SNMP Polling Replies from Different IP in 2GFI Compared to 4GFI

Contents

Introduction

Prerequisites

Requirements

Components Used

Background Information

Test Output Shows Different Behavior of 6200 and 6400 FI when VIP is SNMP Polled

FI 6248 with UCSM Firmware 4.0.4e

FI 6454 with UCSM Firmware 4.0.4d

Related Information

Introduction

This document describes different behavior when Simple Network Monitoring Protocol (SNMP) walks or gets are directed to 6200 Fabric Interconnect (FI) compared to 6454 FI. Stateful Firewalls may block physical IP responses to SNMP walks of Virtual IPs (VIP) in FI 6200 while the issue is not seen in 6454 FI.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SNMP Walk Tool installed on a server with connectivity to Unified Computing System Manager (UCSM) Domain.
- 6248 FI and 6454 FI

Components Used

The information in this document is based on these software and hardware versions:

- SNMP Walk Tool installed on a server with connectivity to Unified Computing System Manager (UCSM) Domain.
- 6248 FI with UCSM Firmware 4.0(4e)
- 6454 FI with UCSM Firmware 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. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardware and software versions:

- Any 3rd Party SNMP Walk or Polling Software
- 6296 FI

Background Information

Firewalls between FI and SNMP Collectors/Walk servers may be set for Stateful Inspection, this means that when a request is sent from a certain IP address the response is only allowed from that same IP address. Fabric Interconnects use a Virtual IP (VIP) that the Primary FI responds to. Firewall's Stateful Inspection may block SNMP replies in 2nd generation FI like the 6248 if the SNMP Get or Walk is requested of the VIP as in that model FI the reply comes from the physical IP of the Primary FI. The Firewall with stateful inspection only allows replies from the targeted IP so the packets are blocked. In tests 4th generation FI like the 6454 reply with what IP is requested the VIP or either Physical IP will reply if they are the targeted IP.

The workaround for 2nd Generation FI like the 6248 and 6296 is to target the Physical IP of the Primary FI or to alter the Firewall rules to allow replies from either Physical IP of FI if a request is made of the VIP.

Test Output Shows Different Behavior of 6200 and 6400 Fl when VIP is SNMP Polled

FI 6248 with UCSM Firmware 4.0.4e

SNMP Walk Server Command Line Output:

```
[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
```

FI Packet Capture:

```
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 with UCSM Firmware 4.0.4d

SNMP Walk Server Command Line Output:

[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 FI Packet Capture:

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
```

Related Information

- Cisco UCS Manager System Monitoring Guide, Release 4.0
- Technical Support & Documentation Cisco Systems