GSR: Receber listas de controle de acesso

Índice

Introdução

Este documento descreve um novo recurso de segurança chamado de listas de controle de acesso de recebimento (rACLs)1 e fornece recomendações e diretrizes de implementação de rACL. Os ALCs de recepção são usados para aumentar a segurança em Cisco 12000 routers, protegendo o GRP (gigabit route processor) do roteador de tráfego desnecessário e possivelmente abominável. As ACLs de recebimento foram adicionadas como um waiver especial ao acelerador de manutenção para o Cisco IOS ® Software Release 12.0.21S2 e integradas no Cisco IOS Software Release 12.0(22)S.

Proteção GRP

Os dados recebidos por um Gigabit Switch Router (GSR) podem ser divididos em duas categorias amplas:

- Trafique que passagens através do roteador através do trajeto de encaminhamento.
- Trafique que deve ser enviado através do trajeto da recepção ao GRP para a análise mais aprofundada.

Nas operações normal, a grande maioria do tráfego corre através simplesmente de um GSR a caminho a outros destinos. Contudo, o GRP deve segurar determinados tipos de dados, especialmente protocolos de roteamento, acesso do roteador remoto, e tráfego de gerenciamento de rede (tal como o [SNMP] do protocolo administración de red simple). Além do que este tráfego, outro pacotes da camada 3 pôde exigir a flexibilidade de processamento do GRP. Estes incluiriam determinadas opções IP e determinados formulários de pacotes do Internet Control Message Protocol (ICMP). Refira o apêndice sobre recebem adjacências e pacotes punted para detalhes adicionais em relação ao rACLs e recebem o tráfego do trajeto no GSR.

Um GSR tem diversos trajetos de dados, cada formulários diferentes de conservação do tráfego. O tráfego de trânsito é encaminhado da placa de ingresso (LC) para a tela e depois para a placa de saída referente à entrega do próximo salto. Além do que o trajeto de dados do tráfego de trânsito, um GSR tem outros dois trajetos para o tráfego que exige o processamento local: LC a LC CPU e a LC a LC CPU à tela ao GRP. A tabela a seguir mostra os caminhos dos diversos recursos e protocolos normalmente utilizados.

Tipo de tráfego	Trajeto de dados
Tráfego normal (do trânsito)	LC à tela ao LC
Distribuindo Protocols/SSH/SNMP	LC a LC CPU à tela ao GRP
Eco ICMP (sibilo)	LC a LC CPU
Registro	

O processador da rota para o GSR tem uma capacidade limitada para processar o tráfego entregue dos LCs destinados para o próprio GRP. Se um volume alto dos dados exige punting ao GRP, esse tráfego pode oprimir o GRP. Isto conduz a um ataque de recusa de serviço (DOS) eficaz. O CPU do GRP esforça-se para prosseguir com a análise de pacote e começa-se a deixar cair pacotes, inundando a entrada-posse e as filas do Selective Packet Discard (SPD). [2] GSR devem ser protegidos contra três encenações, que podem resultar dos ataques DoS dirigidos em um GRP do roteador.

- Perda de Routing Protocol Packet a partir de uma inundação de prioridade normal
- Perda de pacotes da sessão de gerenciamento ([SSH] do telnet, do Secure Shell, SNMP) de uma inundação da prioridade normal
- Perda de pacote de inundação de alta prioridade falsificada

A Perda potencial de dados do protocolo de roteamento durante uma inundação da prioridade normal é aliviada atualmente a classificação estática e pela limitação da taxa do tráfego destinada ao GRP dos LC. Infelizmente, este enfoque tem limitações. A taxa que limita para o tráfego da prioridade normal destinado ao GRP é insuficiente para garantir a proteção aos dados prioritários do protocolo de roteamento se um ataque é entregado através de diversos LC. Abaixando o ponto inicial em que os dados da prioridade normal são deixados cair para fornecer tal proteção agrava somente a perda de tráfego de gerenciamento de uma inundação da prioridade normal.

Enquanto esta imagem mostra, o rACL está executado em cada LC antes que o pacote esteja transmitido ao GRP.

