Exinda AI

GFI Exinda AI & Firewalls



GFI Software™

Document Navigation

Section	Page no.
1. Objective	3
2. Introduction	3
3. Similarities between GFI Exinda AI and Firewall	5
4. Comparison with GFI KerioControl	7
a. Visibility	7
i. GFI Exinda AI	8
ii. GFI KerioControl	10
b. Final Remarks	11

Objective

To cover different scenarios where GFI Exinda AI might be compared to a firewall and understand how and **why** the comparison is not realistic in most cases. We will first differentiate the features that are present only in GFI Exinda AI, and then go in-depth on the features that often overlap with firewalls and the position that can be taken in such scenarios.

Introduction

Looking at GFI Exinda AI from a higher level sometimes gives birth to the misconception that its functionality and purpose are similar to a firewall. However, the reality is entirely different. While a firewall's core purpose is to protect the network, GFI Exinda AI's objective is to optimize its performance to ensure the critical applications are performing efficiently. Since both items require dealing with similar protocols and traffic, firewalls and bandwidth shaping tools have some features that overlap - but neither can replace the other. In this whitepaper, we will explore why that is the case.

To take an example from a different IT domain, most of the mailserver solutions in the market have anti-virus, spam filters, archiving, and backup functionality available. But standalone gateway email security, archiving, and backup products still exist and are heavily used. The reason is that the mail server's core task is email communication, and not its security and redundancy. Therefore, while it includes those features at a surface level for added value, it is not nearly as robust as the products that are developed strictly for that purpose.

To approach this, there are two key verticals to cover:

- Features that are associated with GFI Exinda AI only.
- Features of GFI Exinda AI that are found in firewalls; however, they lack the depth.

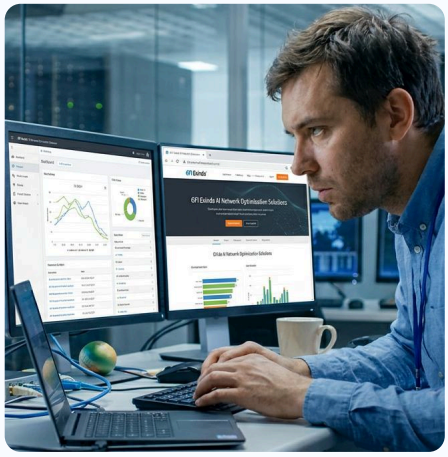
The below table gives a quick overview of that:

Feature	Firewall	GFI Exinda AI
Bandwidth Shaping	Partially	Yes
Acceleration	No	Yes
Edge Cache	Yes	Yes
Application Control	Partially	Yes
Visibility	Partially	Yes
Application Performance Monitoring	No	Yes

***Partially** = Some firewall vendors are offering features that touch this area, but not as deep as GFI Exinda AI does.*

Case 1

The following items, symptoms, or issues are seen in the customer's environment and they're looking for a product to solve it:



- Multiple branches that are interconnected - and acceleration is needed to virtually increase the bandwidth of the link between them.
- Critical applications are suffering and/or are not performing consistently at an optimal performance level.
- Customer already has a firewall in their environment.

In this case, GFI Exinda AI would very likely be a no-brainer for them, as it is a product that is dedicated to this purpose and the features within their firewall are not sufficient to perform this, and they're already aware of that; hence their research for a product to solve this problem for them.

In this scenario, there is a lower chance of coming across the "firewall has the needed visibility" question, but even if it does - Case # 2 provides a detailed position to take. However, they might be considering increasing their bandwidth. If so, the following reasoning might help clear the air:

- With a 10 Mbps connection, you download a file at ~ 1MBps speed.
- If you upgrade to a 100Mbps connection, you would be downloading the same file at 10MBps speed.
- Meaning, that no matter how much bandwidth you throw at the applications, they will continue to consume the maximum available amount. Hence, upgrading the bandwidth simply ignores the root cause of the issue i.e. unsanctioned application traffic and not isolating your business-critical applications.

