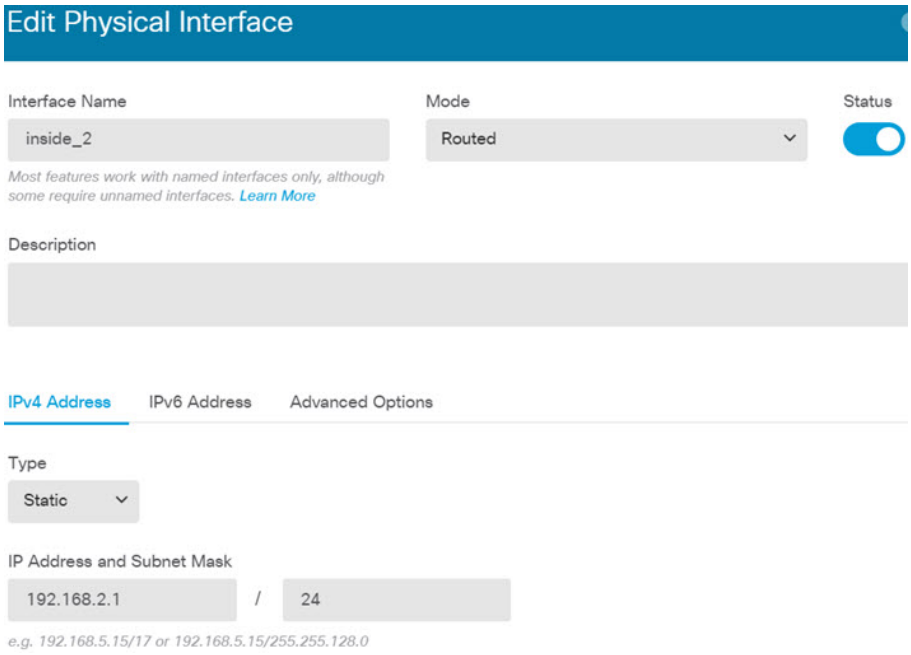
Étape 1 Configurez l'interface.

a) Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé des **Interfaces**. Cliquez ensuite sur le type d'interfaces pour consulter la liste des interfaces.

b) Passez la souris sur la cellule **Actions** sur le côté droit de la ligne pour l'interface que vous avez câblée, puis cliquez sur l'icône de modification ( ).

c) Configurez les propriétés de base de l'interface.

- **Name** (nom) : Un nom unique pour l'interface. Dans cet exemple, le nom sera **inside_2**.
- **Mode** : Sélectionnez **Routed** (routage).
- **Status** (état) : Cliquez sur le bouton d'état pour activer l'interface.
- Onglet **IPv4 Address** : Sélectionnez **Static** (statique) pour le **Type**, puis entrez **192.168.2.1/24**.



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

La liste des interfaces affiche l'état de l'interface mis à jour et l'adresse IP configurée.

Étape 2 Configurez le serveur DHCP pour l'interface.

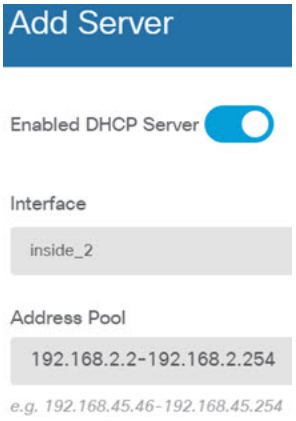
a) Cliquez sur **Device (périphérique)**.

b) Cliquez sur **System Settings (paramètres système)** > **DHCP Server (serveur DHCP)**.
c) Cliquez sur l'onglet **DHCP Servers** (serveurs DHCP).

Le tableau répertorie tous les serveurs DHCP existants. Si vous utilisez la configuration par défaut, la liste en comprend une pour l'interface interne.

d) Cliquez sur + au-dessus du tableau.
e) Configurez les propriétés du serveur.

