Cisco IOS Firewall/IPS clássico: Configurando o Context-Based Access Control (CBAC) para a proteção da recusa de serviço

Índice

Introdução

Este documento descreve o procedimento de ajustamento para a recusa de parâmetros do serviço (DoS) no Firewall clássico do ® do Cisco IOS com CBAC.

O CBAC fornece funcionalidade avançada do filtragem de tráfego e pode ser usado como uma parte integral de seu firewall de rede.

O DoS refere geralmente a atividade de rede que oprime intencionalmente ou involuntariamente recursos de rede tais como a largura de banda de enlace MACILENTO, as tabelas de conexão do Firewall, a memória do host final, o CPU, ou as capacidades de serviço. Em um cenário de caso pior, a atividade DoS oprime (ou visado) o recurso vulnerável ao ponto que o recurso se torna não disponível, e proibe o acesso da conectividade de WAN ou do serviço aos usuários legítimos.

O Cisco IOS Firewall pode contribuir à mitigação da atividade DoS se mantém contadores do número de conexões de TCP “entreabertas”, assim como à taxa de conexão total através do software do Firewall e da prevenção de intrusão no Firewall clássico (o **IP inspeciona**) e no Firewall Zona-baseado da política.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

As conexões meio aberta são as conexões de TCP que não terminaram o aperto de mão tripartido SYN-SYN/ACK-ACK que é usado sempre por pares TCP para negociar os parâmetros de sua conexão mútua. Um grande número conexões meio aberta podem ser indicativas da atividade mal-intencionada, tal como ataques DoS ou de ataque de negação de serviço distribuído (DDoS). Um exemplo de um tipo de ataque DoS é conduzido pelo software malicioso, intencional-em desenvolvimento, tal como worms ou pelos vírus que contaminam host múltiplos no Internet e tentam oprimir servidores de Internet específicos com os ataques SYN, onde um grande número conexões SYN são enviadas a um server por host múltiplos no Internet ou dentro da rede privada de uma organização. Os ataques SYN representam um perigo aos servidores de Internet desde que as tabelas de conexão dos server podem ser carregadas com as tentativas de conexão “falsas” SYN que chegam mais rapidamente do que o server podem tratar as novas conexões. Este é um tipo de ataque DoS porque o número grande de conexões na lista da conexão de TCP do server da vítima impede o acesso de usuário legítimo aos servidores de Internet da vítima.

O Cisco IOS Firewall igualmente considera sessões do User Datagram Protocol (UDP) com tráfego em somente um sentido como “entreaberto” porque muitos aplicativos que usam o UDP para o transporte reconhecem a recepção dos dados. As sessões de UDP sem tráfego de retorno são provavelmente indicativas da atividade ou das tentativas DoS conectar entre dois anfitriões, onde um dos anfitriões se tornou sem resposta. Muitos tipos de UDP traficam, como mensagens de registro, tráfego de gerenciamento de rede SNMP, fluindo media da Voz e do vídeo, e tráfego de sinalização, simplesmente tráfego do uso em um sentido para levar seu tráfego. Muitos destes tipos de tráfego aplicam a inteligência característica da aplicação impedir que os testes padrões de tráfego unidirecional afetem adversamente o Firewall e o IPS do comportamento DoS.

Antes do Cisco IOS Software Release 12.4(11)T e de 12.4(10), a inspeção de pacote de informação do stateful do Cisco IOS forneceu a proteção dos ataques DoS como um padrão quando uma regra da inspeção era aplicada. O Cisco IOS Software Release 12.4(11)T e 12.4(10) alteraram os ajustes DoS do padrão de modo que a proteção de DOS não fosse aplicada automaticamente, mas os contadores da atividade da conexão são ainda ativos. Quando a proteção de DOS é ativa, isto é, quando os valores padrão estão usados em uns software release mais velhos, ou nos valores estiveram ajustados à escala que afetam o tráfego, a proteção de DOS é permitida na relação onde a inspeção é aplicada, no sentido em que o Firewall é aplicado,

para que os protocolos de configuração da política de firewall inspecionem. A proteção de DOS está permitida somente no tráfego de rede se o tráfego incorpora ou deixa uma relação com a inspeção aplicada no mesmo sentido do tráfego inicial (pacote SYN ou primeiro pacote de UDP) para uma conexão de TCP ou uma sessão de UDP.

A inspeção do Cisco IOS Firewall fornece diversos valores ajustáveis para proteger contra ataques DoS. Os Cisco IOS Software Release antes de 12.4(11)T e de 12.4(10) têm os valores DoS do padrão que podem interferir com a operação da rede adequada se não são configurados para o nível apropriado da atividade de rede nas redes onde as taxas de conexão excedem os padrões. Estes parâmetros permitem que você configure os pontos em que a proteção de DOS de seu roteador de firewall começa a tomar o efeito. Quando os contadores DoS de seu roteador excedem o padrão ou os valores configurados, o roteador restaura uma conexão meio aberta velha para cada nova conexão que excede os altos valores configurados máximas incompleta ou do minuto até o número de gotas entreabertas das sessões abaixo dos valores baixos máximas incompleta. O roteador envia um mensagem do syslog se registrar está permitido, e se um Intrusion Prevention System (IPS) está configurado no roteador, o roteador de firewall envia um mensagem de assinatura DoS com a troca do evento do dispositivo de segurança (SDEE). Se os parâmetros DoS não são ajustados ao comportamento normal de sua rede, a atividade da rede normal pode provocar o mecanismo da proteção de DOS, que causa falhas de aplicativo, o desempenho da rede deficiente, e a utilização elevada 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.

Recusa de serviço que ajusta para o Firewall do Cisco IOS Software (o IP inspeciona) e o sistema clássicos da prevenção de intrusão

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

A inspeção clássica do Firewall do Cisco IOS fornece a proteção do ataque DoS à revelia quando um Firewall clássico é aplicado. A proteção de DOS é permitida em todas as relações onde a inspeção é aplicada, no sentido em que o Firewall é aplicado, para cada serviço ou protocolo que a política de firewall é configurada para inspecionar. O Firewall clássico fornece diversos valores ajustáveis para proteger contra ataques DoS. As configurações padrão do legado (das imagens do software antes da liberação 12.4(11)T) mostradas na tabela 1 podem interferir com a operação da rede adequada se não são configuradas para o nível apropriado da atividade de rede nas redes onde as taxas de conexão excedem os padrões. Os ajustes DoS podem ser vistos com o exec command show **IP inspecionam a configuração**, e os ajustes são incluídos com a saída do **IP sh inspecionam tudo**.

O CBAC usa intervalos e pontos iniciais para determinar quanto tempo controlar a informação de estado para uma sessão, assim como determinar quando deixar cair as sessões que não se tornam estabelecidas inteiramente. Estes intervalos e pontos iniciais aplicam-se globalmente a todas as sessões.

Limites clássicos da proteção de DOS do padrão do Firewall da tabela 1		
Valor da proteção de DOS	**Antes de 12.4(11)T/12.4(10)**	**12.4(11)T/12.4(10) e mais atrasado**
alto valor máxima incompleta	500	Ilimitado
valor baixo máxima incompleta	400	Ilimitado
alto valor do minuto	500	Ilimitado
valor baixo do minuto	400	Ilimitado
valor máxima incompleta do host tcp	50	Ilimitado

O Roteadores configurado para aplicar o Firewall VRF-ciente do Cisco IOS mantém um grupo de contadores para cada VRF.

O contador para o “IP inspeciona a elevação do minuto” e o “IP inspeciona o ponto baixo do minuto” mantém uma soma de todo o TCP, UDP, e tentativas de conexão do Internet Control Message Protocol (ICMP) dentro do minuto prévio do funcionamento do roteador, se as conexões foram bem sucedidas ou não. Uma taxa de conexão de aumentação pode ser indicativa de uma infecção do worm em uma rede privada ou de um ataque tentado DoS contra um server.

Quando você não puder “desabilitar” a proteção de DOS de seu Firewall, você pode ajustar a proteção de DOS de modo que não tome o efeito a menos que muito um número grande de conexões meio aberta estar presente na tabela da sessão de seu roteador de firewall.

Proteção de firewall DoS

Siga este procedimento para ajustar a proteção de DOS de seu Firewall à atividade de sua rede:

1. Seja certo que sua rede não está contaminada com vírus ou worms que podem conduzir aos valores erroneamente grandes da conexão meio aberta ou às taxas de conexão tentadas. Se sua rede não está “limpa,” não há nenhuma maneira de ajustar corretamente a proteção de DOS de seu Firewall. Você deve observar a atividade de sua rede dentro de um período de atividade típica. Se você ajusta os ajustes da proteção de DOS de sua rede dentro de um período de atividade de rede do ponto baixo ou da quietude, os níveis de atividade normal excedem provavelmente os ajustes da proteção de DOS.
2. Ajuste os altos valores máximas incompleta muito aos altos valores:
   `ip inspect max-incomplete high 20000000 ip inspect one-minute high 100000000 ip inspect tcp max-incomplete host 100000 block-time 0` Isto impede que o roteador forneça a proteção de DOS quando você observar os testes padrões da conexão de sua rede. Se você deseja deixar a proteção de DOS desabilitada, pare este procedimento agora.**Nota:** Se seu roteador executa o Cisco IOS Software Release 12.4(11)T ou Mais Recente, ou o 12.4(10) ou mais atrasado, você não precisa de levantar os valores da proteção de DOS do padrão; são

ajustados já a seus limite máximos à revelia.**Nota:** Se você quer permitir a prevenção host-específica mais agressiva da recusa de serviço TCP que inclui a obstrução da iniciação de conexão a um host, você deve ajustar o bloco-tempo especificado no **comando ip inspect tcp max-incomplete host**

3. Cancele as estatísticas do Cisco IOS Firewall com este comando:
   show ip inspect statistics reset
4. Deixe o roteador configurado neste estado por algum tempo, talvez enquanto 24 a 48 horas, assim que você podem observar o teste padrão da rede sobre pelo menos um dia inteiro do ciclo de atividade da rede típica.**Nota:** Quando os valores forem ajustados aos níveis muitos altos, sua rede não tira proveito do Cisco IOS Firewall ou do IPS da proteção de DOS.
5. Após o período de observação, verifique os contadores DoS com este comando:
   show ip inspect statistics Os parâmetros que você deve observar com qual para ajustar sua proteção de DOS são destacados em **corajoso**:`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. Configurar o **IP inspecionam a elevação máxima incompleta a um** valor 25-percent mais altamente do que o valor entreaberto indicado do contagem de sessão do maxever de seu roteador. 1.25 uma altura livre das ofertas 25-percent do multiplicador 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`**Nota:** Este documento descreve o uso de um multiplicador de 1.25 vezes a atividade típica de sua rede ajustar limites para contratar a proteção de DOS. Se você observa sua rede dentro dos picos da atividade da rede típica, este deve fornecer o headroom adequado para evitar a ativação da proteção de DOS do roteador sob tudo com exceção das circunstâncias atípicas. Se sua rede considera periodicamente as grandes explosões da atividade de rede legítima que excedem este valor, o roteador contrata as capacidades da proteção de DOS, que podem causar um impacto negativo em algum do tráfego de rede. Você deve monitorar seus log de roteador para detecções de atividade DoS e para ajustar o **IP inspecione a elevação máxima incompleta** e/ou o **IP inspeciona** limites **altos do minuto** para evitar provocar o DoS, depois que você determina que os limites estiveram encontrados em consequência da atividade de rede legítima. Você pode reconhecer o aplicativo da proteção de DOS pela presença de mensagens de registro tais como esta:
7. Configurar o **IP inspecionam o ponto baixo máxima incompleta ao** valor que seu roteador indicou para seu valor entreaberto do contagem de sessão 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 o **IP inspeciona a elevação do minuto** e o **ponto baixo do minuto** mantém uma soma de todo o TCP, UDP, e tentativas de conexão do Internet Control Message Protocol (ICMP) dentro do minuto prévio da operação de roteador, se as conexões foram bem sucedidas ou não. Uma taxa de conexão de aumentação pode ser indicativa de uma infecção do worm em uma rede privada, ou de um ataque tentado DoS contra um server. Uma estatística adicional da inspeção foi adicionada à **mostra IP inspeciona a** saída das **estatísticas em** 12.4(11)T e 12.4(10) para revelar a marca da água superior para a taxa da criação de sessão. Se você executa um Cisco IOS Software Release mais cedo do que 12.4(11)T ou 12.4(10), as estatísticas da inspeção não contêm esta linha:`Maxever session creation rate [value]`Os Cisco IOS Software Release antes de 12.4(11)T e de 12.4(10) não mantêm um valor para a taxa de conexão do minuto do maxever da inspeção, assim que você deve calcular o valor que você se aplica baseado do “em valores observados do contagem de sessão maxever”. As observações de diversas redes que usam a inspeção stateful da liberação 12.4(11)T do Cisco IOS Firewall na produção mostraram que as taxas da criação de sessão do maxever tendem a exceder a soma dos três valores (estabelecido, entreaberto, e terminando) do “no contagem de sessão maxever” por aproximadamente dez por cento. A fim calcular o IP inspecione o valor baixo do minuto, multiplicam 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 executa o Cisco IOS Software Release 12.4(11)T ou Mais Recente, ou o 12.4(10) ou mais atrasado, você pode simplesmente aplicar o valor mostrado do “na estatística da inspeção da taxa da criação de sessão maxever”:`Maxever session creation rate 330`Configurar:`ip inspect one-minute low 330`
9. Calcule e configurar o **IP inspecionam a elevação do minuto**. O IP inspeciona o alto valor do minuto deve ser 25-percent maior do que o valor baixo calculado do minuto, por exemplo:`ip inspect one-minute low (330) * 1.25 = 413` Configurar:`ip inspect one-minute high 413`**Nota:** Este documento descreve o uso de um multiplicador de 1.25 vezes a atividade típica de sua rede ajustar limites para contratar a proteção de DOS. Se você observa sua rede dentro dos picos da atividade da rede típica, este deve fornecer o headroom adequado para evitar a ativação da proteção de DOS do roteador sob tudo com exceção das circunstâncias atípicas. Se sua rede considera periodicamente as grandes explosões da atividade de rede legítima que excedem este valor, o roteador contrata as capacidades da proteção de DOS, que podem causar um impacto negativo em algum do tráfego de rede. Você deve monitorar seus log de roteador para detecções de atividade DoS e para ajustar o **IP inspecione a elevação máxima incompleta** e/ou o **IP inspeciona** limites **altos do minuto** para evitar provocar o DoS, depois que você determina que os limites estiveram encontrados em consequência da atividade de rede legítima. Você pode reconhecer o aplicativo da proteção de DOS pela presença de mensagens de registro tais como esta:
10. Você precisa de definir um valor para o **IP inspeciona o host máxima incompleta tcp** de acordo com seu conhecimento da capacidade de seus server. Este documento não pode fornecer diretrizes para a configuração da proteção de DOS do por-host desde que este valor varia baseado extensamente no desempenho do hardware e software do host final. Se você é incerto sobre os limites apropriados configurar para a proteção de DOS, você tem eficazmente duas opções com que definir o DoS limita:A opção preferível é configurar a proteção de DOS roteador-baseada do por-host a um alto valor (inferior ou igual ao valor

máximo de 4,294,967,295), e aplica a proteção host-específica oferecida pelo sistema operacional de cada host ou por um sistema de proteção contra intrusão host-baseado externo tal como o Cisco Security Agent (CSA).Examine a atividade e o desempenho entra seus host de rede e determina sua taxa de conexão sustentável máxima. Desde que o Firewall clássico oferece somente um contador global, você deve aplicar o valor máximo que você determina depois que você verifica todos seus host de rede para ver se há suas taxas de conexão máxima. É ainda aconselhável que você usa limites OS-específicos da atividade e um IPS host-baseado tal como o CSA.**Nota:** O Cisco IOS Firewall oferece proteção limitada contra ataques dirigidos em vulnerabilidades específicas do sistema operacional e do aplicativo. A proteção de DOS do Cisco IOS Firewall não oferece nenhuma garantia da proteção do acordo nos serviços de host final que são expostos aos ambientes potencialmente hostis.

11. Monitore a atividade da proteção de DOS sua rede. Idealmente, você deve usar um servidor de SYSLOG, ou idealmente, Cisco que monitora e que relata estações (MARTE) às ocorrências de registro da detecção de ataque DoS. Se a detecção acontece muito frequentemente, você precisa de monitorar e ajustar seus parâmetros da proteção de DOS.Para obter mais informações sobre dos ataques DoS TCP SYN, refira a definição de estratégias para proteger contra o ataque de recusa de serviço TCP SYN.

Verificar

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

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

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