Case 2



First off, we have to acknowledge that many firewalls are indeed offering functionalities that are quite similar to one of the core functions of GFI Exinda AI: Bandwidth shaping, Application Control, and Traffic Monitoring/Visibility. However, the **difference** is in the granularity and depth. All of that is linked to one key item: **Visibility**.

Visibility provides the information you need to **perform bandwidth shaping, performance optimization & traffic orchestration** in general. How well your network performs is dependent on the quality and granularity of information you have at hand. GFI Exinda AI provides deeper and more holistic visibility than any firewall in the market, for the reason that we discussed earlier: A firewall's core purpose is **not** network performance, **but** network security. Therefore, those features would always be *secondary* for the vendor.

Now that we have more clarity on the kinds of cases we might encounter, let's dive into the features that are *similar* and see how GFI Exinda AI goes a step further.

Similarities between GFI Exinda AI and Firewall

Visibility

Firewall vendors have connection details including the application being used, the source and destination IP addresses, and the user (if authenticated) for a specific connection or traffic, as well as traffic statistics for users specifically as well. **What value does GFI Exinda AI add over here?**

- The visibility provided by firewalls is limited, hence the insights that can be generated from them are shallow. **Let's take a real-world example:**

  Information: It has been raining almost every day for the last 60 days.

  Now try to answer the below questions with the above information:

  - Which days saw the highest rain volume?
  - Was there a pattern in terms of time for when it rained? For instance, it mostly rained during the afternoon hours?
  - For the days that it didn't rain, were they the same days across the 60-day period?
  - Was the rain observed across the whole city or just a specific area of the town?
  - Did the rain cause flooding or loss of critical services like electricity, etc. during any of these days?

  To associate the above with GFI Exinda AI's use case, just replace rain with network congestion and most of the above questions will make sense for that scenario as well.

- The above questions cannot be answered by the statement we saw because it lacked the granularity needed to generate valuable insights that could be used to predict future behavior, which brings us to our next point.

Bandwidth Shaping policies

Top-tier firewall vendors also have bandwidth-shaping policies available. You can reserve or limit it for an app, a user, a group of users, etc. So, what exactly does GFI Exinda AI do that justifies the cost?

Policies and strategies are formed based on data and insights. Yes, GFI Exinda AI provides more granularity in terms of the policies themselves too (more options to "configure" granular policies), but the real value doesn't lie there. It too is very closely integrated with the monitoring and visibility. See the below examples:

- The majority of rain usually occurs every day at 2 PM.
- Its volume gradually builds up till the afternoon with light showers in the morning, peaks at around 2 PM, and then starts to drop again.
- The peak rain times are mainly due to heavy rains in the Windows Updates and P2P areas of the city from Monday to Thursday. On Fridays, Social media town appears to be the main area hit by heavy rains.
- The rain in P2P, Windows updates town causes the Zoom and Office 365 town to flood as well.

The above information is actionable insight. You can generate **strong, reliable policies** based on that. So, it's not just the *flexibility and options* you have to add a policy but the **strength** of the policies, which is actually driven by the visibility and information you have.

Let's take a short network-based example to quickly understand this.

- GFI Exinda AI shows network congestion/peak usage frequently in the early morning.
- Zoom's performance score during those times is observed to drop to quite a low level.
- GFI Exinda AI's monitoring charts show:
  - Windows Updates Services start running across 10+ hosts each day in the morning times.
  - Three host machines generate a high amount of torrent traffic during that time.
  - Sales team has high Youtube data consumption during that time.
  - Development Team is generating high HTTP and FTP traffic during that time as well.
- Based on the above, further analysis shows:
  - Sales team's Youtube usage and Development Teams HTTP and FTP traffic usage is justified and critical during those times of the day.
  - Windows Update Services can be run during low activity times, or post-working hours as that is not critical.
  - Torrent traffic is undesirable and potentially illegal.
- Using the final insights above, you can form policies to:
  - Limit Windows Update Services during high network traffic hours and give them a bigger chunk during low network activity times, as this is not critical within your organization and can be delayed.
  - Block P2P traffic across all hosts within the network, or block it specifically for the hosts that have shown high usage.