- **Enable DHCP Server (activer le serveur DHCP)** : Ce bouton permet d'activer le serveur.
- **Interface** : Sélectionnez l'interface sur laquelle vous fournissez des services DHCP. Dans cet exemple, sélectionnez inside_2.
- **Address Pool** (ensemble d'adresse) : Les adresses que le serveur peut fournir aux périphériques du réseau. Entrez 192.168.2.2-192.168.2.254. Assurez-vous de ne pas inclure l'adresse réseau (.0), l'adresse d'interface (.1) ou l'adresse de diffusion (.255). En outre, si vous avez besoin d'adresses statiques pour des périphériques sur le réseau, excluez ces adresses du groupe. Le pool doit être composé d'une seule série continue d'adresses. Choisissez donc des adresses statiques en début ou en fin de plage.



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

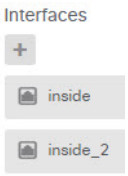
#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

Étape 3 Ajoutez l'interface à la zone de sécurité interne.

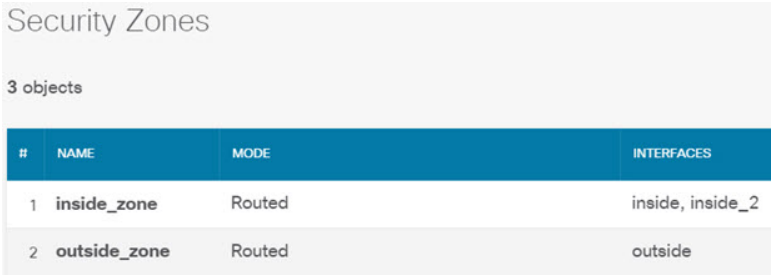
Pour établir des politiques sur une interface, l'interface doit appartenir à une zone de sécurité. Vous établissez des politiques pour les zones de sécurité. Ainsi, lorsque vous ajoutez et supprimez des interfaces dans les zones, vous modifiez automatiquement les politiques appliquées à l'interface.

a) Cliquez sur **Objects** (objets) dans le menu principal.
b) Sélectionnez **Security Zones** (zones de sécurité) dans la table des matières.
c) Passez la souris sur la cellule **Actions** sur le côté droit de la ligne pour l'objet **inside_zone**, puis cliquez sur l'icône de modification ( ).

d) Cliquez sur + sous **Interfaces**, sélectionnez l'interface inside_2, puis cliquez sur **OK** dans la liste des interfaces.



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



Étape 4 Créez une règle de contrôle d'accès qui autorise le trafic entre les réseaux internes.

Le trafic n'est pas autorisé automatiquement entre les interfaces. Vous devez créer des règles de contrôle d'accès pour autoriser le trafic que vous souhaitez. La seule exception : si vous autorisez le trafic dans l'action par défaut de la règle de contrôle d'accès. Pour les besoins de cet exemple, nous supposerons que vous avez conservé l'action de blocage par défaut que l'assistant de configuration de périphérique configure. Ainsi, vous devez créer une règle qui autorisera le trafic entre les interfaces internes. Si vous avez déjà créé une règle comme celle-ci, ignorez cette étape.

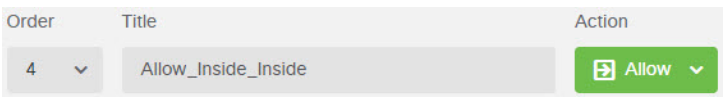
a) Cliquez sur **Policies** (politiques) dans le menu principal.

Assurez-vous que la politique de contrôle d'accès (**Access Control**) est affichée.

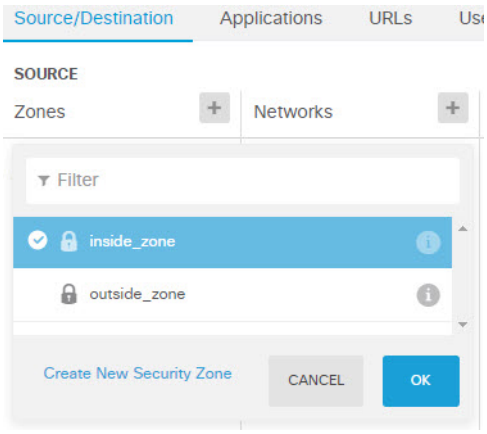
b) Cliquez sur + pour ajouter une nouvelle règle.

c) Configurez l'ordre, le titre et l'action.

