Unveiling network intelligence:

Leveraging GFI ClearView for enhanced GFI KerioControl policies

GFI Software™

Introduction

In today's dynamic and interconnected digital landscape, effective network management and security have become paramount. The intricate interplay between gaining real-time insights into network activities and promptly translating those insights into decisive actions lies at the heart of modern cybersecurity. This document delves into a powerful symbiotic relationship between two cutting-edge solutions: GFI ClearView and GFI KerioControl.

Example use cases

Efficient bandwidth utilization hinges on two key actions:

1. Creating bandwidth thresholds for unrestricted traffic—be it user-specific or company-wide.
2. Establishing bandwidth reservations for mission-critical applications.

#1 Controlling throughput peaks by non-critical applications

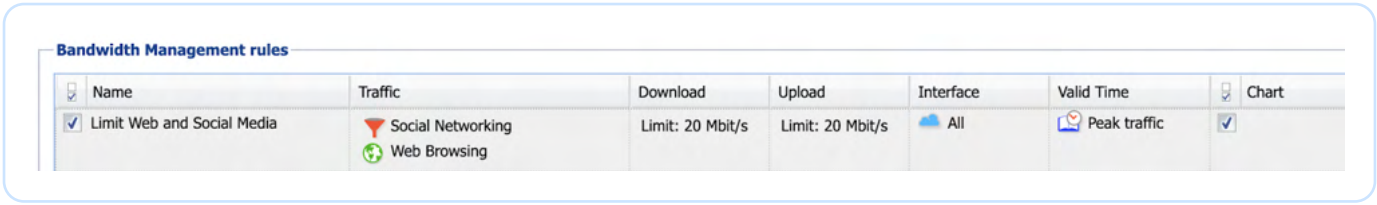
Top 30 Inbound Application Groups

Name [-] Hide Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows	RTT (ms)
GFI Products	1362698153	1919432.337	473.03	614040.34	1653	128
Social Networking	240479290	300250.544	933.77	29746.08	547	134
Web	446026750	206028.255	46.15	335043.23	17188	132

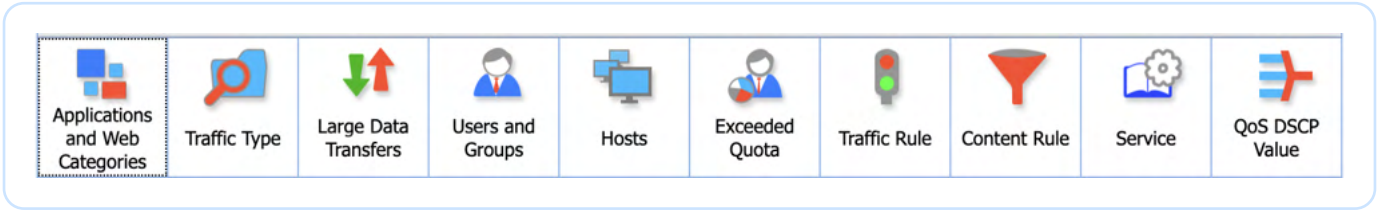
As depicted in the GFI ClearView image above, the top three inbound application groups exhibited peak throughput usage values as follows (throughput in kbps - maximum):

