ASA 8.X et plus tard : Ajoutez ou modifiez une liste d'accès par l'exemple de configuration GUI ASDM

Contenu

Introduction

Ce document explique comment utiliser le Cisco Adaptive Security Device Manager (ASDM) afin de fonctionner avec des listes de contrôle d'accès. Ceci inclut la création d'une nouvelle liste d'accès, comment éditer une liste d'accès existante et d'autres fonctionnalités avec les Listes d'accès.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptable Cisco (ASA) avec la version 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) avec la version 6.3.X

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Des Listes d'accès sont principalement utilisées pour contrôler le trafic traversent le Pare-feu. Vous pouvez permettre ou refuser les types de trafic spécifiques avec des Listes d'accès. Chaque liste d'accès contient un certain nombre d'entrées de liste d'accès (as) ce contrôle la circulation d'une source spécifique à une destination spécifique. Normalement, cette liste d'accès est liée à une interface pour informer la direction de l'écoulement lequel elle devrait examiner. Des Listes d'accès sont principalement classées par catégorie dans deux larges types.

1. Listes d'accès en entrée
2. Listes d'accès sortantes

Les listes d'accès en entrée s'appliquent au trafic qui écrit cette interface, et les listes d'accès sortantes s'appliquent au trafic qui quitte l'interface. Notation d'arrivée/sortante se rapporte à la direction du trafic en termes de cette interface mais pas au mouvement du trafic entre plus élevé et les interfaces à niveau de sécurité inférieur.

Pour des connexions de TCP et UDP, vous n'avez pas besoin d'une liste d'accès pour permettre le trafic de renvoi parce que les dispositifs de sécurité permettent tout le trafic de renvoi pour les connexions bidirectionnelles établies. Pour des protocoles sans connexions tels que l'ICMP, les dispositifs de sécurité établissent des sessions unidirectionnelles, ainsi vous avez besoin de Listes d'accès pour appliquer des Listes d'accès à la source et aux interfaces de destination afin de permettre l'ICMP dans les deux directions, ou de vous le besoin d'activer l'engine d'inspection d'ICMP. L'engine d'inspection d'ICMP traite des sessions d'ICMP en tant que connexions bidirectionnelles.

De la version 6.3.X ASDM, il y a deux types de Listes d'accès que vous pouvez configurer.

1. Règles d'accès d'interface
2. Règles d'accès mondial

Remarque: La règle d'accès se rapporte à une entrée de la liste d'accès individuel (ACE).

Des règles d'accès d'interface sont liées à n'importe quelle interface au moment de leur création. Sans les lier à une interface, vous ne pouvez pas les créer. Ceci diffère de la ligne de commande exemple. Avec le CLI, vous créez d'abord la liste d'accès avec la **commande de liste d'accès**, et liez ensuite cette liste d'accès à une interface avec l'ordre d'**access-group**. ASDM 6.3 et plus tard,

la liste d'accès est créé et lié à une interface comme tâche simple. Ceci s'applique au trafic traversant cette interface spécifique seulement.

Des règles d'accès mondial ne sont liées à aucune interface. Ils peuvent être configurés par l'onglet de gestionnaire d'ACL dans l'ASDM et sont appliqués au trafic entrant global. Ils sont mis en application quand il y a une correspondance basée sur la source, la destination, et le type de protocole. Ces règles ne sont pas répliquées sur chaque interface, ainsi elles ménagent de l'espace mémoire.

Quand ces deux règles doivent être mises en application, les règles d'accès d'interface a normalement la priorité au-dessus des règles d'accès mondial.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ajoutez une nouvelle liste d'accès

Terminez-vous ces étapes afin de créer une nouvelle liste d'accès avec l'ASDM :