- **Order** (ordre) : la valeur par défaut consiste à ajouter de nouvelles règles à la fin de la politique de contrôle d'accès. Cependant, vous devez placer cette règle avant (au-dessus) de toute règle qui correspondrait à la même source ou destination et à d'autres critères, sinon la règle ne sera jamais mise en correspondance (une connexion se conforme à une seule règle, c.-à-d. la première règle à laquelle elle correspond dans le tableau). Pour cette règle, nous utiliserons des critères de Source/Destination uniques, donc l'ajout de la règle à la fin de la liste est acceptable.
- **Title** (title) : Attribuez un nom significatif à la règle, par exemple Allow_Inside_Inside.
- **Action** : Sélectionnez **Allow** (autoriser).

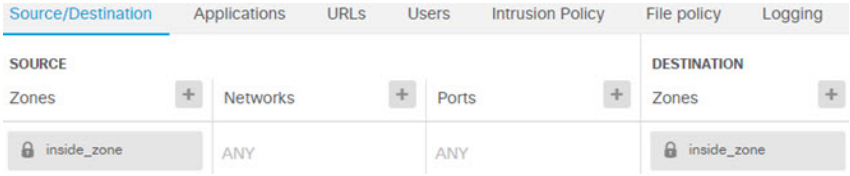


d) Dans l'onglet **Source/Destination**, cliquez sur + pour **Source** > **Zones**, sélectionnez **inside_zone**, puis cliquez sur **OK** dans la boîte de dialogue des zones.



e) Selon cette même méthode, pour définir les zones de destination, sélectionnez **inside_zone** sous **Destination** > **Zones**.

Une zone de sécurité doit contenir au moins deux interfaces pour sélectionner la même zone pour la source et la destination.



f) (Facultatif) Configurez l'inspection des intrusions et des logiciels malveillants.

Bien que les interfaces internes se trouvent dans une zone de confiance, il est courant que les utilisateurs connectent des ordinateurs portables au réseau. Ainsi, un utilisateur pourrait inconsciemment introduire une menace à l'intérieur de votre réseau à partir d'un réseau externe ou d'un point d'accès Wi-Fi. Vous pouvez rechercher les intrusions et les logiciels malveillants dans le trafic entre vos réseaux internes.

Pensez à faire ce qui suit.

- Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions) et activez la politique, et sélectionnez la politique Balanced Security and Connectivity (équilibre entre la sécurité et la connectivité).
- Cliquez sur l'onglet **File Policy**, puis sélectionnez la politique visant à bloquer les logiciels malveillants (Block Malware All).

g) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **Select Log Action (choisir l'action de journalisation)** > **At Beginning and End of Connection (au début et à la fin de la connexion)**.

Vous devez activer la journalisation pour obtenir des informations sur les connexions qui correspondent à cette règle. La journalisation ajoute des statistiques au tableau de bord et affiche les événements dans le visualiseur d'événements.

h) Cliquez sur **OK** pour enregistrer la règle.

Étape 5 Vérifiez que les politiques requises sont définies pour le nouveau sous-réseau.

En ajoutant l'interface à la zone de sécurité inside_zone, toutes les politiques existantes pour inside_zone s'appliquent automatiquement au nouveau sous-réseau. Cependant, prenez le temps d'inspecter vos politiques et assurez-vous qu'aucune politique supplémentaire n'est nécessaire.

Si vous avez terminé la configuration initiale de l'appareil, les politiques suivantes devraient déjà s'appliquer.