Insights Generation

As discussed in the Visibility section, both firewall and GFI Exinda AI provide visibility into network activity. Firewall vendors however would not retain that data for a long period of time, as that is not their core function. GFI Exinda AI keeps data for up to 2 years. The value of that is significant - would it be wise to say that "it rained for the last two weeks on a Friday, so it will rain this Friday as well"? No. But, if the same pattern was observed over a longer period of time, say for the last six months, that would validate that it is a clear pattern and policies can be formed to react to it.

Application Performance Tracking

Most, if not all, firewall vendors do not have this feature. The reason is the same as the previous items, firewall tracks **threats, and security risks,** not **performance.** So, if you're only using a firewall, the first time you will know about a critical application performing badly would be directly from the **user.**

Additionally, while firewalls may be able to identify some applications, GFI Exinda AI's application inventory would very well be bigger, plus you can add custom L7 Application Signatures to identify any custom applications that might be used within your organization. The value it adds is that GFI Exinda AI can continuously track for you how your critical apps are performing - if it drops, you can quickly verify if it was an anomaly or a consistent behavior/drop, and react accordingly. This actually provides you with an opportunity to stop the problem in its tracks, rather than wait till it becomes unbearable and employee complaints start piling up.

Adaptive Response

Top-tier firewalls *can be expected* to have a basic version of adaptive response; however, GFI Exinda AI provides it with much more granularity – you can specify different alerts as well areas where you would like to put the limitations.

- Internet Download Manager, Torrent Clients, and other such bandwidth-hogging applications can take up the majority of the available bandwidth - no matter how much you expand your bandwidth, applications like these when running will continue to hog your bandwidth. Gigabytes of data can be downloaded over these apps in a very short span of time on high-speed connections.

  Result - during those sprees, critical applications will suffer.

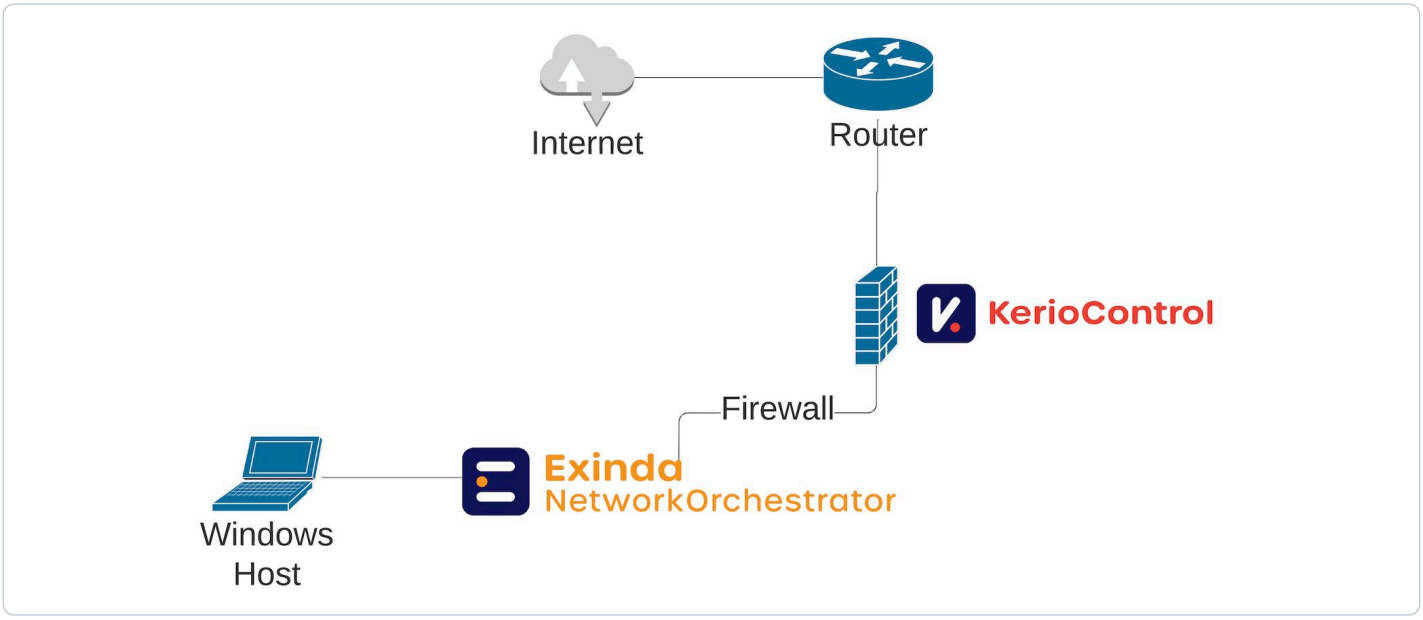
- Adaptive response can be used to set up policies like limiting traffic for a host if they transfer (up/down or both) 500MB of data in 1 minute (an indicator of bandwidth-hogging).
- Airports, cafes, and other public places specifically can leverage this quite well i.e. by generating a time-based limitation - free 100MB data for one hour only. To ensure that people don't sit all day there for free wifi, and/or perform activities that would slow the whole link.