1. Choisissez la **configuration > le Pare-feu > les règles d'accès**, et cliquez sur le bouton de **règle d'accès d'ajouter**.
2. Choisissez l'interface à laquelle cette liste d'accès doit lier, avec l'action d'être exécuté sur du trafic l'autorisation c.-à-d.,/refusez. Cliquez sur alors le Detailsbutton afin de sélectionner le réseau de source.**Remarque:** Voici une brève explication des différents champs qui sont affichés dans cette fenêtre :**Interface** — Détermine l'interface à laquelle cette liste d'accès est liée.**Action** — Détermine le type d'action de la nouvelle règle. Deux options sont disponibles. **Laissez** permet tout le trafic assorti et **refuse à des** blocs tous le trafic assorti.**Le par la source** ce champ spécifie la source de trafic. Ceci peut être quelque chose parmi une adresse IP simple, un réseau, une adresse IP d'interface du Pare-feu ou un groupe d'objet de réseau. Ceux-ci peuvent être sélectionnés avec le bouton de **détails**.**Destination** — Ce champ spécifie la source de trafic. Ceci peut être quelque chose parmi une adresse IP simple, un réseau, une adresse IP d'interface du Pare-feu ou un groupe d'objet de réseau. Ceux-ci peuvent être sélectionnés avec le bouton de **détails**.**Service** — Ce champ détermine le protocole ou le service du trafic auquel cette liste d'accès est appliquée. Vous pouvez également définir un service-groupe qui contient un ensemble de différents protocoles.
3. Après que vous cliquiez sur les **détails** se boutonnent, une nouvelle fenêtre qui contient les objets de réseau existant est affichée. Sélectionnez l'à l'intérieur-**réseau**, et cliquez sur OK.
4. Vous êtes retourné à la fenêtre de **règle d'accès d'ajouter**. En introduisez au clavier le champ de destination. et cliquez sur OK afin de se terminer la configuration de la règle d'accès.

Ajoutez une règle d'accès avant existante :

Terminez-vous ces étapes afin d'ajouter une règle d'accès juste avant déjà une règle d'accès existante :

1. Sélectionnez l'entrée de liste d'accès existante, et cliquez sur l'**insertion du** menu déroulant d'**ajouter**
2. Choisissez la source et la destination, et cliquez sur le bouton de **détails du** champ de service pour choisir Protocol.
3. Choisissez le HTTP le protocole, et cliquez sur OK.
4. Vous êtes retourné à la fenêtre de règle d'accès d'insertion. Le champ de service est rempli de **TCP/HTTP** comme protocole sélectionné. Cliquez sur OK afin de se terminer la configuration de la nouvelle entrée de liste d'accès.

Vous pouvez maintenant observer la nouvelle règle d'accès affichée juste avant l'entrée déjà existante pour l'À l'intérieur-réseau.

Remarque: La commande des règles d'accès est très importante. Tout en traitant chaque paquet pour filtrer, l'ASA examine si le paquet apparie le critère l'un des de règle d'accès dans une commande séquentielle et si une correspondance se produit, elle implémente l'action de cette règle d'accès. Quand une règle d'accès est appariée, elle ne poursuit pas d'autres à règles d'accès et les vérifie de nouveau.

Ajoutez une règle d'accès après existante :

Terminez-vous ces étapes afin de créer une règle d'accès juste après déjà une règle d'accès existante.

1. Sélectionnez la règle d'accès après quoi vous le besoin d'avoir une nouvelle règle d'accès, et choisissez l'**insertion ensuite du** menu déroulant d'ajouter.
2. Spécifiez les champs d'interface, d'action, de source, de destination et de service, et cliquez sur OK pour se terminer la configuration cette règle d'accès.

Vous pouvez visualiser que la règle d'accès nouvellement configurée se repose juste après que déjà configurée.

Créez une liste d'accès standard

Terminez-vous ces étapes afin de créer une liste d'accès standard avec le GUI ASDM.

1. Choisissez la **configuration > le Pare-feu > a avancé > ACL standard > ajoutent**, et cliquent sur Add l'**ACL**.
2. Donnez un nombre dans la plage permise pour la liste d'accès standard, et cliquez sur OK.
3. Cliquez avec le bouton droit la liste d'accès, et choisissez **ajoutent ACE** afin d'ajouter une règle d'accès à cette liste d'accès.
4. Sélectionnez l'**action**, et spécifiez l'**adresse source**. S'il y a lieu, spécifiez la **description** également. Cliquez sur OK afin de se terminer la configuration de la règle d'accès.