- **Access Control** (contrôle d'accès) : La règle Inside_Outside_Règlement devrait autoriser tout le trafic entre le nouveau sous-réseau et le réseau externe. Si vous avez suivi les scénarios d'utilisation précédents, la politique prévoit également une inspection des intrusions et des logiciels malveillants. Vous devez établir une règle qui autorise le trafic entre le nouveau réseau et le réseau externe, sinon les utilisateurs ne peuvent pas accéder à Internet ou à d'autres réseaux externes.
- **NAT** : La règle InsideOutsideNATrule s'applique à n'importe quelle interface allant vers l'interface externe et applique le PAT d'interface. Si vous respectez cette règle, le trafic du nouveau réseau vers l'extérieur verra l'adresse IP traduite en un port unique sur l'adresse IP de l'interface externe. Si vous n'avez pas de règle qui s'applique à toutes les interfaces ou aux interfaces inside_zone, lorsque vous passez à l'interface externe, vous devrez peut-être en créer une maintenant.
- **Identity** (identity) : Aucune politique d'identité par défaut n'a été établie. Cependant, si vous avez suivi les scénarios d'utilisation précédents, vous pourriez avoir une politique d'identité qui nécessite déjà une authentification pour le nouveau réseau. Si aucune politique d'identité ne s'applique, créez-en une maintenant si vous souhaitez obtenir des informations basées sur l'utilisateur pour le nouveau réseau.

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.

Prochaine étape

Vérifiez que les stations de travail du nouveau sous-réseau obtiennent des adresses IP à l'aide de DHCP et qu'elles peuvent atteindre d'autres réseaux internes et externes. Utilisez les tableaux de bord de surveillance et le visualiseur d'événements pour évaluer l'utilisation du réseau.

Comment surveiller passivement le trafic sur un réseau

Un périphérique Cisco Firepower Threat Defense est normalement déployé comme pare-feu actif et dispositif de sécurité IPS (système de prévention des intrusions). La fonction principale de l'appareil est de fournir une protection active au réseau en supprimant les connexions indésirables et les menaces.

Cependant, vous pouvez également déployer le système en mode passif. Dans ce mode, l'appareil analyse simplement le trafic sur les ports de commutation surveillés. Ce mode se destine principalement à des fins de démonstration ou de test. Il vous permet de vous familiariser avec le périphérique avant de le déployer en tant

que pare-feu actif. Grâce à un déploiement passif, vous pouvez surveiller les types de menaces qui apparaissent sur le réseau, les catégories d'URL parcourues par les utilisateurs, etc.

Bien que vous utilisiez normalement le mode passif à des fins de démonstration ou de test uniquement, vous pouvez également utiliser le mode passif dans un environnement de production s'il fournit un service dont vous avez besoin, tel que l'IDS (système de détection des intrusions sans prévention). Vous pouvez combiner des interfaces passives avec des interfaces actives de routage de pare-feu pour fournir la combinaison exacte des services requis par votre organisation.

La procédure suivante explique comment déployer le système de manière passive pour analyser le trafic passant par un nombre limité de ports de commutation.

Remarque Cet exemple concerne un périphérique Cisco Firepower Threat Defense matériel. Vous pouvez également utiliser le mode passif pour for FTDv, mais la configuration du réseau est différente. Pour de plus amples renseignements, consultez la section Configurer le VLAN pour une interface passive FTDv. Sinon, cette procédure s'applique également à FTDv.

Avant de commencer

Cette procédure suppose que vous avez connecté les interfaces interne et externe et terminé la configuration initiale du périphérique avec l'assistant. Même dans un déploiement passif, vous avez besoin d'une connexion Internet pour télécharger les mises à jour des bases de données du système. Vous devez également être en mesure de vous connecter à l'interface de gestion pour ouvrir FDM, ce que vous pouvez faire au moyen de connexions directes au port intérieur ou de gestion.

Cet exemple suppose également que vous avez activé syslog pour les politiques de prévention des intrusions dans la page **Policies** > **Intrusion**.