Lastly, and this is very important: Firewall's core job is to protect against security breaches and threats. Adding the bandwidth shaping, visibility, and performance management overhead to it would drop its performance. This is also often seen across mailservers that are performing multiple purposes: spam filtering, archiving, virus scanning, attack protection, etc. Due to that, the best practice is to keep the mailserver separated from the protection aspect of email communications so that its performance is not impacted. Additionally, the gateway email security engine would be solely focused on the security aspect, hence would offer wider coverage in that area. Similarly, it is best to keep the firewall dedicated to the security aspect to ensure optimal performance of the firewall itself.

Comparison with GFI KerioControl

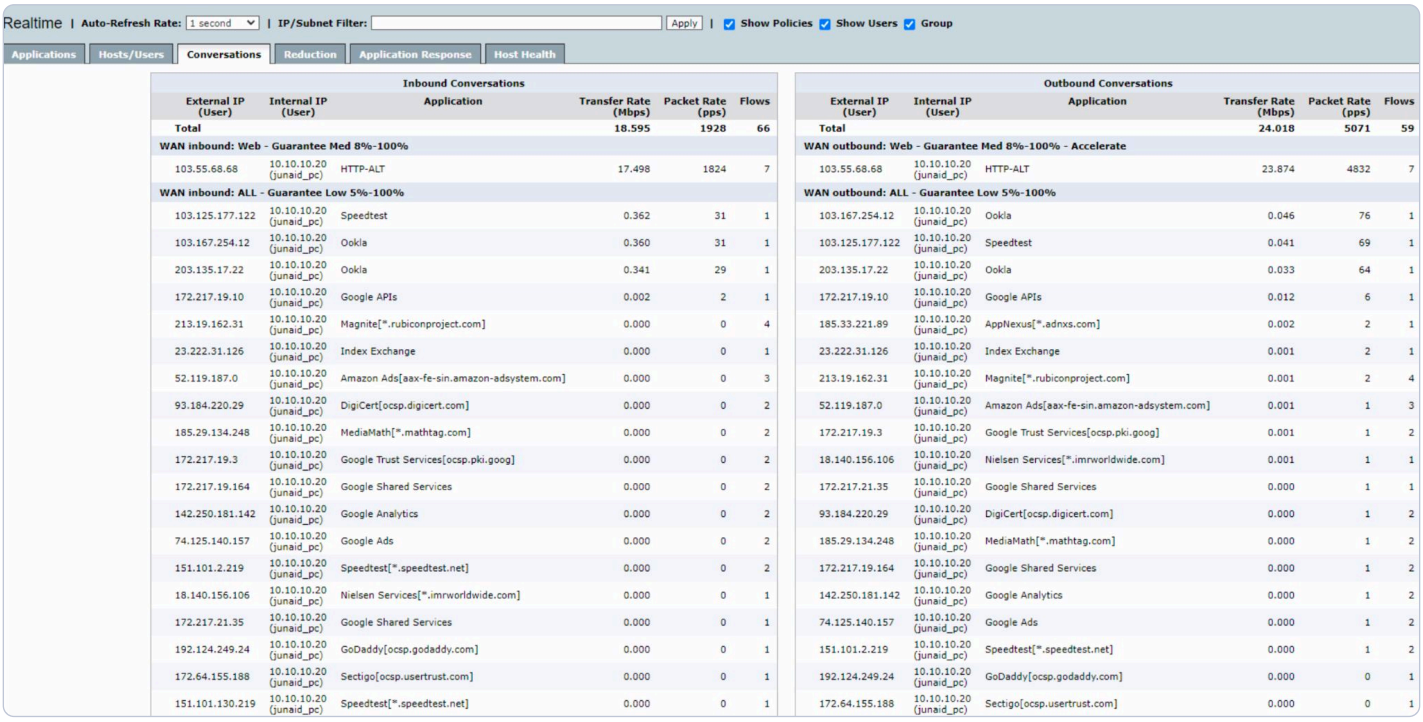
Visibility