- 614 Mbps - GFI Products
- 29 Mbps - Social Networking
- 335 Mbps - Web

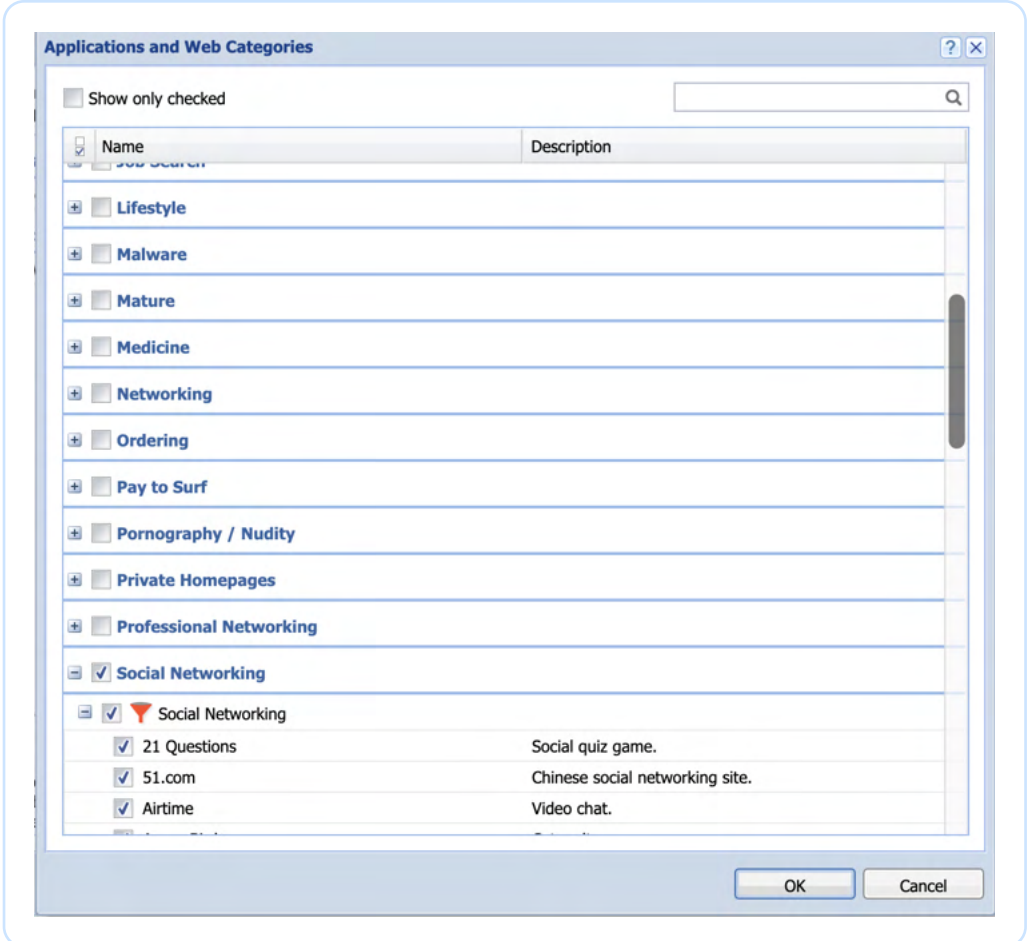
This indicates that during peak loads, critical applications might have suffered performance setbacks due to the load placed by these non-critical applications. To circumvent this, a QoS policy can be configured within KerioControl, especially during peak usage times. The following presents a sample policy:



It's important to note that while the above example showcases only three categories, a real-world environment would involve multiple application types. GFI KerioControl seamlessly manages such complexity, boasting the ability to identify thousands of applications and websites. It facilitates the creation of QoS policies across various categories.



Within the Application and Web Categories, you have over 140 categories (P2P, Streaming, Music, Television, social networking, etc.), each with dozens of individual applications and websites.



#1.1 Enhancing the above scenario

Often, instances of undesirable behavior—such as excessive social networking usage—stem from a handful of applications or users. GFI ClearView's interactive graphs empower deeper investigation into such behaviors. For instance, by clicking on "Social Networking," you can uncover specific problematic applications within that group and further identify users or hosts engaging excessively.

