Pesquisando defeitos a utilização da alta utilização da CPU no processo de entrada IP

Índice

Introdução

Este original explica como pesquisar defeitos o valor de utilização da alta utilização da CPU ao processo de entrada IP.

Note: Este original não fornece estratégias para impedir tipos diferentes de ataques.

Pré-requisitos

Requisitos

Cisco recomenda que você lê a utilização da alta utilização da CPU do Troubleshooting no Roteadores de Cisco antes que você continue com este original.

Componentes Utilizados

Este original não é restringido à versão de software e hardware específica.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se você está trabalhando em uma rede viva, assegure-se de que você compreenda o impacto potencial do comando any antes do usar.

Convenções

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

Entrada de IP

O processo de software do ® do Cisco IOS chamou a *entrada IP* toma de pacotes IP do switching por processo. Se o processo de entrada IP usa raramente recursos da alta utilização da CPU, o roteador é switching por processo muito tráfego IP. Verifique estas edições:

- **O switching de interrupção é desabilitado em uma relação (ou em relações) que tenha (tenha) muito tráfego**O switching de interrupção refere o uso dos algoritmos de switching diferentes da comutação do processo. Os exemplos incluem o interruptor rápido, switching ótima, Cisco Express Forwarding Switching, e assim por diante (refira princípios do ajuste de desempenho para detalhes). Examine a saída do **comando show interfaces switching** ver que relação é carregada com o tráfego. Você pode verificar o **comando show ip interface** ver que método de switching é usado em cada relação. Re-permita o switching de interrupção nessa relação. Recorde que o interruptor rápido regular está configurado em interfaces de saída: se o interruptor rápido é configurado em uma relação, os pacotes que saem dessa relação são fast-switched. O Cisco Express Forwarding Switching é configurado em interfaces de entrada. Para criar o banco de informação de encaminhamento (FIB) e as entradas de tabela de contiguidade em uma interface particular, configurar o Cisco Express Forwarding Switching em todas as relações que distribuem a essa relação.
- **O interruptor rápido na mesma relação é desabilitado**Se uma relação tem muitos endereços secundários ou os subinterfaces e lá são muito tráfego originado da relação e destinado para um endereço nessa mesma relação, a seguir todos aqueles pacotes processo-estão comutados. Nesta situação, você deve permitir a mesmo-relação do cache de rota IP na relação. Quando a comutação Cisco Express Forwarding é usada, não é necessário habilitar a comutação Cisco Express Forwarding switching na mesma interface separadamente.
- **O interruptor rápido em uma relação que fornece o roteamento de política é desabilitado**Se um mapa de rotas esteve configurado em uma relação, e muito tráfego está segurado pelo mapa de rotas, então o processo-Switches do roteador este tráfego. Nesta situação, você deve permitir o ip route-cache policy na relação. Verifique as limitações mencionadas “permitindo na seção do roteamento baseado em política fast-switched” de configurar o roteamento baseado em política.
- **Trafique que não pode interrupção-ser comutado chega**Este pode ser alguns dos tipos de tráfego listados. Clique artigos sobre ligados para mais informação.Pacotes para que não há nenhuma entrada contudo no cache de switchingMesmo se rápido, o melhor, ou o Cisco Express Forwarding Switching (CEF) é configurado, um pacote para que lá não é nenhum fósforo no cache de switching rápido ou MENTE e as tabelas de adjacência são processadas. Uma entrada é criada então no esconderijo ou na tabela apropriada, e todos os pacotes subsequente que combinam os mesmos critérios são rápidos, os melhores, ou comutados por CEF. Nas circunstâncias normal, estes pacotes processados não causam a utilização da alta utilização da CPU. Contudo, se há um dispositivo na rede que 1) gerencie pacotes em uma taxa extremamente alta para os dispositivos alcançáveis através do roteador, e 2) usam a fonte ou endereços IP de destino diferentes, não há um fósforo para estes pacotes no cache de switching ou na tabela, assim que são processados pelo processo de entrada IP (se o Netflow Switching as portas é configurado, do fonte e do TCP destino são verificadas contra entradas no netflow cache também). Este dispositivo de origem pode ser um dispositivo NON-funcional ou, mais provável, um dispositivo tentando um ataque.(*) Somente com adjacências glean. Refira o Cisco Express Forwarding para obter mais informações sobre das

adjacências do Cisco Express Forwarding.Pacotes destinados ao roteadorEstes são exemplos de pacotes destinados para o roteador:Atualizações de roteamento que chegam em uma taxa extremamente alta. Se o roteador recebe uma quantidade enorme de atualizações de roteamento que têm que ser processadas, esta tarefa pôde sobrecarregar o CPU. Normalmente, isto não pode acontecer em uma rede estável. A maneira que você pode recolher mais informação depende do protocolo de roteamento você configurou. Contudo, você pode começar verificar periodicamente a saída do **comando show ip route summary**. Os valores que mudam rapidamente são um sinal de uma rede instável. O meio frequente das alterações de tabela de roteamento aumentou o protocolo de roteamento que processa, que conduz à utilização CPU aumentada. Para mais informações sobre de como pesquisar defeitos esta edição, refira pesquisando defeitos a seção TCP/IP do guia de Troubleshooting da rede interna.Algum outro tipo do tráfego destinado para o roteador. Verificação que é entrada ao roteador e às ações de usuário. Se alguém é entrado e emite os comandos que produzem saídas longas, a utilização da alta utilização da CPU pelo processo entrado “IP” é seguida por uma utilização CPU muito mais alta pelo processo de EXEC virtual.Ataque falso. Para identificar o problema, emita o **comando show ip traffic** verificar a quantidade de tráfego IP. Se há um problema, o número de pacotes recebidos com um destino local é significativo. Em seguida, examine a saída do para verificar que relação os pacotes estão vindo. Uma vez que você identificou a relação de recepção, gire sobre a **contabilidade IP na** interface enviada e veja se há um teste padrão. Se há um ataque, o endereço de origem é quase sempre diferente, mas o endereço de destino é o mesmo. Uma lista de acessos pode ser configurada para resolver temporariamente a edição (preferivelmente no dispositivo o mais próximo à fonte dos pacotes), mas a solução real é seguir para baixo o dispositivo de origem e parar o ataque.Tráfego de broadcastVerifique o número de pacotes de transmissão na saída do **comando show interfaces**. Se você compara a quantidade de transmissões à quantidade total de pacotes que estiveram recebidos na relação, você pode ganhar uma ideia de se há umas despesas gerais das transmissões. Se há um LAN com diverso Switches conectado ao roteador, a seguir este pode indicar um problema com a medida - árvore.Pacotes IP sem opçõesPacotes que exigem a Conversão de protocoloProtocolo multilink point-to-point (apoiado no Cisco Express Forwarding Switching)Tráfego compactadoSe há o adaptador de serviço do No Compression (CSA) no roteador, os pacotes compactados devem processo-ser comutados.Tráfego criptografadoSe há o adaptador de serviço do no encryption (ESA) no roteador, os pacotes criptografado devem processo-ser comutados.Pacotes que atravessam interfaces serial com o encapsulamento X.25No conjunto de protocolos X.25, o controle de fluxo é executado na segunda camada do abrir interconexão do sistema (OSI).

- Muitos pacotes, isso chegam em uma taxa extremamente alta, para um destino diretamente em uma sub-rede conectada, para que não há nenhuma entrada na tabela do Address Resolution Protocol (ARP). Isto não deve acontecer com tráfego TCP devido ao mecanismo de janelamento, mas pode acontecer com tráfego do User Datagram Protocol (UDP). Para identificar o problema, repita as ações sugeridas a fim seguir para baixo um ataque falso.
- Muito tráfego multicast dirige o roteador. Infelizmente, não há nenhuma maneira fácil examinar a quantidade do tráfego de transmissão múltipla. **O comando show ip traffic** mostra somente a informação sumária. Contudo, se você configurou o roteamento de transmissão múltipla no roteador, você pode permitir o switching rápido dos pacotes de transmissão múltipla com o **comando ip mroute-cache interface configuration** (o switching rápido dos pacotes de transmissão múltipla está à revelia).
- O roteador é oversubscribed. Se o roteador é usado e não pode segurar esta quantidade de tráfego, tente distribuir a carga entre o outro Roteadores ou comprar um roteador de produto

avançado.

- A tradução de endereço de rede IP (NAT) é configurada no roteador, e em lotes de pacotes do Domain Name System (DNS) dirige o roteador. O UDP ou os pacotes de TCP com porta de origem ou destino 53 (DNS) punted sempre ao nível de processo pelo NAT.
- Há outros tipos de pacotes que são direcionados para o processamento.
- Há uma fragmentação do IP datagram. Há um aumento pequeno no CPU e na carga adicional devido da memória a fragmentar de um IP datagram. Refira a fragmentação de IP da resolução, as edições MTU, MSS, e PMTUD com GRE e IPSEC para obter mais informações sobre de como pesquisar defeitos esta edição.

O que quer que a razão para a utilização da alta utilização da CPU no processo de entrada IP, a fonte do problema pode ser seguida para baixo se você debuga os pacotes IP. Desde que a utilização CPU é já alta, o processo debugar tem que ser executado com o cuidado extremo. O processo debugar produz lotes das mensagens, tão somente **registrar protegidas** deve ser configurado.

Registrar a um console levanta interrupções desnecessárias para o CPU e aumenta a utilização CPU. Registrar a um host (ou ao logging de monitor) gerencie o tráfego adicional em relações.

O processo debugar pode ser começado com o **comando debug ip packet detail exec**. Esta sessão não deve durar mais por muito tempo de três a cinco segundos. Os mensagens de debugging são redigidos no logging buffer. Uma captação de uma sessão do IP debugging da amostra é fornecida na seção do exemplo de ip packet debugging session deste original. Uma vez que o dispositivo de origem de pacotes IP indesejáveis é encontrado, este dispositivo pode ser desligado da rede, ou uma lista de acessos pode ser criada no roteador para deixar cair pacotes desse destino.

Exemplo de sessão de depuração de pacote IP

Os destinos de registro configurados devem ser verificados primeiramente com o **comando show logging**:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 52 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 148 messages logged
    Trap logging: level informational, 64 message lines logged
        Logging to 192.168.100.100, 3 message lines logged
        Logging to 192.168.200.200, 3 message lines logged
 --More--
```

Desabilite todos os destinos de registro exceto o logging buffer, e o logging buffer claro:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#no logging console
router(config)#no logging monitor
router(config)#no logging 192.168.100.100
router(config)#no logging 192.168.200.200
router(config)#^Z
router#clear logging
Clear logging buffer [confirm]
router#
```

Para a melhor legibilidade do resultado do debug, o datetime e os formatos de tempo de milisegundo devem ser permitidos:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service timestamps log datetime msec
router(config)#service timestamps debug datetime msec
router(config)#end
router#
```

Um sessão de debugging pode agora ser começado:

```
router#debug ip packet detail
IP packet debugging is on (detailed)
```

A eliminação de erros não deve durar mais de três a cinco segundos. A sessão pode ser parada com o comando undebug all exec:

```
router#undebug all
All possible debugging has been turned off
```

Os resultados podem ser verificados com o comando show logging exec:

```
router#show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

O log mostra aquele:

- Um pacote foi recebido cada quatro milissegundos
- O endereço IP de origem é 192.168.40.53
- Os pacotes vieram dentro na relação Ethernet0/1
- Os pacotes possuem diferentes endereços IP de destino
- Os pacotes foram enviados na interface da Ethernet0/0
- O endereço IP do próximo salto é 10.200.40.1
- Os pacotes eram os pedidos ICMP (type=8)Neste exemplo, você pode ver que a utilização da alta utilização da CPU no processo de entrada IP esteve causada por uma inundação de ping do endereço IP 192.168.40.53.Inundações de SYN podem ser facilmente detectadas desse modo porque a presença de flag SYN é indicada na saída de depuração:
  ```
  router#show logging
  ```

```
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 145 messages logged
    Trap logging: level informational, 61 message lines logged
Log Buffer (64000 bytes):

*Mar  3 03:43:27.320: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.204
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.324: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.205
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.324: ICMP type=8, code=0
*Mar  3 03:43:27.328: IP: s=192.168.40.53 (Ethernet0/1), d=144.254.2.206
   (Ethernet0/0), g=10.200.40.1, len 100, forward
*Mar  3 03:43:27.328: ICMP type=8, code=0
...
```

Informações Relacionadas

- Troubleshooting de Alta Utilização de CPU em Cisco Routers
- Comando show processes
- Alta Utilização da CPU em Catalyst 2900XL/3500XL Switches
- Conceitos básicos de ajuste de desempenho
- Suporte técnico & documentação - Cisco Systems