Créez une règle d'accès mondial

Terminez-vous ces étapes afin de créer une liste d'accès étendue qui contient des règles d'accès mondial.

1. Choisissez la **configuration > le Pare-feu > a avancé > gestionnaire d'ACL > ajoutent**, et cliquent sur Add le bouton d'**ACL**.
2. Spécifiez un nom pour la liste d'accès, et cliquez sur OK.

3. Cliquez avec le bouton droit la liste d'accès, et choisissez **ajoutent ACE** afin d'ajouter une règle d'accès à cette liste d'accès.
4. Terminez-vous les champs d'action, de source, de destination, et de service, et cliquez sur OK afin de se terminer la configuration de la règle d'accès mondial.

Vous pouvez maintenant visualiser la règle d'accès mondial, comme affiché.

Éditez une liste d'accès existante

Cette section discute comment éditer un accès existant.

Éditez le champ de Protocol pour créer un groupe de service :

Terminez-vous ces étapes afin de créer un nouveau service-groupe.

1. Cliquez avec le bouton droit la règle d'accès qui doit être modifiée, et choisissez **éditent** afin de modifier cette règle d'accès spécifique.
2. Cliquez sur les **détails** se boutonnent afin de modifier le protocole associé avec cette règle d'accès.
3. Vous pouvez sélectionner n'importe quel protocole autre que le HTTP s'il y a lieu. S'il y a seulement un seul protocole à sélectionner, alors il n'y a aucun besoin de créer le groupe de service. Il est utile de créer un groupe de service quand il y a une condition requise d'identifier de nombreux protocoles non adjacents à apparier par cette règle d'accès.Choisissez **ajoutent > groupe de service de TCP** afin de créer un nouveau groupe de service de TCP.**Remarque:** De la même manière, vous pouvez également créer un nouveau groupe de service d'UDP ou groupe d'ICMP et etc.
4. Spécifiez un nom pour ce groupe de service, sélectionnez le protocole relatif au menu de côté gauche, et cliquez sur Add afin de les déplacer aux membres dans le menu de groupe du côté droit. Des protocoles nombreux peuvent être ajoutés comme membres d'un groupe de service basé sur la condition requise. Les protocoles sont ajoutés un. Après tout les membres sont ajoutés, cliquent sur OK.
5. Le groupe de service de création récente peut être visualisé sous les **groupes de service de TCP d'**onglet. Cliquez sur OK le bouton pour retourner à la fenêtre de règle d'accès d'éditer.
6. Vous pouvez voir que le champ de service est rempli avec le groupe de service de création récente. Cliquez sur OK afin de se terminer l'éditer.
7. Passer au-dessus votre souris au-dessus de ce groupe de service spécifique afin de visualiser tous les protocoles associés.

Éditez la source/champs de destination pour créer un groupe d'objet de réseau :

Des groupes d'objets sont utilisés pour simplifier la création et la maintenance des Listes d'accès. Quand vous groupez comme des objets ensemble, vous pouvez utiliser le groupe d'objets à ACE simple au lieu de devoir entrer dans ACE pour chaque objet séparément. Avant que vous créiez le groupe d'objets, vous devez créer les objets. En terminologie ASDM, l'objet s'appelle l'objet de réseau et le groupe d'objets s'appelle groupe d'objet de réseau.

Procédez comme suit :

1. Choisissez la **configuration > le Pare-feu > les objets > les objets de réseau/groupes > ajoutent**, et cliquent sur l'**objet de réseau** afin de créer un nouvel objet de réseau.
2. Complétez les champs de **nom**, d'**adresse IP** et de **netmask**, et cliquez sur OK.