To show the difference in visibility that GFI Exinda AI provides in comparison to the GFI KerioControl firewall, we will generate some traffic in a network that has both and show the insights both deliver for the same traffic. Below is what the network architecture roughly looks like.



Visiting a website and running a SpeedTest on a host machine for 1 minute generates the following statistics within GFI Exinda AI and the GFI KerioControl firewall. It is clear that GFI Exinda AI is able to capture the background traffic being generated by the host e.g. Google Shared Services, third-party requests/traffic generated by the website visit (great for identifying shadow apps too), etc; whereas, the info available through the firewall is at a very basic level. It also does not go a step further to use that data from different dimensions to be able to generate insights. See the screenshots below.

GFI Exinda AI



Realtime | Auto-Refresh Rate: 1 second | IP/Subnet Filter: Apply | Show Policies Show Users Group

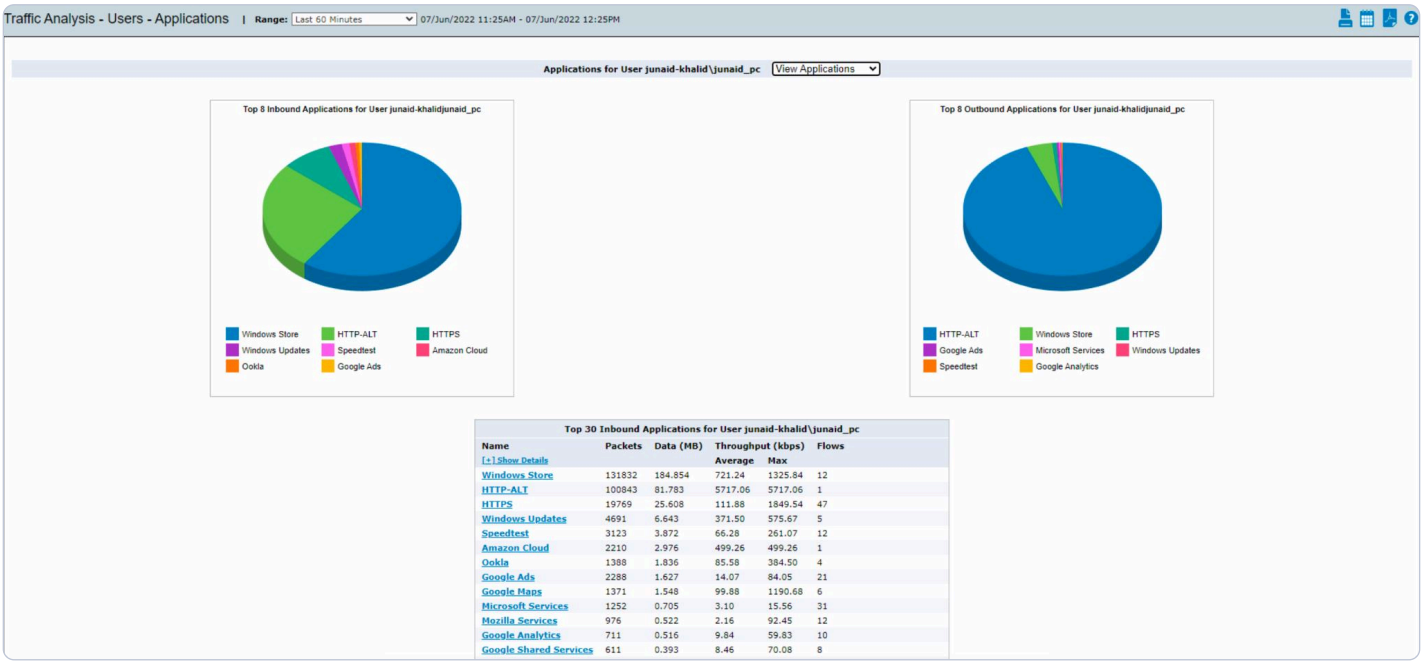
Applications | Hosts/Users | Conversations | Reduction | Application Response | Host Health

