Firewall Clássico/IPS do Cisco IOS: Configurando o Controle de Acesso Baseado em Contexto (CBAC - Context-Based Access Control) para Proteção contra Negação de Serviço

Contents

Introduction

Este documento descreve o procedimento de ajuste para parâmetros de negação de serviço (DoS) no Cisco IOS® Classic Firewall com CBAC.

O CBAC oferece funcionalidade avançada de filtragem de tráfego e pode ser usado como parte integrante do firewall de rede.

DoS geralmente se refere à atividade da rede que sobrecarrega intencionalmente ou não intencionalmente os recursos da rede, como largura de banda de link de WAN, tabelas de conexão de firewall, memória do host final, CPU ou recursos de serviço. Na pior das hipóteses, a atividade do DoS sobrecarrega o recurso vulnerável (ou direcionado) a ponto de o recurso se tornar indisponível e proíbe a conectividade da WAN ou o acesso ao serviço para usuários legítimos.

O Cisco IOS Firewall pode contribuir para a mitigação da atividade de DoS se mantiver contadores do número de conexões TCP "meio abertas", bem como a taxa total de conexão por meio do firewall e do software de prevenção de invasão no Firewall Clássico (**ip inspect**) e no Firewall de Política Baseado em Zona.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

Conexões meio abertas são conexões TCP que não completaram o handshake triplo SYN-SYN/ACK-ACK que é sempre usado por pares TCP para negociar os parâmetros de sua conexão mútua. Um grande número de conexões meio abertas pode ser indicativo de atividades mal-intencionadas, como ataques DoS ou DDoS (Distributed-Denial-of-Service, negação de serviço distribuído). Um exemplo de um tipo de ataque de DoS é conduzido por software mal-intencionado e intencionalmente desenvolvido, como worms ou vírus que infectam vários hosts na Internet e tentam sobrecarregar servidores de Internet específicos com ataques SYN, onde grandes números de conexões SYN são enviadas a um servidor por vários hosts na Internet ou na rede privada de uma organização. Os ataques SYN representam um risco para os servidores de Internet, uma vez que as tabelas de conexão dos servidores podem ser carregadas com tentativas de conexão SYN "falsas" que chegam mais rápido do que o servidor pode lidar com as novas conexões. Esse é um tipo de ataque de DoS porque o grande número de conexões na lista de conexões TCP do servidor da vítima impede o acesso legítimo do usuário aos servidores da Internet da vítima.

O Cisco IOS Firewall também considera sessões UDP (User Datagram Protocol, protocolo de datagrama do usuário) com tráfego em apenas uma direção como "semiaberto", pois muitos aplicativos que usam UDP para transporte reconhecem a recepção de dados. Sessões UDP sem tráfego de retorno são provavelmente indicativas de atividade do DoS ou tentativas de conexão entre dois hosts, onde um dos hosts não respondeu. Muitos tipos de tráfego UDP, como mensagens de log, tráfego de gerenciamento de rede SNMP, transmissão de mídia de voz e vídeo e tráfego de sinalização, usam apenas o tráfego em uma direção para transportar seu tráfego. Muitos desses tipos de tráfego aplicam inteligência específica de aplicativos para evitar que padrões de tráfego unidirecional afetem adversamente o comportamento de firewall e de DoS de IPS.

Antes do Cisco IOS Software Release 12.4(11)T e 12.4(10), a Inspeção de Pacotes Stateful do Cisco IOS fornecia proteção contra ataques de DoS como padrão quando uma regra de inspeção era aplicada. O Cisco IOS Software Release 12.4(11)T e 12.4(10) modificaram as configurações

padrão do DoS de modo que a proteção do DoS não seja aplicada automaticamente, mas os contadores da atividade de conexão ainda estão ativos. Quando a proteção DoS está ativa, isto é, quando os valores padrão são usados em versões de software mais antigas ou os valores foram ajustados para o intervalo que afeta o tráfego, a proteção DoS é ativada na interface em que a inspeção é aplicada, na direção em que o firewall é aplicado, para que os protocolos de configuração de política de firewall sejam inspecionados. A proteção DoS só é ativada no tráfego de rede se o tráfego entrar ou sair de uma interface com inspeção aplicada na mesma direção do tráfego inicial (pacote SYN ou primeiro pacote UDP) para uma conexão TCP ou sessão UDP.