3. L'objet de réseau de création récente peut être vu dans la liste des objets. Cliquez sur **OK**.
4. Choisissez la **configuration > le Pare-feu > les objets > les objets de réseau/groupes > ajoutent**, et cliquent sur le **groupe d'objet de réseau** afin de créer un nouveau groupe d'objet de réseau.
5. La liste disponible de tous les objets de réseau peut être trouvée sur le volet gauche de la fenêtre. Sélectionnez les différents objets de réseau, et cliquez sur le bouton d'**ajouter** afin de leur faire des membres du groupe d'objet de réseau de création récente. Le nom de groupe doit être spécifié dans le domaine alloué pour lui.
6. Cliquez sur OK après que vous ajoutiez tous les membres dedans pour grouper.Vous pouvez maintenant visualiser le groupe d'objet de réseau.
7. Afin de modifier n'importe quels source/champ de destination de liste d'accès existante avec un objet de groupe de réseau, cliquer avec le bouton droit la règle d'accès spécifique, et choisir **éditez**.
8. La fenêtre de règle d'accès d'éditer apparaît. Cliquez sur en fonction le bouton de **détails du** champ de source afin de le modifier.
9. Sélectionnez le groupe d'objet de réseau de Tout-Interne-**hôtes**, et cliquez sur OK le bouton.
10. Cliquez sur **OK**.
11. Passer au-dessus votre souris au-dessus du champ de source de la règle d'accès afin de visualiser les membres du groupe.

Éditez le port de source :

Terminez-vous ces étapes afin de modifier le port de source d'une règle d'accès.

1. Afin de modifier le port de source d'une règle d'accès existante, la cliquer avec le bouton droit, et choisir **éditez**.La fenêtre de règle d'accès d'éditer apparaît.
2. Cliquez sur **plus de** bouton de déroulant d'**options** afin de modifier le champ de service de source, et cliquez sur OK.Vous pouvez visualiser la règle d'accès modifiée, comme affiché.

Supprimez une liste d'accès

Terminez-vous ces étapes afin de supprimer une liste d'accès :

1. Avant que vous supprimiez une liste d'accès existante, vous devez supprimer les entrées de liste d'accès (les règles d'accès). Il n'est pas possible de supprimer la liste d'accès à moins que vous supprimiez d'abord toutes les règles d'accès.Cliquez avec le bouton droit la règle d'accès d'être supprimé, et choisissez l'**effacement**.
2. Terminez-vous la même exécution d'effacement sur toutes les règles d'accès existantes, et puis sélectionnez la liste d'accès et choisissez l'**effacement** afin de le supprimer.

Exportez la règle d'accès

Les règles d'accès ASDM lient la liste d'accès avec l'interface respective tandis que le gestionnaire d'ACL dépiste toutes les Listes d'accès étendues. Les règles d'accès qui sont créées avec le gestionnaire d'ACL ne lient à aucune interface. Ces Listes d'accès sont généralement utilisées afin de Nat-exempt, du VPN-filtre et de semblable d'autres fonctions où il n'y a aucune association avec l'interface. Le gestionnaire d'ACL contient toutes les entrées que vous avez dans la section de **configuration > de Pare-feu > de règles d'accès**. En outre, le **gestionnaire d'ACL** contient également les règles d'accès mondial qui ne sont associées à aucune interface. L'ASDM est organisé de telle manière que vous puissiez exporter une règle d'accès de n'importe quelle

liste d'accès à un autre facilement.

Par exemple, si vous avez besoin d'une règle d'accès qui est déjà une partie d'une règle d'accès mondial d'être associé avec une interface, vous n'avez pas besoin de configurer cela de nouveau. Au lieu de cela, vous pouvez exécuter une **coupe et coller l'**exécution pour réaliser ceci.

1. Cliquez avec le bouton droit la règle d'accès spécifiée, et choisissez la **coupe**.
2. Sélectionnez la liste d'accès requise dans laquelle vous devez insérer cette règle d'accès. Vous pouvez employer la **pâte** dans la barre d'outil pour insérer la règle d'accès.

Exportez les informations de liste d'accès

Vous pouvez exporter les informations de liste d'accès à un autre fichier. Deux formats sont pris en charge pour exporter ces informations.

1. Format de la valeur séparé par virgule (CSV)
2. Format HTML

Cliquez avec le bouton droit les règles d'accès l'unes des, et choisissez l'**exportation** afin d'envoyer les informations de liste d'accès à un fichier.

Voici l'information affichée de liste d'accès dans le format HTML.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Exemples et TechNotes de configuration ASDM
- Exemples et Technotes de configuration ASA
- Support et documentation techniques - Cisco Systems