

# Use NBAR e ACLs para bloquear o worm "Code Red"

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Como bloquear o worm "Código Vermelho"](#)

[Plataformas suportadas](#)

[Detecte a tentativa de infecção nos registros da Web do IIS](#)

[Marcar hack recebido como "Código Vermelho" utilizando recurso de marcação com base em classe de IOS](#)

[Método A: Use um ACL](#)

[Método B: Use o Policy-Based Routing \(PBR\)](#)

[Método C: Usar vigilância baseada em classe](#)

[Restrições NBAR](#)

[Problemas conhecidos](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece um método para bloquear o worm "Code Red" em pontos de entrada de rede através do NBAR (Network-Based Application Recognition) e das ACLs (Access Control Lists, listas de controle de acesso) no software Cisco IOS® em roteadores Cisco. Essa solução deve ser usada em conjunto com as correções recomendadas para os servidores IIS da Microsoft.

**Observação:** este método não funciona nos Cisco 1600 Series Routers.

**Observação:** alguns tráfegos P2P não podem ser totalmente bloqueados devido à natureza de seu protocolo P2P. Esses protocolos P2P mudam dinamicamente suas assinaturas para ignorar qualquer mecanismo de DPI que tente bloquear completamente seu tráfego. Portanto, é recomendável limitar a largura de banda em vez de bloqueá-la completamente. Acelere a largura de banda desse tráfego. Oferecer muito menos largura de banda; entretanto, deixe a conexão passar.

## [Prerequisites](#)

## [Requirements](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Políticas de serviço de Qualidade de Serviço (QoS - Quality of Service) usando os comandos da [interface de linha de comando de QoS modular](#) (CLI - Command Line Interface).
- NBAR
- ACLs
- Roteamento baseado em políticas

## Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. A configuração neste documento foi testada no Cisco 3640 que executa o Cisco IOS versão 12.2(24a)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## Como bloquear o worm "Código Vermelho"

A primeira coisa que você deve fazer para combater o "Código Vermelho" é aplicar o patch disponível da Microsoft (veja os links na seção [Método A: Use uma ACL](#) abaixo). Isso protege sistemas vulneráveis e remove o worm de um sistema infectado. No entanto, a aplicação do patch em seus servidores apenas impede que o worm infecte os servidores, ele não impede que as solicitações HTTP GET atinjam os servidores. Ainda há o potencial para o servidor ser bombardeado com uma enxurrada de tentativas de infecção.

A solução detalhada neste aviso foi projetada para funcionar em conjunto com o patch da Microsoft para bloquear as solicitações HTTP GET "Code Red" em um ponto de entrada de rede.

Essa solução tenta bloquear a infecção, mas não soluciona problemas causados pelo acúmulo de grandes números de entradas de cache, adjacências e entradas NAT/PAT, já que a única maneira de analisar o conteúdo da solicitação HTTP GET é seguindo o estabelecimento de uma conexão TCP. O procedimento a seguir não ajudará a proteger contra uma varredura da rede. No entanto, protegerá um site contra infestação de uma rede externa ou reduzirá o número de tentativas de infecção que uma máquina deve atender. Em combinação com a filtragem de entrada, a filtragem de saída evita que os clientes infectados espalhem o worm "Code Red" para a Internet global.

## Plataformas suportadas

A solução descrita neste documento requer o recurso de marcação baseado em classe no software Cisco IOS. Especificamente, a capacidade de corresponder em uma parte de um URL de HTTP usa o recurso de classificação de subporta HTTP dentro do NBAR. As plataformas suportadas e os requisitos mínimos do Cisco IOS Software estão resumidos a seguir:



Consulte o [Symantec Advisory](#) para obter mais detalhes.

Às 18:24h EDT, 6 de agosto de 2001, gravamos um novo volume. Desde então, aprendemos que esta é a pegada deixada para trás pelo [scanner de vulnerabilidade do eEye](#).

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

A técnica para bloquear o "Código Vermelho" fornecida neste aviso também pode bloquear essas tentativas de digitalização simplesmente apertando a definição do mapa de classes como mostrado na próxima seção.

## [Marcar hack recebido como "Código Vermelho" utilizando recurso de marcação com base em classe de IOS](#)

Para bloquear o worm "Code Red", use um dos três métodos descritos abaixo. Todos os três métodos classificam o tráfego mal-intencionado usando o recurso Cisco IOS MQC. Em seguida, esse tráfego é descartado conforme descrito abaixo.

### [Método A: Use um ACL](#)

Esse método usa uma ACL na interface de saída para descartar os pacotes marcados como "Code Red". Vamos usar o diagrama de rede a seguir para ilustrar as etapas neste método:



Aqui estão as etapas para configurar este método:

1. Classifique hacks "Code Red" de entrada com o recurso de marcação baseado em classe no software Cisco IOS, como mostrado abaixo:

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "**default.ida*"
Router(config-cmap)#match protocol http url "**cmd.exe*"
Router(config-cmap)#match protocol http url "**root.exe"
```

O mapa de classe acima procura dentro de URLs HTTP e corresponde a qualquer uma das strings especificadas. Observe que incluímos outros nomes de arquivos além do padrão.ida de "Código Vermelho". Você pode usar esta técnica para bloquear tentativas de hackers semelhantes, como o vírus Sadhead, que é explicado nos seguintes

documentos:<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp><http://www.sophos.com/virusinfo/analyses/unixsadmind.html>

2. Crie uma política e use o comando **set** para marcar hacks "Code Red" de entrada com um mapa de política. Este documento usa um valor de DSCP de 1 (em decimal), pois é improvável que qualquer outro tráfego de rede esteja carregando esse valor. Aqui, marcamos

hacks "Code Red" de entrada com um mapa de política chamado "mark-inbound-http-hacks".

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. Aplique a política como uma política de entrada na interface de entrada para marcar os pacotes "Code Red" que chegam.

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. Configure uma ACL que corresponda ao valor de DSCP de 1, conforme definido pela política de serviço.

