



ID do Documento: 118735

Atualizado em: fevereiro 10, 2015

Contribuído por Sumit Bist, engenheiro de TAC da Cisco.



[Transferência PDF](#)



[Imprimir](#)

[\[+\] Feedback](#)

Produtos Relacionados

- [Segurança](#)
- [Módulo de serviços de firewall Cisco Catalyst série 6500](#)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Condições](#)

[Verificar](#)

[Solução](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento descreve um problema específico com gotas intermitentes do tráfego no módulo de serviços de firewall (FWSM) após um upgrade de software para liberar 4.1.11 ou mais atrasado.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no FWSM com Software Release 4.1(11) ou Mais Recente.

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.

Informações de Apoio

Conforme o comportamento FWSM, se você usa o TCP enquanto o protocolo de transporte de registo a fim enviar mensagens a um servidor de SYSLOG, ele nega novas conexões como uma medida de Segurança se o FWSM é incapaz de alcançar o servidor de SYSLOG. Você pode usar **logging permit-hostdown** o comando a fim remover esta limitação.

Problema

Há uma edição intermitente da gota do tráfego no FWSM após uma elevação para liberar 4.1.11 ou mais atrasado. Os começos FWSM para negar todas as novas conexões.

A gota a mais visível do tráfego é para o Internet Control Message Protocol (ICMP), desde que cada requisição de eco ICMP é tratada como uma nova conexão. A Conectividade é restaurada uma vez que a conexão de TCP ao servidor de SYSLOG é bem sucedida.

Para o FWSM libere 4.1.11 ou mais atrasado, se o servidor de SYSLOG com base em TCP não é alcançável mesmo com política da “licença-hostdown”, o FWSM nega todas as novas conexões. “A característica da licença-hostdown de registo” já não trabalha depois que uma elevação FWSM para liberar 4.1.11 ou mais atrasado.

O FWSM continua a reconectar ao servidor de SYSLOG TCP cada minuto até que o Time Server estiver acima. Assim, uma única falha do cumprimento de TCP conduz a uma indisponibilidade minuto mínima para todas as **novas conexões**, porque o FWSM tenta contactar outra vez o servidor de SYSLOG TCP, somente depois que um minuto.

Condições

- A liberação 4.1.11 das corridas FWSM ou mais atrasado.
- O FWSM deve reagir do modo simples.
- O servidor de SYSLOG TCP deve ser inacessível do FWSM.

Verificar

A fim identificar este comportamento, verifique as estatísticas lentas do trajeto (NP3). O contador dos conns da negação (estado conexão) aumenta se o servidor de SYSLOG com base em TCP não é alcançável, mesmo com política da “licença-hostdown”.

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <-----Counter to monitor
```

```
pri/act# show clock
09:32:06.020 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 46634
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 46235 <-----Counter seen increasing
```

Solução

Um defeito foi arquivado para seguir esta edição, mas não será fixo desde que o FWSM alcançou a extremidade da data de versão de manutenção de software.

[Fim--venda e anúncio End-of-Life para os módulos de serviços de firewall](#)

A fim fixar esta edição, mude a configuração de servidor de logging ao transporte UDP.

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <-----Counter to monitor
```

```
pri/act# show clock
09:32:06.020 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
```

Discard Statistics

Egress Discards : 46634

ACL Denied Packets : 157

Rev Route Lkup Fail : 202

Self Route Packets : 40

Deny Conns (Conn State): 46235 <-----Counter seen increasing

Informações Relacionadas

- [Referência de comandos: licença-hostdown de registo](#)
- [Referência de comandos: logging host](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: fevereiro 10, 2015

ID do Documento: 118735