GFI ClearView: Troubleshooting the deployment





Overview

If you do not see any traffic in the GFI ClearView appliance after deployment, it is either because the appliance is not licensed or there is no traffic reaching it. In this guide, we will cover how you can troubleshoot your GFI ClearView deployment to identify which part of the link is broken.

Step-by-Step Guide

Verify that the appliance is licensed

From the WebUI, navigate to the **Dashboard > System** tab. Verify that the **SS Expiry Date** field shows a date in the future.

2 Verify that port mirroring is enabled on the switch

As covered in the deployment guide, verify from your managed switch's control panel/ management user interface that mirroring is correctly enabled to copy all traffic to an unused port.

³ Verify that the cable from the switch to the host machine is connected

At this stage, verify that the host machine's NIC has a connection to the unused port on the switch that has mirroring enabled.

4 Verify through a packet sniffer that the host's port is receiving traffic

In the majority of the cases when GFI ClearView does not pick up traffic, the issue is the *host machine NIC not receiving any traffic*. To verify that the host NIC is receiving traffic, you can use a packet sniffing tool like Wireshark.

In the below image, we can see traffic on the "Ethernet" interface, confirming that the mirroring is working correctly.

Capture		
using this filter: 📙 Enter a capt	ture filter	
Ethernet	A . A	

It is also recommended to do a packet capture on the interface to ensure it's actual traffic from hosts, and not merely DNS, loopback, or other such requests. The below image shows an example from a working deployment:

	Lie Zien Zien Zo Zehner Busher Stephen Eine O O M.										
R hopiy a display filter <ctrl-></ctrl->											
lo.	Time	Source	Destination	Protocol	Length	info					
	139 1.259161	10.10.10.13	208.115.231.62	TCP	1466	35117 + 443	[ACK]	K] Seq=77236 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	140 1.259161	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=78648 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	141 1.259161	10.10.10.13	208.115.231.62	TLSv1.2	1000	Application	n Data,	a, Application Data			
	142 1.272926	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=81006 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	143 1.272926	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=82418 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	144 1.272926	10.10.10.13	208.115.231.62	TLSv1.2	471	Application	n Data	1			
	145 1.272926	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=84247 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	146 1.273319	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=85659 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	147 1.273319	10.10.10.13	208.115.231.62	TCP	1466	35117 → 443	[ACK]	K] Seq=87071 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	148 1.273319	10.10.10.13	208.115.231.62	TCP	1466	35117 + 443	[ACK]	K] Seq=88483 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			
	149 1.273319	10.10.10.13	208.115.231.62	TLSv1.2	633	Application	Data				
	150 1.296910	10.10.10.22	101.50.113.17	TCP	60	52279 + 80	[ACK]] Seq=1 Ack=1 Win=512 Len=1			
	151 1.296910	101.50.113.17	10.10.10.22	TCP	66	30 → 52279	[ACK]	Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2			
	152 1.325089	51.132.193.105	10.10.10.13	TCP	60	143 + 45069	[ACK]	K] Seq=1 Ack=1 Win=2051 Len=0			
	153 1.327315	10.10.10.13	51.132.193.105	TCP	60	TCP ACKed	unseen	en segment] 45069 → 443 [ACK] Seq=1 Ack=2 Win=1021 Len=0			
	154 1.446870	208.115.231.62	10.10.10.13	TCP	60	443 + 35117	7 [ACK]	K] Seq=3151 Ack=80060 Win=9966 Len=0			
	155 1.446870	208.115.231.62	10.10.10.13	TCP	60	443 → 35117	[ACK]	K] Seq=3151 Ack=81006 Win=9983 Len=0			
	156 1.450650	10.10.10.13	208.115.231.62	TCP	1466	35117 + 443	ACK]	K] Seq=90474 Ack=3151 Win=512 Len=1412 [TCP segment of a reassembled PDU]			

5 Verify that mirroring is enabled on the GFI ClearView port

In the GFI ClearView Web UI, navigate to **Configuration > System > Network > IP Address** tab. For the virtual adapter bridged to the host NIC with mirrored traffic (eth1 in the below example), ensure that the "Mirror" option is checked (click on *apply changes* if it was not checked earlier).

0		_							
Traffic Policies	NICs IP Address Routes DNS HTTP Proxy Email SNMP Active Directory	7							
Optimizer	Choose the mode of operation and enter IP Address and Netmask details for that mode. Also specify a Defr	r that mode. Also specify a Default Route.							
	Note: Take care when making changes here as this appliance may become unreachable.								
Objects	Groups [eth0]								
Network									
Users & Groups									
VLANs									
Protocols	Interface Settings	Interface Settings							
Applications	br0								
Schedules	Role: Cluster Mirror WCCP PBR								
Adaptive Response	Autoconf: IPv4: 🗹 DHCP IPv6: 🗌 SLAAC								
Service Levels	eth0 Dynamic Addresses: 192.168.49.128/24								
HTML Response	Static Addresses: /								
	Comment:								
System	Role: Cluster Z Mirror WCCP PBR								
Basic Install Wizard	Autoconf: IPv4: DHCP IPv6: SLAAC								
Network	eth1 Dynamic Addresses: fe80::20c:29ff;feb9:d12c/64								
Setup	Static Addresses: /								
Optimization	Comment:								
Certificates	Gateway Settings								
Authentication	IPv4:								
Logging	10, 6								

6 Verify that the management interface has access to the Internet

In the image in the previous step, ethO is the management interface. Please ensure that it is connected to a virtual adapter on the hypervisor with **internet access**. This ensures that the GFI ClearView can get its updates.

Conclusion

The troubleshooting steps should help with any deployment of GFI ClearView. It is important to remember that the mirroring setup is very straightforward from the ClearView appliance. In the majority of cases, the issue would result from the traffic not successfully getting mirrored from the switch to the host machine.

If you are still facing issues, please do not hesitate to create a ticket with our customer support team.