Um mecanismo de proteção para o GRP é exigido. o tráfego da influência do rACLs a que é enviado ao GRP devido recebe adjacências. Receba adjacências são adjacências do Cisco Express Forwarding para o tráfego destinado aos endereços IP de Um ou Mais Servidores Cisco ICM NT do roteador, tais como o endereço de broadcast ou os endereços configurado nas relações do roteador. [3] veja que o apêndice para secionar para mais detalhes em recebe adjacências e pacotes punted.

Trafique que incorpora um LC é enviado primeiramente ao CPU local do LC, e os pacotes que exigem o processamento pelo GRP são enfileirados enviando ao processador de rotas. O ACL de recebimento é criado no GRP e enviado para os CPUs dos diversos LCs. Antes que o tráfego esteja enviado do LC CPU ao GRP, o tráfego está comparado ao rACL. Se permitido, o tráfego passa ao GRP, quando todo tráfego restante for negado. O rACL é inspecionado antes para o LC

para a função de limitação de taxa GRP. Uma vez que o rACL é usado para todas as adjacências de recepção, alguns pacotes tratados pelo LC CPU (como requisições de eco) estão sujeitos também à filtragem de rACL. Isso deve ser levado em consideração ao designar entradas rACL.

Receba ACL são a parte uma de um alcance de programa de multiparte de mecanismos para proteger os recursos em um roteador. O trabalho futuro incluirá um componente da taxa limite ao rACL.

Impacto de desempenho

Nenhuma memória é consumida a não ser aquela necessária guardar a única entrada de configuração e a lista de acessos definida própria. O rACL é copiado a cada LC, assim que uma leve área de memória é tomada em cada LC. Totais, os recursos utilizados são minúsculos, especialmente quando comparados com os benefícios do desenvolvimento.

Uma recepção ACL não afeta o desempenho do tráfego enviado. O rACL aplica-se somente para receber o tráfego da adjacência. O tráfego enviado é nunca sujeito ao rACL. O tráfego de trânsito é filtrado usando ACLs de interface. Estes ACL “regulares” são aplicados às relações em um sentido especificado. O tráfego é sujeito ao processamento ACL antes do processamento RACL, assim que o tráfego negado pela relação ACL não será recebido pelo rACL. [4]

O LC que executa a filtração real (ou seja o LC que recebe o tráfego filtrado pelo rACL) terá aumentado a utilização CPU devido ao processamento do rACL. Esta utilização CPU aumentada, contudo, é causada por um volume alto do tráfego destinado ao GRP; o benefício do GRP da proteção rACL aumenta distante a utilização CPU aumentada em um LC. O uso de CPU em uma LC varia de acordo com o tipo de mecanismo LC. Por exemplo, dado o mesmo ataque, um Engine 3 LC terá uma mais baixa utilização CPU do que um motor 0 LC.

Permitir o turbocompressor ACL (usando o **comando access-list compiled**) converte ACL em uma série altamente eficiente de entradas de tabela da consulta. Quando o turbocompressor ACL é permitido, a profundidade rACL não afeta o desempenho. Ou seja a velocidade de processamento é independente do número de entradas no ACL. Se o rACL é curto, o turbocompressor ACL não aumentará significativamente o desempenho mas consumirá a memória; com rACLs curto, os ACL compilados são não necessários provável.

Protegendo o GRP, as ajudas do rACL asseguram o roteador e, finalmente, a estabilidade de rede durante um ataque. Como descrito acima, o rACL é processado no LC CPU, assim que a utilização CPU em cada LC aumentará quando um de grande volume dos dados é dirigido no roteador. No E0/E1 e nos alguns pacotes E2, a utilização CPU de 100+% pôde conduzir às gotas do protocolo de roteamento e da camada de link. Esses descartes estão localizados na placa, e os processos de roteamento de GRP são protegidos, mantendo assim a estabilidade. Os cartões E2 com microcódigo estrangular-permitido [5] ativam o modo de aceleração quando sob a carga pesada e somente a precedência dianteira 6 e 7 trafique ao protocolo de roteamento. Outros tipos de Engine têm arquiteturas da multi-fila; por exemplo, os cartões E3 têm três filas ao CPU, com pacotes de protocolo de roteamento (precedência 6/7) em um separado, fila de alta prioridade. O LC alto CPU, a menos que os pacotes de alta precedência o causarem, não conduzirá às gotas do protocolo de roteamento. Os pacotes às filas de baixa prioridade Tail-serão deixados cair. Finalmente, os cartões E4-based têm oito filas ao CPU, com o um dedicado aos pacotes de protocolo de roteamento.

Sintaxe

Uma recepção ACL é aplicada com o seguinte comando global configuration distribuir o rACL a cada LC no roteador.

[no] ip receive access-list *<num>*
Nesta sintaxe, o *<num>* é definido como segue.

[no] ip receive access-list *<num>*

Template básico e exemplos de ACL

Para poder usar este comando, você precisa de definir uma lista de acessos que identifique o tráfego que deve ser permitido falar ao roteador. A lista de acesso precisa incluir protocolos de roteamento e tráfego de gerenciamento (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF], SNMP, SSH, Telnet). Consulte a seção sobre diretrizes de distribuição para obter mais detalhes.

A seguinte amostra de ACL fornece um descrição simples e apresenta alguns exemplos de configuração que podem ser adaptador para usos específicos. A ACL ilustra as configurações exigidas para diversos serviços/protocolos comumente necessários. Para o SSH, o telnet, e o SNMP, um endereço de loopback é usado como o destino. Para os protocolos de roteamento, o endereço real da relação é usado. A escolha de interfaces do encaminhador para usar no rACL é determinada por políticas e operações do site local. Por exemplo, se os laços de retorno são usados para todas as sessões de peer BGP, a seguir somente aqueles laços de retorno precisam de ser permitidos nas indicações da **licença** para o BGP.

[no] ip receive access-list *<num>*
Como com todo o Cisco ACL, há uma **instrução de negação** implícita na extremidade da lista de acessos, tão todo o tráfego que não combinar uma entrada no ACL será negado.

Nota: A palavra-chave do **log** pode ser usada para ajudar a classificar o tráfego destinado ao GRP que não é permitido. Embora a palavra-chave do **log** forneça o insight valioso nos detalhes de batidas ACL, as batidas excessivas a uma entrada ACL que use esta palavra-chave aumentarão a utilização CPU LC. O impacto no desempenho associado com o registro variará com tipo de Engine LC. Geralmente, registrar deve ser usado somente quando necessário nos motores 0/1/2. Para os motores 3/4/4+, registrar resulta dentro distante menos de um impacto devido ao desempenho da CPU aumentado e à arquitetura da multi-fila.

O nível de granularidade dessa lista de acessos é determinado pela política de segurança local (por exemplo, o nível de filtragem necessário para vizinhos OSPF).

rACLS e pacotes fragmentados

Os ACL têm uma palavra-chave dos **fragmentos** que permita o comportamento fragmentado especializado do manuseio de pacotes. Geralmente, os fragmentos não iniciais que combinam as indicações L3 (independentemente da informação L4) em um ACL são afetados pela indicação do **permit or deny da** entrada combinada. Note que o uso da palavra-chave dos **fragmentos** pode forçar ACL a nega ou permite fragmentos não iniciais com mais granularidade.

No contexto rACL, filtrar fragmentos adiciona uma camada adicional de proteção contra um ataque DoS que use somente fragmentos não iniciais (como FO > 0). O uso de uma instrução

deny para fragmentos não-iniciais no começo do rACL impede que todos os fragmentos não-iniciais acessem o roteador. Sob circunstâncias raras, uma sessão válida pôde exigir a fragmentação e consequentemente ser filtrado se uma indicação do **fragmento da negação** existe no rACL.

Por exemplo, considere o ACL parcial mostrado abaixo.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

Adicionar estas entradas ao começo de um rACL nega todo o acesso do fragmento não inicial ao GRP, quando os pacotes não fragmentados ou os fragmentos iniciais passarem às linhas seguintes do rACL não afetado pelas indicações do **fragmento da negação**. O snippet rACL acima igualmente facilita a classificação do ataque desde cada protocolo – o protocolo de datagrama universal (UDP), o TCP, e o ICMP – incrementos separa contadores no ACL.

Refira listas de controle de acesso e fragmentos IP para uma discussão detalhada das opções.

Avaliação de risco

Assegure-se de que o rACL não filtre o tráfego crítico tal como protocolos de roteamento ou acesso interativo ao Roteadores. O tráfego necessário de filtração podia conduzir a uma incapacidade alcançar remotamente o roteador, assim exigindo uma conexão de console. Por este motivo, as configurações de laboratório devem imitar a distribuição real de tão perto quanto possível.

Como sempre, Cisco recomenda que você testa esta característica no laboratório antes do desenvolvimento.

Apêndices e notas

Receber adjacências e pacotes punted

Como descrito mais cedo neste documento, alguns pacotes exigem o processamento de GRP. Os pacotes são direcionados do plano de encaminhamento de dados para o GRP. Esta é uma lista dos formulários comuns dos dados da camada 3 que exigem o acesso GRP.

- Protocolos de Roteamento
- Tráfego de controle de transmissão múltipla (OSPF, [HSRP] do protocolo de roteador do standby recente, [TDP] do protocolo de distribuição da etiqueta, [PIM] da transmissão múltipla independente de protocolo, e tais)
- Pacotes do Multiprotocol Label Switching (MPLS) que precisam a fragmentação
- Pacotes com certas opções de IP, como alerta de roteador
- Primeiro pacote de fluxos de transmissão múltipla
- Pacotes ICMP fragmentados que exigem a remontagem
- Todos traficam destinado ao roteador próprios (à exceção do tráfego segurado no LC)

Desde que o rACLs se aplica para receber adjacências, o rACL filtra algum tráfego que não punted ao GRP mas é uma adjacência da recepção. O exemplo mais comum é uma requisição de

eco ICMP (ping). As requisições de eco ICMP dirigidas ao roteador são seguradas pelo LC CPU; desde que os pedidos são receba adjacências, elas são filtrados igualmente pelo rACL. Portanto, para permitir ping nas interfaces (ou loopbacks) do roteador, rACLS deve permitir explicitamente as solicitações de eco.

Épossível ver a recepção de adjacências usando o comando show ip cef.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

Diretrizes de distribuição

Cisco recomenda práticas conservadoras do desenvolvimento. Para distribuir com sucesso o rACLs, as exigências existentes do controle e do acesso do plano de gerenciamento devem bem ser compreendidas. Em algumas redes, determinar o perfil de tráfego exato necessário construir as lista de filtração pôde ser difícil. As seguintes diretrizes descrevem um método bastante conservador para implantar rACLs usando configurações rACL iterativas para ajudar a identificar e eventualmente filtrar o tráfego.

1. **Identifique os protocolos usados na rede com uma classificação ACL.**Distribua um rACL que permita todos os protocolos conhecidos que alcançam o GRP. Este rACL do " descoberta " deve ter ambos os endereços de rementente e destinatário ajustados a **alguns**. Registrar pode ser usado para desenvolver uma lista de endereços de origem que combinam as instruções de permissão de protocolo. Além do que a instrução de permissão de protocolo, uma **licença toda a qualquer linha de registro na** extremidade do rACL pode ser usada para identificar outros protocolos que seriam filtrados pelo rACL e que puderam exigir o acesso ao GRP.O objetivo é determinar quais protocolos a rede específica utiliza. Registrar deve ser usado para que a análise determine “que outro” pôde comunicar com o roteador.**Nota:** Embora a palavra-chave do **log** fornecesse o insight valioso nos detalhes de batidas ACL, as batidas excessivas a uma entrada ACL que usasse esta palavra-chave puderam conduzir a um número opressivamente de entradas de registro e possivelmente de uso alto do CPU de roteador. Use a palavra-chave log para pequenos períodos de tempo e somente quando necessário para ajudar a classificar o tráfego.
2. **Reveja pacotes identificados e comece a filtrar o acesso ao GRP.**Assim que os pacotes filtrados pelo rACL na etapa 1 tenham sido identificados e revistos, implemente um rACL com uma instrução permit any any para os protocolos permitidos. Apenas como em etapa 1, a palavra-chave do **log** pode fornecer mais informação sobre os pacotes que combinam as entradas da **licença**. O uso de deny any any log no final pode ajudar a identificar pacotes inesperados destinados ao GRP. Este rACL fornecerá proteção básica e permitirá que os engenheiros da rede assegurem que todo o tráfego necessário seja permitido.O objetivo é testar a escala dos protocolos que precisam de se comunicar com o roteador sem ter a escala explícita do origem de IP e dos endereços de destino.
3. **Restrinja uma escala macro dos endereços de origem.**Permita que apenas o intervalo total de seu Classless Interdomain Routing (CIDR) Block seja permitido como o endereço de origem. Por exemplo, se você foi atribuído 171.68.0.0/16 para sua rede, a seguir permita endereços de origem de apenas 171.68.0.0/16.Esta etapa reduz o risco sem interromper

