

Usando o Cisco IOS Firewall para permitir Java applets dos locais conhecidos ao negar outro

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Negue Java applets do Internet](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Esta configuração de exemplo demonstra como usar o Firewall de Cisco IOS® para permitir Java applets das websites especificadas, e nega todas as outro. Este tipo de obstrução nega o acesso aos Java applets que não são encaixados em uma arquivada ou em um arquivo compactado. O Cisco IOS Firewall foi introduzido nos Cisco IOS Software Releases 11.3.3.T e 12.0.5.T. Está somente atual em que determinados conjuntos de recursos são comprados.

Você pode ver que conjuntos de características do IOS Cisco apoiam o firewall de IOS com o [Software Advisor](#) (clientes registrados somente).

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 1751 Router
- Cisco IOS Software Release c1700-k9o3sy7-mz.123-8.T.bin

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Negue Java applets do Internet

Siga este procedimento:

1. Crie o Access Control Lists (ACLs).
2. Adicionar **comandos ip inspect http java** à configuração.
3. Aplique **comandos ip inspect e access-list** à interface externa. **Nota:** Neste exemplo, o ACL 3 permite Java applets de um local amigável (10.66.79.236) quando negar implicitamente Java applets de outros locais. Os endereços mostrados na parte externa do roteador não são Internet roteável porque este exemplo foi configurado e testado em um laboratório. **Nota:** **A lista de acesso está exigida já não** para ser aplicada na interface externa se você usa o Cisco IOS Software Release 12.3.4T ou Mais Recente. Isto é documentado na [característica nova do desvio do Firewall ACL](#).

Configurar

Esta seção apresenta-o com a informação que você pode se usar a fim configurar as características este documento descreve.

Nota: A fim encontrar a informação adicional nos comandos que este documento se usa, refere-se a [ferramenta de consulta de comandos \(clientes registrados somente\)](#).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza esta configuração:

Configuração do roteador
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

```

Verificar

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show ip inspect sessions [detail]** — Sessões existentes das mostras atualmente seguidas e inspecionadas pelo Cisco IOS Firewall. O **detalhe das** palavras-chave opcionais mostra a informação adicional sobre estas sessões.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: [Antes de emitir comandos de depuração, consulte Informações Importantes sobre Comandos de Depuração.](#)

- **nenhum IP inspeciona alerta-fora** — Permite mensagens de alerta do Cisco IOS Firewall. Se o HTTP nega é configurado, você pode os ver do console.
- **debug ip inspect** — Mostra mensagens sobre eventos do Cisco IOS Firewall.

Este é exemplo de debug do **comando debug ip inspect detail** depois que uma tentativa de conectar aos servidores de Web em 10.66.79.236 e em um outro local não confiável que tenha Java applets (como definido no ACL).

Log negado 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 permitido 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)

Informações Relacionadas

- [Página de suporte de firewall do IOS](#)
- [Controle de acesso com base no contexto: Introdução e configuração](#)
- [Melhorando a Segurança em Cisco Routers](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)