Procédure

Étape 1 Configurez un port de commutation comme port SPAN (Switched Port Analyzer) et configurez une session de surveillance pour les interfaces source.

Dans l'exemple suivant, un port SPAN et une session de surveillance sont configurés pour deux interfaces sources sur un commutateur de la gamme Cisco Nexus 5000. Si vous utilisez un type de commutateur différent, les commandes requises pourraient différer.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

Pour vérifier :

```
switch# show monitor session 1 brief
   session 1
```

```
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

Étape 2 Connectez l'interface Cisco Firepower Threat Defense au port SPAN du commutateur.

Il est préférable de sélectionner un port actuellement inutilisé sur le périphérique Cisco Firepower Threat Defense. Selon l'exemple de configuration du commutateur, vous devez connecter le câble à l'Ethernet 1/48 du commutateur. Il s'agit de l'interface de destination pour la session de surveillance.

Étape 3 Configurez l'interface Cisco Firepower Threat Defense en mode passif.

a) Cliquez sur **Device** (périphérique), puis sur le lien dans le **résumé des** interfaces. Cliquez ensuite sur **Interfaces** ou **EtherChannels**.

b) Cliquez sur l'icône de modification ( ) pour l'interface physique ou le port EtherChannel que vous souhaitez modifier.

Choisissez une interface actuellement inutilisée. Si vous avez l'intention de convertir une interface en cours d'utilisation en interface passive, vous devez d'abord supprimer l'interface de toute zone de sécurité et supprimer toutes les autres configurations qui utilisent l'interface.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) Configurez les éléments suivants :

- **Interface Name** : le nom de l'interface (jusqu'à 48 caractères). Les caractères alphabétiques doivent être en minuscules. Par exemple, **surveiller**.
- **Mode** : Sélectionnez **Passive** (passif).

e) Cliquez sur **OK**.

Étape 4 Créez une zone de sécurité passive pour l'interface.

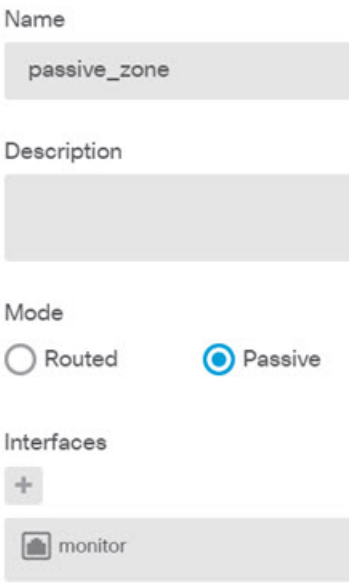
a) Sélectionnez **Objects** (objets), puis **Security Zones** (zones de sécurité) dans la table des matières.

b) Cliquez sur le bouton **+**.

c) Entrez un nom pour l'objet (sous **Name**) et, facultativement, une description. Par exemple, **passive_zone**.

d) Sous **Mode**, sélectionnez **Passive** (passif).

e) Cliquez sur **+** et sélectionnez l'interface passive.



f) Cliquez sur **OK**.

Étape 5 Configurez une ou plusieurs règles de contrôle d'accès pour la zone de sécurité passive.

Le nombre et le type de règles que vous créez dépendent des informations que vous souhaitez réunir. Par exemple, si vous souhaitez configurer le système en tant qu'IDS (système de détection des intrusions), vous devez configurer au moins une règle d'autorisation comprenant une politique de prévention des intrusions attribuée. Si vous souhaitez réunir des données sur des catégories d'URL, vous avez besoin d'au moins une règle comprenant une catégorie d'URL précisée.