A inspeção do Cisco IOS Firewall fornece vários valores ajustáveis para proteção contra ataques de DoS. As versões do Cisco IOS Software anteriores a 12.4(11)T e 12.4(10) têm valores de DoS padrão que podem interferir na operação de rede apropriada se não estiverem configuradas para o nível apropriado de atividade de rede em redes onde as taxas de conexão excedem os padrões. Esses parâmetros permitem configurar os pontos nos quais a proteção DoS do roteador de firewall começa a entrar em vigor. Quando os contadores DoS do roteador excederem os valores padrão ou configurados, o roteador redefinirá uma antiga conexão semiaberta para cada nova conexão que exceder os valores máximos incompletos configurados ou altos de um minuto até que o número de sessões semiabertas caia abaixo dos valores mínimos máximos incompletos. O roteador envia uma mensagem de syslog se o registro estiver ativado e se um sistema de prevenção de intrusão (IPS) estiver configurado no roteador, o roteador de firewall envia uma mensagem de assinatura do DoS através do Security Device Event Exchange (SDEE). Se os parâmetros do DoS não forem ajustados ao comportamento normal da rede, a atividade normal da rede pode acionar o mecanismo de proteção do DoS, o que causa falhas no aplicativo, mau desempenho da rede e alta utilização da CPU no roteador do Cisco IOS Firewall.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Ajuste de negação de serviço para o Firewall Clássico do Software Cisco IOS (inspeção de IP) e o Sistema de prevenção de intrusão

O Cisco IOS Firewall clássico mantém um conjunto global de contadores DoS para o roteador e todas as sessões de firewall para todas as políticas de firewall em todas as interfaces são aplicadas ao conjunto global de contadores de firewall.

O Cisco IOS Classic Firewall Inspection fornece proteção contra ataques de DoS por padrão quando um Classic Firewall é aplicado. A proteção DoS é ativada em todas as interfaces em que a inspeção é aplicada, na direção em que o firewall é aplicado, para cada serviço ou protocolo que a política de firewall está configurada para inspecionar. O Firewall Clássico fornece vários valores ajustáveis para proteção contra ataques de DoS. As configurações padrão legadas (de imagens de software anteriores à versão 12.4(11)T) mostradas na Tabela 1 podem interferir na operação de rede apropriada se não estiverem configuradas para o nível apropriado de atividade de rede em redes onde as taxas de conexão excedem os padrões. As configurações do DoS podem ser visualizadas com o comando exec **show ip inspect config**, e as configurações são incluídas com a saída de **sh ip inspect all**.

O CBAC usa intervalos e limites para determinar por quanto tempo gerenciar informações de estado de uma sessão, bem como para determinar quando as sessões que não estão totalmente estabelecidas devem ser descartadas. Esses intervalos e limites aplicam-se globalmente a todas as sessões.

Tabela 1 Limites de proteção de DoS padrão do firewall clássico		
Valor da proteção DoS	Anterior a 12.4(11)T/12.4(10)	12.4(11)T/12.4(10) e posterior
valor máximo incompleto	500	Ilimitado
valor mínimo incompleto	400	Ilimitado
valor alto de um minuto	500	Ilimitado
valor baixo de um minuto	400	Ilimitado
valor máximo de host tcp incompleto	50	Ilimitado

Os roteadores configurados para aplicar o Cisco IOS VRF-Aware Firewall mantêm um conjunto de contadores para cada VRF.

O contador para "ip inspect one-minute high" (inspeção de ip com um minuto de altura) e "ip inspect one-minute low" (inspeção de ip com um minuto de profundidade) mantém uma soma de todas as tentativas de conexão TCP, UDP e ICMP (Internet Control Message Protocol) no minuto anterior da operação do roteador, independentemente de as conexões terem sido bem-sucedidas ou não. Uma taxa de conexão crescente pode ser indicativa de uma infecção de worm em uma rede privada ou de uma tentativa de ataque de DoS contra um servidor.

Embora não seja possível "desativar" a proteção DoS do firewall, você pode ajustar a proteção DoS para que ela não entre em vigor, a menos que um número muito grande de conexões semiabertas esteja presente na tabela de sessões do seu roteador de firewall.

