Respostas de pesquisa SNMP de IP diferente em 2GFI em comparação com 4GFI

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[A saída do teste mostra um comportamento diferente de 6200 e 6400 FI quando o VIP é interrogado por SNMP](#)
[FI 6248 com firmware UCSM 4.0.4e](#)
[FI 6454 com firmware UCSM 4.0.4d](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve um comportamento diferente quando o Simple Network Monitoring Protocol (SNMP) caminha ou é direcionado para a interconexão de estrutura (FI) 6200 em comparação com a FI 6454. Firewalls stateful podem bloquear respostas IP físicas a caminhadas SNMP de IPs virtuais (VIP) no FI 6200, enquanto o problema não é visto no FI 6454.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta Walk SNMP instalada em um servidor com conectividade com o domínio Unified Computing System Manager (UCSM).
- 6248 FI e 6454 FI

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Ferramenta Walk SNMP instalada em um servidor com conectividade com o domínio Unified Computing System Manager (UCSM).
- 6248 FI com firmware UCSM 4.0(4e)
- 6454 FI com firmware UCSM 4.0(4f)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Qualquer software de pesquisa ou passeio SNMP de terceiros
- FI 6296

Informações de Apoio

Os firewalls entre os servidores FI e SNMP Collectors/Walk podem ser configurados para a Inspeção Stateful, o que significa que quando uma solicitação é enviada de um determinado endereço IP, a resposta é permitida apenas desse mesmo endereço IP. As interconexões em malha usam um IP virtual (VIP) ao qual o FI principal responde. A Inspeção Stateful do Firewall pode bloquear respostas SNMP em FI de segunda geração como o 6248 se o SNMP Get ou Walk for solicitado do VIP como nesse modelo se a resposta vier do IP físico do FI primário. O Firewall com inspeção stateful permite somente respostas do IP de destino para que os pacotes sejam bloqueados. Nos testes da 4ª geração de FI, como a resposta 6454 com qual IP é solicitado, o VIP ou o IP físico responderá se for o IP de destino.

A solução alternativa para FI de segunda geração, como o 6248 e o 6296, é direcionar o IP Físico do FI Primário ou alterar as regras do Firewall para permitir respostas de IP Físico do FI se for feita uma solicitação do VIP.

A saída do teste mostra um comportamento diferente de 6200 e 6400 FI quando o VIP é interrogado por SNMP

FI 6248 com firmware UCSM 4.0.4e

Saída da linha de comando do servidor de passeio SNMP:

```
[SNMP Walk Server]$ snmpwalk -c 'xxx' 172.16.0.52 <<< SNMP Walk of the Physical IP of FI
snmpwalk: No securityName specified <<<<<<<<<<<<<<<<< No network errors so successful reply
[SNMP Walk Server]$ snmpwalk -c 'xxx' 172.16.0.53 <<< SNMP Walk of the Virtual IP
snmpwalk: Timeout <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Network Error
```

Captura de pacote FI:

```
FI-B(nxos)# ethanalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-captured-
frames 0
Capturing on eth0
2020-01-06 11:44:00.739413 10.0.45.154 -> 172.16.0.52 SNMP get-request <<< SNMP Walk of the
Physical IP of FI
2020-01-06 11:44:01.274570 172.16.0.52 -> 10.0.45.154 SNMP report <<<<<<<< FI replies with
Physical IP of Primary FI
```

```
FI-B(nxos)# ethanalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-captured-
frames 0
Capturing on eth0
2020-01-06 11:44:50.886972 10.0.45.154 -> 172.16.0.53 SNMP get-request <<< SNMP Walk of the
```

```
Virtual IP
2020-01-06 11:44:50.887350 172.16.0.52 -> 10.0.45.154 SNMP report <<<<<<<< FI Replies with the
IP of the Primary FI Physical IP Stateful Firewall may block this reply
2020-01-06 11:44:51.886878 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:51.887223 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:52.887808 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:52.888161 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:53.888741 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:53.889087 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:54.889477 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:54.889816 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:55.890280 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:55.890623 172.16.0.52 -> 10.0.45.154 SNMP report
```

FI 6454 com firmware UCSM 4.0.4d

Saída da linha de comando do servidor de passeio SNMP:

```
[SNMP Walk Server]$ snmpwalk -c 'fgING$df' 172.16.0.94 <<< SNMP Walk of the Physical IP of FI
snmpwalk: No securityName specified <<<<<<<<<<<<<<<<< No network errors so successful reply
[SNMP Walk Server]$ snmpwalk -c 'fgING$df' 172.16.0.93 <<< SNMP Walk of the Virtual IP
snmpwalk: No securityName specified <<<<<<<<<<<<<<<<< No network errors so successful reply
```

Captura de pacote FI:

```
stha99u11-B(nx-os)# ethanalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-
captured-frames 0

Capturing on mgmt0
2020-01-06 12:01:31.866959 10.0.45.154 -> 172.16.0.94 SNMP get-request <<< SNMP Walk of the
Physical IP of FI
2020-01-06 12:01:31.868620 172.16.0.94 -> 10.0.45.154 SNMP report 1.3.6.1.6.3.15.1.1.4.0 <<< FI
replies from Physical IP no issues with Stateful Firewall
2020-01-06 12:01:47.647205 10.0.45.154 -> 172.16.0.93 SNMP get-request <<< SNMP Walk of the
Virtual IP
2020-01-06 12:01:47.648800 172.16.0.93 -> 10.0.45.154 SNMP report 1.3.6.1.6.3.15.1.1.4.0 <<< FI
replies from IP of Virtual IP no issues with Stateful Firewall
```

Informações Relacionadas

- Guia de monitoramento do sistema do Cisco UCS Manager, versão 4.0
- Suporte Técnico e Documentação - Cisco Systems