Vous pouvez créer des règles de blocage pour consulter de l'information sur les connexions que le système aurait bloquées sur une interface à routage actif. Ces connexions ne sont pas bloquées, car l'interface est passive, mais vous verrez clairement comment le système aurait préparé le trafic sur le réseau.

Les scénarios d'utilisation suivants couvrent les principales utilisations des règles de contrôle d'accès. Ceux-ci s'appliquent également aux interfaces passives. Il suffit de sélectionner la zone de sécurité passive comme zone source pour les règles que vous créez.

- Comment bloquer les menaces, à la page 15
- Comment bloquer les logiciels malveillants, à la page 20
- Comment mettre en œuvre une politique d'utilisation acceptable (filtrage d'URL), à la page 23
- Comment contrôler l'utilisation des applications, à la page 28

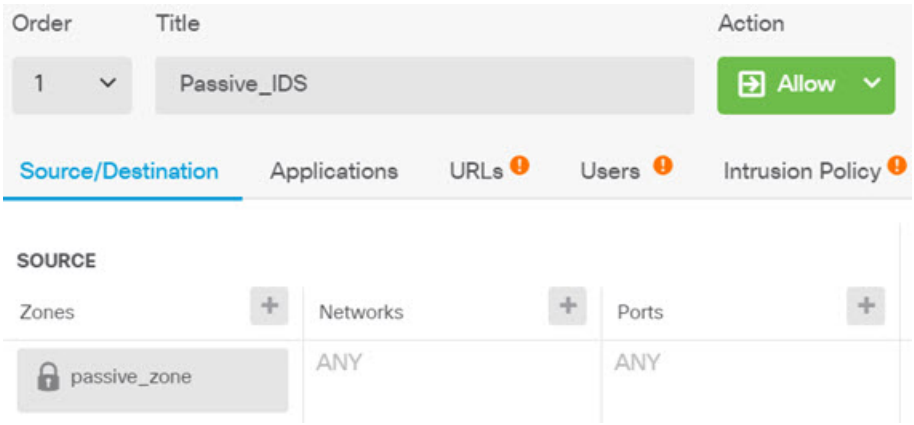
La procédure suivante crée deux règles d'autorisation pour appliquer une politique de prévention des intrusions et pour réunir des données de catégorie d'URL.

a) Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.
b) Cliquez sur le signe plus (+) pour ajouter une règle autorisant tout trafic, mais appliquant une politique de prévention des intrusions.
c) Sélectionnez **1** comme ordre des règles. Cette règle est plus spécifique que la règle par défaut, mais ne la chevauche pas. Si vous avez déjà établi des règles personnalisées, sélectionnez la position appropriée pour que le trafic vers l'interface passive ne corresponde pas à ces règles.
d) Saisissez un nom pour la règle, par exemple **Passive_IDS**.

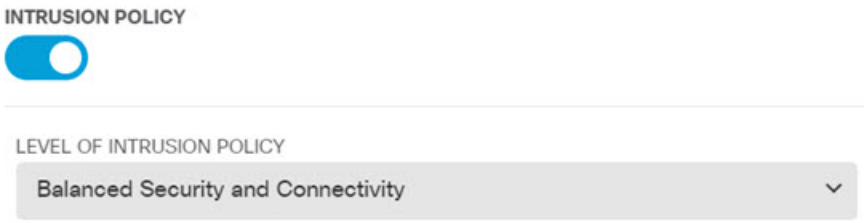
e) Sélectionnez **Allow** (autoriser) sous **Action**.

f) Sous l'onglet **Source/Destination**, sélectionnez la zone passive pour **Source** > **Zones**. Ne configurez aucune autre option pour l'onglet.

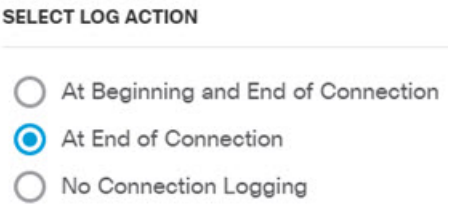
Lors de l'exécution en mode d'évaluation, la règle devrait être la suivante :



g) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions), réglez le curseur sur **On** (activée) et sélectionnez une politique de prévention des intrusions, comme la politique **Balanced Security and Connectivity** (équilibre entre la sécurité et la connectivité), qui est recommandée pour la plupart des réseaux.



h) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **At End of Connection**(à la fin de la connexion) pour l'option de journalisation.



i) Cliquez sur **OK**.

j) Cliquez sur **+** pour ajouter une règle qui exigera que le système effectue une inspection approfondie pour déterminer l'URL et la catégorie de toutes les requêtes HTTP.

Cette règle vous permet de voir les informations de catégorie d'URL dans les tableaux de bord. Pour économiser du temps de traitement et améliorer les performances, le système détermine la catégorie d'URL uniquement s'il existe au moins une règle de contrôle d'accès qui spécifie une condition de catégorie d'URL.

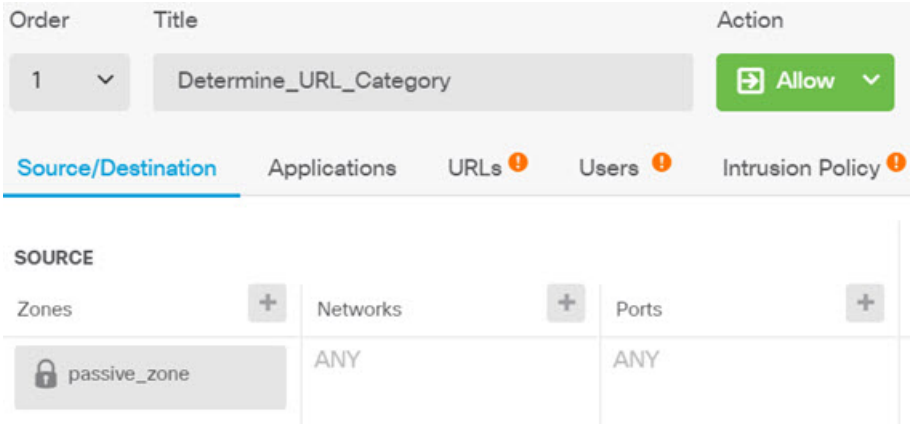