Proteção de firewall DoS

Siga este procedimento para ajustar a proteção DoS do firewall à atividade da rede:

1. Certifique-se de que a sua rede não está infectada com vírus ou worms que podem levar a valores de conexão semiabertos ou taxas de conexão tentadas erroneamente grandes. Se a sua rede não estiver "limpa", não há como ajustar corretamente a proteção DoS do firewall. Você deve observar a atividade da sua rede dentro de um período de atividade típica. Se você ajustar as configurações de proteção do DoS da sua rede em um período de atividade de rede baixa ou inativa, os níveis normais de atividade provavelmente excederão as configurações de proteção do DoS.
2. Defina os valores altos máximos incompletos como valores muito altos:

```
ip inspect max-incomplete high 20000000
```

```
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

Isso evita que o roteador forneça proteção DoS enquanto você observa os padrões de conexão de sua rede. Se você quiser deixar a proteção DoS desabilitada, pare este procedimento agora.**Observação:** se o roteador executar o Cisco IOS Software Release 12.4(11)T ou posterior, ou 12.4(10) ou posterior, você não precisa aumentar os valores padrão de Proteção DoS; por padrão, eles já estão definidos com seus limites máximos.**Observação:** se quiser habilitar a prevenção de negação de serviço específica do host TCP mais agressiva que inclui o bloqueio da iniciação de conexão a um host, você deve definir o tempo de bloqueio especificado no comando **ip inspect tcp max-complete host**

3. Limpe as estatísticas do Cisco IOS Firewall com este comando:

```
show ip inspect statistics reset
```

4. Deixe o roteador configurado nesse estado por algum tempo, talvez de 24 a 48 horas, para que você possa observar o padrão de rede em pelo menos um dia inteiro do ciclo de atividade de rede típico.**Observação:** embora os valores sejam ajustados para níveis muito altos, sua rede não se beneficia da proteção do Cisco IOS Firewall ou IPS DoS.
5. Após o período de observação, verifique os contadores DoS com este comando:

```
show ip inspect statistics
```

Os parâmetros que você deve observar para ajustar sua proteção DoS estão destacados em **negrito**:

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. Configure **ip inspect max-complete high** para um valor 25% mais alto que o valor de meia-abertura da contagem de sessões do maxever indicado para o seu roteador. Um multiplicador 1,25 oferece 25% de espaço acima do comportamento observado, por exemplo:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

```
56 * 1.25 = 70
```

Configurar:

```
router(config)
   #ip inspect max-incomplete high 70
```

Observação: este documento descreve o uso de um multiplicador 1,25 vezes a atividade típica de sua rede para definir limites para envolver a proteção DoS. Se você observar sua rede dentro dos picos de atividade típicos da rede, isso deve fornecer espaço suficiente para evitar a ativação da proteção DoS do roteador em todas as circunstâncias, exceto atípicas. Se a sua rede periodicamente vir grandes surtos de atividade de rede legítima que excedem esse valor, o roteador aciona os recursos de proteção do DoS, o que pode causar um impacto negativo em parte do tráfego de rede. Você deve monitorar os registros do roteador em busca de detecções da atividade DoS e ajustar o **ip inspect max-complete high** e/ou **ip inspect one-minute high** limit para evitar o acionamento de DoS, depois de determinar que os limites foram encontrados como resultado de uma atividade de rede legítima. Você pode reconhecer o aplicativo de proteção DoS pela presença de mensagens de log como esta:

7. Configure **ip inspect max-complete low** para o valor exibido pelo seu roteador para o valor de meia-abertura da contagem de sessões do maxever, por exemplo:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

Configurar:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. O contador para **ip inspect one-minute high** and **one-minute low** mantém uma soma de todas as tentativas de conexão TCP, UDP e ICMP (Internet Control Message Protocol) no minuto anterior da operação do roteador, independentemente de as conexões terem sido bem-sucedidas ou não. Uma taxa de conexão crescente pode ser indicativa de uma infecção de worm em uma rede privada ou de uma tentativa de ataque de DoS contra um servidor. Uma estatística de inspeção adicional foi adicionada à saída **show ip inspect statistics** em 12.4(11)T e 12.4(10) para revelar a marca d'água alta para a taxa de criação da sessão. Se você executar um Cisco IOS Software Release antes de 12.4(11)T ou 12.4(10), as estatísticas de inspeção não conterão esta linha:

```
Maxever session creation rate [value]
```

As versões do software Cisco IOS anteriores a 12.4(11)T e 12.4(10) não mantêm um valor para a taxa de conexão máxima de um minuto de inspeção, portanto você deve calcular o valor que aplica com base nos valores observados de "contagem máxima de sessões". Observações de várias redes que usam a inspeção stateful do Cisco IOS Firewall versão 12.4(11)T na produção mostraram que as taxas de criação de sessão do Maxever tendem a exceder a soma dos três valores (estabelecido, meio aberto e terminando) em "contagem máxima de sessões" em aproximadamente dez por cento. Para calcular o valor baixo de um minuto de inspeção de ip, multiplique o valor "estabelecido" indicado por 1.1, por exemplo:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

Configurar:

```
ip inspect one-minute low 328
```

Se o roteador executar o Cisco IOS Software Release 12.4(11)T ou posterior, ou 12.4(10) ou posterior, você pode simplesmente aplicar o valor mostrado na estatística de inspeção "Taxa de criação de sessão Maxever":

```
Maxever session creation rate 330
```

Configurar:

```
ip inspect one-minute low 330
```

9. Calcule e configure o **ip inspect com um minuto de altura**. O valor alto de um minuto de inspeção de ip deve ser 25% maior que o valor baixo de um minuto calculado, por exemplo:

   ```
   ip inspect one-minute low (330) * 1.25 = 413
   ```

   Configurar:

   ```
   ip inspect one-minute high 413
   ```

   Observação: este documento descreve o uso de um multiplicador 1,25 vezes a atividade típica de sua rede para definir limites para envolver a proteção DoS. Se você observar sua rede dentro dos picos de atividade típicos da rede, isso deve fornecer espaço suficiente para evitar a ativação da proteção DoS do roteador em todas as circunstâncias, exceto atípicas. Se a sua rede periodicamente vir grandes surtos de atividade de rede legítima que excedem esse valor, o roteador aciona os recursos de proteção do DoS, o que pode causar um impacto negativo em parte do tráfego de rede. Você deve monitorar os registros do roteador em busca de detecções da atividade DoS e ajustar o **ip inspect max-complete high** e/ou **ip inspect one-minute high** limit para evitar o acionamento de DoS, depois de determinar que os limites foram encontrados como resultado de uma atividade de rede legítima. Você pode reconhecer o aplicativo de proteção DoS pela presença de mensagens de log como esta:
10. Você precisa definir um valor para o **host tcp max-incompleto do ip inspect** de acordo com seu conhecimento da capacidade dos servidores. Este documento não pode fornecer diretrizes para a configuração de proteção DoS por host, pois esse valor varia amplamente com base no desempenho de hardware e software do host final. Se você não tiver certeza sobre os limites apropriados para configurar a proteção DoS, você efetivamente terá duas opções com as quais definir os limites do DoS:A opção preferível é configurar a proteção DoS por host baseada em roteador para um valor alto (menor ou igual ao valor máximo de 4.294.967.295) e aplicar a proteção específica do host oferecida pelo sistema operacional de cada host ou um Sistema de Proteção contra Intrusão baseado em host externo, como o Cisco Security Agent (CSA).Examine os logs de atividade e desempenho nos hosts da rede e determine a taxa de conexão sustentável máxima. Como o Firewall Clássico oferece apenas um contador global, você deve aplicar o valor máximo que determinar depois de verificar todos os hosts da rede quanto às taxas de conexão máximas. Ainda é aconselhável usar limites de atividade específicos do SO e um IPS baseado em host, como o CSA.**Observação:** o Cisco IOS Firewall oferece proteção limitada contra ataques direcionados a vulnerabilidades específicas de sistemas operacionais e aplicativos. A proteção DoS do Cisco IOS Firewall não oferece nenhuma garantia de proteção contra comprometimento em serviços de host final expostos a ambientes potencialmente hostis.
11. Monitore a atividade de proteção do DoS na sua rede. Idealmente, você deve usar um Servidor syslog ou, idealmente, uma Cisco Monitoring and Reporting Stations (MARS) para registrar ocorrências de detecção de ataque de DoS. Se a detecção ocorrer com muita frequência, você precisará monitorar e ajustar os parâmetros de proteção do DoS.Para obter mais informações sobre ataques TCP SYN DoS, consulte Definindo estratégias para proteger contra ataques TCP SYN de negação de serviço.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados

comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems