Utilisation du pare-feu Cisco IOS pour autoriser les applets Java provenant de sites connus à l'exclusion des autres

Contenu

Introduction

Cette configuration d'échantillon explique comment employer le Pare-feu de Cisco IOS® pour permettre des applet Java des sites Internet spécifiés, et refuse tous les autres. Ce type de blocage refuse l'accès aux applet Java qui ne sont pas encastrés dans archivé ou un fichier compressé. Le Pare-feu Cisco IOS a été introduit dans des versions du logiciel Cisco IOS 11.3.3.T et 12.0.5.T. Il est seulement présent où certains ensembles de caractéristiques sont achetés.

Vous pouvez voir quels ensembles de fonctionnalités de Cisco IOS prennent en charge le pare-feu d'IOS avec le conseiller de logiciel (clients enregistrés seulement).

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 :

- Routeur Cisco 1751
- Version du logiciel Cisco IOS c1700-k9o3sy7-mz.123-8.T.bin

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Refusez les applet Java de l'Internet

Suivez la procédure suivante :

1. Créez le Listes de contrôle d'accès (ACL).
2. Ajoutez les commandes de **Javas de HTTP d'ip inspect à la** configuration.
3. Appliquez-vous l'**ip inspect** et les **commandes access-list à l'**interface extérieure.**Remarque:** Dans cet exemple, l'ACL 3 permet des applet Java d'un site amical (10.66.79.236) tandis qu'il refuse implicitement des applet Java d'autres sites. Les adresses affichées sur l'extérieur du routeur ne sont pas Internet-routable parce que cet exemple a été configuré et testé dans un laboratoire.**Remarque: La liste d'accès n'est plus exigée** pour être appliquée sur l'interface extérieure si vous utilisez la version du logiciel Cisco IOS 12.3.4T ou plus tard. Ceci est documenté dans la nouvelle caractéristique de contournement d'ACL de Pare-feu.

Configurez

Cette section vous présente avec les informations que vous pouvez employer afin de configurer les caractéristiques ce document décrit.

Remarque: Afin de trouver les informations complémentaires sur les commandes que ce document utilise, se réfère au Command Lookup Tool (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise la configuration suivante :

Configuration du routeur

```
Current configuration : 1224 bytes
!
version 12.3
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname Australia
!
boot-start-marker
boot-end-marker
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
ip cef
ip inspect name firewall tcp ip inspect name firewall
udp !--- ACL used for Java. ip inspect name firewall
http java-list 3 audit-trail on ip ips po max-events 100
no ftp-server write-enable ! interface FastEthernet0/0
ip address 10.66.79.39 255.255.255.224 !--- ACL used to
block inbound traffic !--- except that permitted by
inspects. !--- This is no longer required on Cisco IOS
Software !--- Release 12.3.4T or later. ip access-group
100 in ip nat outside ip inspect firewall out ip
virtual-reassembly speed auto ! interface Serial0/0 no
ip address shutdown no fair-queue ! interface
Ethernet1/0 ip address 192.168.10.1 255.255.255.0 ip nat
inside ip virtual-reassembly half-duplex ! ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.33 no ip http server
no ip http secure-server !--- ACL used for Network
Address Translation (NAT). ip nat inside source list 1
interface FastEthernet0/0 overload ! !--- ACL used for
NAT. access-list 1 permit 192.168.10.0 0.0.0.255 !---
ACL used for Java. access-list 3 permit 10.66.79.236 !--
- ACL used to block inbound traffic !--- except that
permitted by inspects. !--- This is no longer required
on Cisco IOS !--- Software Release 12.3.4T or later.
access-list 100 deny ip any any ! ! control-plane ! !
line con 0 exec-timeout 0 0 line aux 0 line vty 0 4
login ! end
```

Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **sessions de show ip inspect** *[détail]* — Sessions existantes d'expositions actuellement dépistées et examinées par le Pare-feu Cisco IOS. **Le détail** facultatif de mot clé affiche les informations complémentaires au sujet de ces sessions.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'émettre des commandes **debug**, reportez-vous aux Informations importantes sur les commandes de débogage.

- **no ip inspect vigilant-hors fonction** — Messages d'alerte de Pare-feu Cisco IOS d'enables. Si le HTTP refuse sont configurés, vous peut les visualiser de la console.
- **mettez au point l'ip inspect** — Affiche des messages au sujet des événements de Pare-feu Cisco IOS.

C'est exemple de sortie de débogage de la commande de **détail d'ip inspect de débogage** après qu'une tentative de se connecter aux web server sur un 10.66.79.236 et un site non approuvé différent qui a des applet Java (comme défini sur l'ACL).

Log refusé par Javas

```
*Jan 12 21:43:42.919: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2673)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:43.571: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2673).
*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2673) sent 276 bytes
 -- responder (128.138.223.2:80) sent 0 bytes
*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2674)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:43.823: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2672) sent 486 bytes
 -- responder (10.66.79.236:80) sent 974 bytes
*Jan 12 21:43:44.007: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2674).
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2674) sent 276 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2675)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:44.439: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2675).
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2675) sent 233 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2676)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:44.879: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2676).
*Jan 12 21:43:44.879: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2676) sent 233 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.899: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2677)
 -- responder (128.138.223.2:80)
```

Log permis par JAVAS

```
Jan 12 21:44:12.143: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2685)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:12.343: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2686)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:17.343: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2685) sent 626 bytes
 -- responder (10.66.79.236:80) sent 533 bytes
*Jan 12 21:44:17.351: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2686) sent 314 bytes
 -- responder (10.66.79.236:80) sent 126 bytes
*Jan 12 21:44:23.803: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2687)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:27.683: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2691)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.411: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2692)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.451: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2693)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.463: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2694)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.475: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2695)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.487: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2696)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.499: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2697)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.515: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2698)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.527: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2699)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.543: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2700)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.551: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2701)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.075: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2734)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.135: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2735)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.155: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2736)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.159: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2737)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.215: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2739)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.231: %FW-6-SESS_AUDIT_TRAIL_START:
```

```
 Start http session: initiator (192.168.10.2:2740)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.251: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2742)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.395: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2747)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.403: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2748)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.423: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2749)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.091: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2798)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.095: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2799)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.115: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2800)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.119: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2801)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.123: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2802)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.191: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2803)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.219: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2804)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.399: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2805)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.411: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2806)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.423: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2807)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.103: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2843)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.115: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2844)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.127: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2845)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.139: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2846)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.147: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2847)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.159: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2848)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.171: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2849)
```

```
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.183: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2850)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.195: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2851)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.203: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2852)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.107: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2908)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.123: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2909)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.143: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2910)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.163: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2911)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.175: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2912)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.187: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2913)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.199: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2914)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.211: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2915)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.223: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2916)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.235: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2917)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.151: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2982)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.163: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2983)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.175: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2984)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.187: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2985)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.199: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2986)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.211: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2987)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.223: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2988)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.235: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2989)
 -- responder (10.66.79.236:80)
```

```
*Jan 12 21:44:33.251: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2990)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.259: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2991)
 -- responder (10.66.79.236:80)
```

Informations connexes

- Page de support pour le pare-feu d'IOS
- Contrôle d'accès basé sur contexte : Introduction et configuration
- Amélioration de la Sécurité sur des Routeurs de Cisco
- Support et documentation techniques - Cisco Systems