k) Sélectionnez **1** comme ordre des règles. Cela la placera au-dessus de la règle précédente (Passive_IDS). Si vous la placez après cette règle (qui s'applique à tout le trafic), la règle que vous créez maintenant ne sera jamais mise en correspondance.

l) Saisissez un nom pour la règle, par exemple, **Determine_URL_Category**.

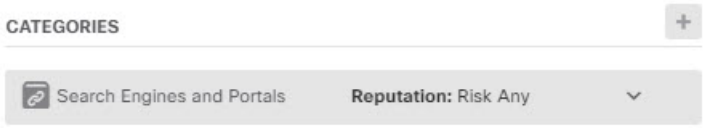
m) Sélectionnez **Allow** (autoriser) sous **Action**.

Sinon, vous pouvez sélectionner **Block** (bloquer). L'une ou l'autre des actions permettra d'atteindre votre objectif pour cette règle.

n) Sous l'onglet **Source/Destination**, sélectionnez la zone passive pour **Source** > **Zones**. Ne configurez aucune autre option pour l'onglet.



o) Cliquez sur l'onglet **URLs**, cliquez sur le signe plus (+) à côté de **Categories** (catégories), puis sélectionnez l'une des catégories. Par exemple, **Search Engines and Portals (portails et moteurs de recherche)**. Vous pouvez éventuellement sélectionner un niveau de réputation ou le laisser à la valeur par défaut « Any » (n'importe lequel).



p) Cliquez sur l'onglet **Intrusion Policy** (politique de prévention des intrusions), réglez le curseur sur **On** (activée), puis sélectionnez la même politique de prévention que pour la première règle.

q) Cliquez sur l'onglet **Logging** (journalisation) et sélectionnez **At End of Connection**(à la fin de la connexion) pour l'option de journalisation.

Toutefois, si vous avez sélectionné l'action **Block** (bloquer), sélectionnez l'option au début et à la fin de la connexion (**At Beginning and End of Connection**). Comme les connexions bloquées ne sont pas terminées en tant que telles, vous obtenez uniquement des informations de journalisation au début de la connexion.

r) Cliquez sur **OK**.

Étape 6 (Facultatif) Configurer d'autres politiques de sécurité.

Vous pouvez également configurer les politiques de sécurité suivantes pour voir leur incidence sur le trafic :

- **Identity** (identité) : Permet de réunir des renseignements sur l'utilisateur. Vous pouvez configurer dans la politique sur l'identité une règle pour vous assurer que l'identité de l'utilisateur associé à une adresse IP est établie. Le processus de mise en œuvre des politiques sur l'identité pour les interfaces passives est

le même que pour les interfaces de routage. Veuillez suivre le scénario d'utilisation décrit dans Comment mieux comprendre le trafic de votre réseau, à la page 7.

- **Security Intelligence** (renseignements sur la sécurité) : Permettent de bloquer les mauvaises adresses IP et URL. Pour de plus amples renseignements, consultez la section Comment bloquer les menaces, à la page 15.

Remarque
Tout le trafic chiffré sur les interfaces passives est classé comme non déchiffrable, de sorte que les règles de déchiffrement SSL sont inefficaces et ne s'appliquent pas aux interfaces passives.