qualquer serviço. Igualmente fornece pontos de dados dos dispositivos/povos fora de seu bloco CIDR que pôde alcançar seu equipamento. Todo o endereço exterior será deixado cair.Os pares do BGP externo exigirão uma exceção, desde que os endereços de fonte permitida para a sessão se encontrarão fora do bloco CIDR.Essa fase pode ser ignorada por alguns dias para coletar dados para a fase seguinte de refinamento da rACL.

4. **Reduza as instruções de permissão rACL para permitir somente endereços de origem autorizados conhecidos.**Limite cada vez mais o endereço de origem para permitir somente as fontes que se comunicam com o GRP.
5. **Limite os endereços de destino no rACL. (*opcional*)**Alguns provedores de serviço da Internet (ISP) podem escolher permitir apenas protocolos específicos para usar endereços de destino específicos no roteador. Essa fase final tem a finalidade de limitar o intervalo dos endereços de destino que aceitarão tráfego para um protocolo. [6]

Exemplo de distribuição

O exemplo a seguir mostra uma ACL de recebimento que protege um roteador com base no seguinte endereçamento.

- O bloco de endereço do ISP é 169.223.0.0/16.
- O bloco da infraestrutura do ISP é 169.223.252.0/22.
- O circuito de retorno do roteador é 169.223.253.1/32.
- O roteador é um roteador de backbone central, portanto somente sessões de BGP estão ativas.

Dado esta informação, a inicial recebe o ACL poderia ser algo como o exemplo abaixo. Como conhecemos o bloco de endereço de infra-estrutura, permitiremos primeiro o bloco inteiro. Mais tarde, umas entradas de controle de acesso mais detalhadas (ACE) serão adicionadas como os endereços específicos são obtidas para todos os dispositivos que precisam o acesso ao roteador.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
!--- Note: This template must be tuned to the network’s !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
```

```
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 – Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example – Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 – Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

Notas

1. Consulte Understanding Selective Packet Discard (SPD) [&Entendendo o SPD (Descarte seletivo de pacotes)] e mantenha as diretrizes da fila para aumentar a resistência do DoS.
2. Para obter mais informações sobre do Cisco Express Forwarding e das adjacências, refira a vista geral do Cisco Express Forwarding.
3. Para uma discussão detalhada de diretrizes de distribuição e de comandos relacionados ACL, refere a aplicação de ACL em Cisco 12000 Series Internet Router.
4. Isto se refere aos conjuntos Vanilla, Border Gateway Protocol Policy Accounting (BGPPA), Per Interface Rate Control (PIRC) e Frame Relay Traffic Policing (FRTP).
5. A fase II da proteção de caminho da recepção permitirá a criação de uma interface de gerenciamento, limitando automaticamente que endereço IP de Um ou Mais Servidores Cisco ICM NT escutará pacotes recebidos.

Informações Relacionadas

- Página de Suporte das Listas de Acesso
- Suporte Técnico - Cisco Systems