```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

**Observação:** os Cisco IOS Software Releases 12.2(11) e 12.2(11)T apresentam suporte para a palavra-chave **log** na ACL ao definir em mapas de classe para uso com NBAR (CSCdv48172). Se estiver usando uma versão anterior, não use a palavra-chave **log** na ACL. Isso força todos os pacotes a serem comutados por processo em vez de comutados por CEF, e o NBAR não funcionará, pois requer CEF.

5. Aplique a saída da ACL na interface de saída que se conecta aos servidores Web de destino.

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. Verifique se sua solução funciona conforme esperado. Execute o comando **show access-list** e certifique-se de que o valor "match" da instrução deny está aumentando.

```
Router#show access-list 105
Extended IP access list 105
  deny ip any any dscp 1 log (2406 matches)
  permit ip any any (731764 matches)
```

Na etapa de configuração, você também pode desabilitar o envio de mensagens IP inalcançáveis com o comando **no ip unreachable** interface-level para evitar que o roteador desperdice recursos excessivos. Esse método não é recomendado se você puder direcionar o tráfego DSCP=1 para Nulo 0, conforme descrito na seção Método B.

## [Método B: Use o Policy-Based Routing \(PBR\)](#)

Esse método usa o roteamento baseado em políticas para bloquear pacotes marcados como "Code Red". Você não precisa aplicar os comandos neste método se os métodos A ou C já estiverem configurados.

Aqui estão as etapas para implementar este método:



1. Classifique o tráfego e marque-o. Use os comandos **class-map** e **policy-map** mostrados no método A.
2. Use o comando **service-policy** para aplicar a política como uma política de entrada na interface de entrada para marcar pacotes "Code Red" de chegada. Veja o método A.
3. Crie uma ACL IP estendida que corresponda aos pacotes marcados como "Code Red".  
Router(config)#**access-list 106 permit ip any any dscp 1**

4. Use o comando **route-map** para criar uma política de roteamento.

```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```

5. Aplique o mapa de rota à interface de entrada.

```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. Verifique se sua solução funciona conforme esperado com o comando **show access-list**. Se estiver usando ACLs de saída e tiver ativado o registro da ACL, você também poderá usar os comandos **show log**, como mostrado abaixo:

```
Router#show access-list 106
Extended IP access list 106
  permit ip any any dscp 1 (1506 matches)
```

```
Router#show log
Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
  list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
  list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
```

Podemos tomar a decisão de descarte na interface de ingresso do roteador, em vez de precisar de uma ACL de saída em cada interface de saída. Novamente, recomendamos desativar o envio de mensagens IP inalcançáveis com o comando **no ip unreachable**.

## Método C: Usar vigilância baseada em classe

Geralmente, esse método é o mais escalável, pois não depende de PBR ou ACLs de saída.

1. Classifique o tráfego usando os comandos **class-map** mostrados no método A.
2. Crie uma política usando o comando **policy-map** e use o comando **police** para especificar uma ação de descarte para esse tráfego.

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
conform-action drop exceed-action drop violate-action drop
```

3. Use o comando **service-policy** para aplicar a política como uma política de entrada na interface de entrada para descartar os pacotes "Code Red".

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. Verifique se sua solução funciona conforme esperado com o comando **show policy-map interface**. Certifique-se de ver valores incrementais para a classe e os critérios de correspondência individuais.

```
Router#show policy-map interface serial 0/0

Serial0/0
```

```
Service-policy input: drop-inbound-http-hacks
```

```
Class-map: http-hacks (match-any)
  5 packets, 300 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: protocol http url "*default.ida*"
  5 packets, 300 bytes
  5 minute rate 0 bps
Match: protocol http url "*cmd.exe*"
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: protocol http url "*root.exe*"
  0 packets, 0 bytes
  5 minute rate 0 bps
police:
  1000000 bps, 31250 limit, 31250 extended limit
  conformed 5 packets, 300 bytes; action: drop
  exceeded 0 packets, 0 bytes; action: drop
  violated 0 packets, 0 bytes; action: drop
  conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
  5 packets, 300 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

## Restrições NBAR

Ao usar o NBAR com os métodos neste documento, observe que os seguintes recursos não são suportados pelo NBAR:

- Mais de 24 URLs, HOSTs ou correspondências de tipo MIME simultâneos
- Correspondência além dos primeiros 400 bytes em um URL
- Tráfego não IP
- Multicast e outros modos de comutação não CEF
- Pacotes fragmentados
- Solicitações HTTP persistentes implantadas
- URL/HOST/MIME/ classificação com HTTP seguro
- Fluxos assimétricos com protocolos stateful
- Pacotes originados ou destinados ao roteador que executa o NBAR

Não é possível configurar o NBAR nas seguintes interfaces lógicas:

- Fast EtherChannel
- Interfaces que usam tunelamento ou criptografia
- VLANs
- Interfaces de discador
- Multilink PPP

**Note:** O NBAR é configurável em VLANs a partir do Cisco IOS versão 12.1(13)E, mas é suportado somente no caminho de switching do software.

Como o NBAR não pode ser usado para classificar o tráfego de saída em um link de WAN onde o tunelamento ou a criptografia é usado, aplique-o em vez disso a outras interfaces no roteador, como a interface de LAN, para executar a classificação de entrada antes que o tráfego seja

comutado para o link de WAN para saída.

Para obter mais informações sobre NBAR, consulte os links nas [Informações Relacionadas](#)