Étape 7 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 8 Utilisez les tableaux de bord de surveillance pour analyser les types de trafic et les menaces qui traversent le réseau. Si vous décidez que vous souhaitez que le périphérique Cisco Firepower Threat Defense supprime activement les connexions indésirables, redéployez le périphérique afin de pouvoir configurer des interfaces de routage actives qui assurent la protection par pare-feu du réseau surveillé.

Plus d'exemples

En plus des exemples présentés dans le chapitre Use Case (Cas d'utilisation), il existe des exemples de configuration dans certains chapitres qui expliquent des services spécifiques. Les exemples suivants pourraient vous intéresser.

Contrôle d'accès

- Comment contrôler l'accès au réseau à l'aide des balises de groupe de sécurité TrustSec

Traduction d'adresses réseau (NAT)

NAT pour les adresses IPv4

- Fournir l'accès à un serveur Web interne (NAT automatique statique)
- Adresse unique pour FTP, HTTP et SMTP (NAT automatique statique avec traduction de port)
- Traduction différente selon la destination (PAT manuelle dynamique)
- Traduction différente selon l'adresse et le port de destination (PAT manuelle dynamique)
- Modification de la réponse DNS, serveur DNS externe
- Modification de la réponse DNS, serveur DNS sur le réseau hôte

- Exemption du trafic VPN de site à site de la NAT

NAT pour les adresses IPv6

- Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe
- Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS
- Exemple NAT66, de traduction statique entre réseaux
- Exemple de NAT66, PAT d'interface IPv6 simple
- Modification de la réponse DNS64

Réseau privé virtuel d'accès à distance

- Comment mettre en œuvre la modification d'autorisation RADIUS
- Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP
- Comment fournir un accès Internet sur l'interface externe pour les utilisateurs du VPN d'accès à distance (Hair Pinning)
- Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance
- Comment contrôler l'accès VPN RA par groupe
- Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels.
- Comment personnaliser l'icône et le logo client AnyConnect

Réseau privé virtuel site à site (VPN)

- Exemption du trafic VPN de site à site de la NAT
- Comment fournir un accès Internet sur l'interface externe pour les utilisateurs d'un VPN site à site externe (hairpinning)
- Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Déchiffrement SSL/TLS

- Exemple : blocage des anciennes versions SSL/TLS du réseau

Politique FlexConfig

- Comment activer et désactiver les inspections globales par défaut
- Comment annuler vos modifications FlexConfig
- Comment activer les inspections pour les classes de trafic uniques

Routage virtuel

- Fournir un accès Internet à plusieurs routeurs virtuels avec des espaces d'adresses en chevauchement
- Comment effectuer un routage vers un serveur distant à l'aide de routeurs virtuels

- Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels.
- Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

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.