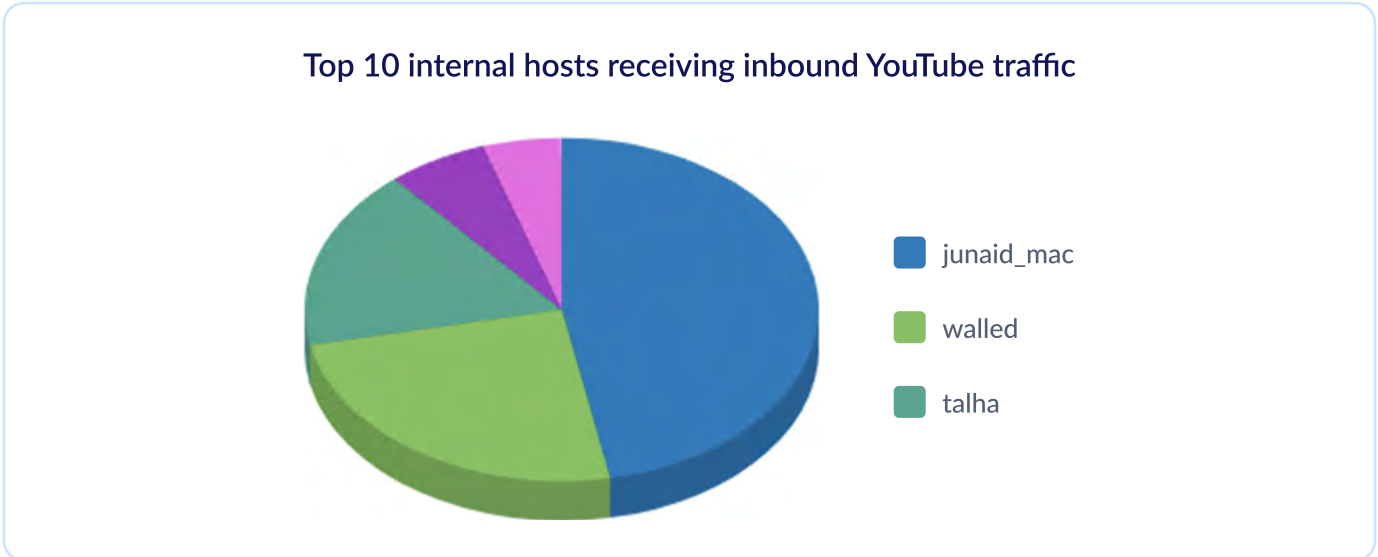
Top 30 Inbound Application Groups

Name [-] Hide Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows	RTT (ms)
GFI Products	1362698153	1919432.337	473.03	614040.34	1653	128
Social Networking	240479290	300250.544	933.77	29746.08	547	134
Web	446026750	206028.255	46.15	335043.23	17188	132

Top 30 Inbound Applications in Group Social Networking

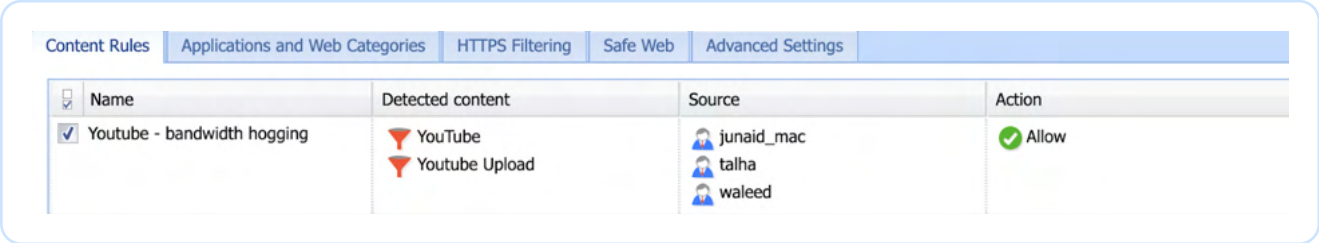
Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows
YouTube (udp)	240305670	300093.384	963.45	29746.08	464
Twitter	86144	52.228	5.42	1089.86	39
Snapchat (udp)	37443	49.479	506.17	3771.44	8
Instagram (udp)	39279	45.374	576.70	2323.03	5
LinkedIn	9090	8.754	60.19	845.84	18
Facebook Chat (udp)	707	0.792	51.10	119.90	5
Facebook	957	0.532	5.51	47.38	8

The data reveals that YouTube emerges as the primary contributor to spikes, accounting for 99% of social networking usage. A closer look reveals that 80% of this usage originates from just three users.

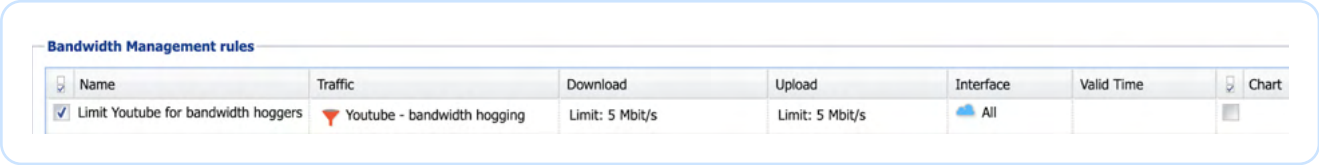


Given this scenario, creating a tailored policy for YouTube usage by these specific hosts within KerioControl can be achieved by following these steps:

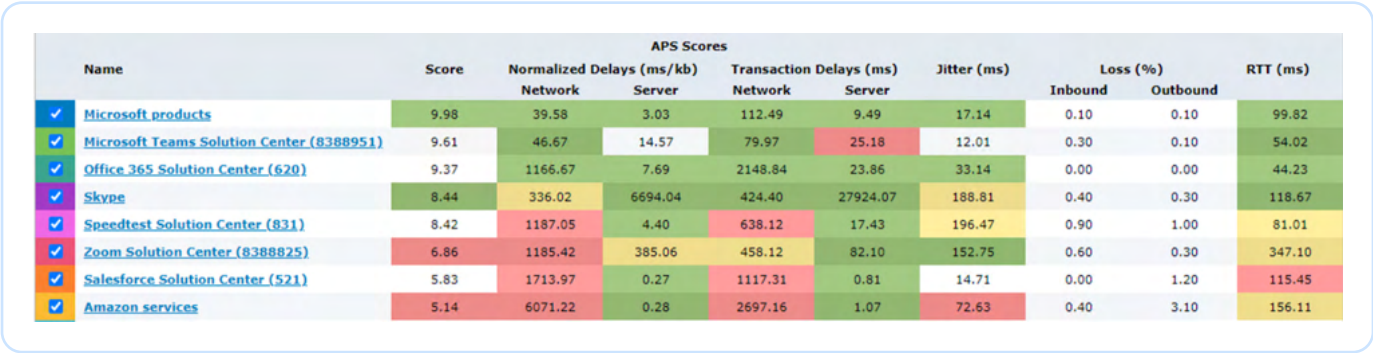
- Create a content filtering rule:



- Establish a corresponding QoS policy utilizing the previously devised content rule:

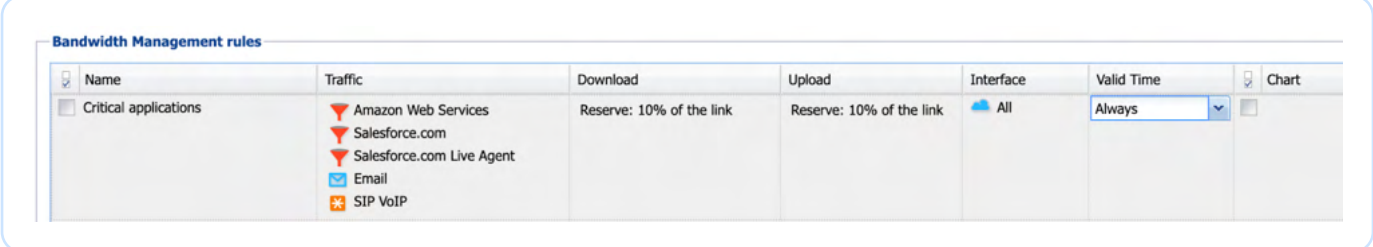


#2 Reserving throughput for critical applications



Name	Score	APS Scores: Normalized Delays (ms/kb) Network	Normalized Delays (ms/kb) Server	Transaction Delays (ms) Network	Transaction Delays (ms) Server	Jitter (ms)	Loss (%) Inbound	Loss (%) Outbound	RTT (ms)
Microsoft products	9.98	39.58	3.03	112.49	9.49	17.14	0.10	0.10	99.82
Microsoft Teams Solution Center (8388951)	9.61	46.67	14.57	79.97	25.18	12.01	0.30	0.10	54.02
Office 365 Solution Center (620)	9.37	1166.67	7.69	2148.84	23.86	33.14	0.00	0.00	44.23
Skype	8.44	336.02	6694.04	424.40	27924.07	188.81	0.40	0.30	118.67
Speedtest Solution Center (831)	8.42	1187.05	4.40	638.12	17.43	196.47	0.90	1.00	81.01
Zoom Solution Center (8388825)	6.86	1185.42	385.06	458.12	82.10	152.75	0.60	0.30	347.10
Salesforce Solution Center (521)	5.83	1713.97	0.27	1117.31	0.81	14.71	0.00	1.20	115.45
Amazon services	5.14	6071.22	0.28	2697.16	1.07	72.63	0.40	3.10	156.11

As depicted in the GFI ClearView image, Salesforce and Amazon services indicate subpar application performance, earning a 5 out of 10 rating. This can likely be attributed to insufficient available bandwidth during peak times, largely due to less critical applications consuming resources. Mitigate this concern by configuring a dedicated QoS policy within KerioControl:



Similarly, you can configure policies for other critical applications like Email, SIP VoIP traffic, video conferencing tools, etc. It is important to note that you can use this to reserve bandwidth for custom applications or services that you might be offering to the public as well. In such case, if you have a traffic rule performing NAT-ing for your DMZ, you can reserve bandwidth for all data that falls within that traffic rule.

Conclusion

Just as an orchestra requires both vision and execution to create a masterpiece, so too does network security demands the collaboration of these two exceptional solutions. GFI ClearView's watchful gaze identifies vulnerabilities and patterns, while GFI KerioControl's swift responses ensure that the network's rhythm remains unbroken. This dynamic duo not only safeguards against threats but also empowers administrators to orchestrate peak performance, ensuring a network that thrives under the spotlight.

Together, GFI ClearView and GFI KerioControl epitomize the synergy of insight and action, creating a safeguarded, high-performance network that stands as a testament to modern cybersecurity excellence.

Try GFI Clearview free for 30 Days