Inbound Conversations

External IP (User)	Internal IP (User)	Application	Transfer Rate (Mbps)	Packet Rate (pps)	Flows
Total			**18.595**	**1928**	**66**
WAN inbound: Web - Guarantee Med 8%-100%					
103.55.68.68	10.10.10.20 (junaid_pc)	HTTP-ALT	17.498	1824	7
WAN inbound: ALL - Guarantee Low 5%-100%					
103.125.177.122	10.10.10.20 (junaid_pc)	Speedtest	0.362	31	1
103.167.254.12	10.10.10.20 (junaid_pc)	Ookla	0.360	31	1
203.135.17.22	10.10.10.20 (junaid_pc)	Ookla	0.341	29	1
172.217.19.10	10.10.10.20 (junaid_pc)	Google APIs	0.002	2	1
213.19.162.31	10.10.10.20 (junaid_pc)	Magnite[*.rubiconproject.com]	0.000	0	4
23.222.31.126	10.10.10.20 (junaid_pc)	Index Exchange	0.000	0	1
52.119.187.0	10.10.10.20 (junaid_pc)	Amazon Ads[aax-fe-sin.amazon-adsystem.com]	0.000	0	3
93.184.220.29	10.10.10.20 (junaid_pc)	DigiCert[ocsp.digicert.com]	0.000	0	2
185.29.134.248	10.10.10.20 (junaid_pc)	MediaMath[*.mathtag.com]	0.000	0	2
172.217.19.3	10.10.10.20 (junaid_pc)	Google Trust Services[ocsp.pki.goog]	0.000	0	2
172.217.19.164	10.10.10.20 (junaid_pc)	Google Shared Services	0.000	0	2
142.250.181.142	10.10.10.20 (junaid_pc)	Google Analytics	0.000	0	2
74.125.140.157	10.10.10.20 (junaid_pc)	Google Ads	0.000	0	2
151.101.2.219	10.10.10.20 (junaid_pc)	Speedtest[*.speedtest.net]	0.000	0	2
18.140.156.106	10.10.10.20 (junaid_pc)	Nielsen Services[*.imrworldwide.com]	0.000	0	1
172.217.21.35	10.10.10.20 (junaid_pc)	Google Shared Services	0.000	0	1
192.124.249.24	10.10.10.20 (junaid_pc)	GoDaddy[ocsp.godaddy.com]	0.000	0	1
172.64.155.188	10.10.10.20 (junaid_pc)	Sectigo[ocsp.usertrust.com]	0.000	0	1
151.101.130.219	10.10.10.20 (junaid_pc)	Speedtest[*.speedtest.net]	0.000	0	1

Outbound Conversations

External IP (User)	Internal IP (User)	Application	Transfer Rate (Mbps)	Packet Rate (pps)	Flows
Total			**24.018**	**5071**	**59**
WAN outbound: Web - Guarantee Med 8%-100% - Accelerate					
103.55.68.68	10.10.10.20 (junaid_pc)	HTTP-ALT	23.874	4832	7
WAN outbound: ALL - Guarantee Low 5%-100%					
103.167.254.12	10.10.10.20 (junaid_pc)	Ookla	0.046	76	1
103.125.177.122	10.10.10.20 (junaid_pc)	Speedtest	0.041	69	1
203.135.17.22	10.10.10.20 (junaid_pc)	Ookla	0.033	64	1
172.217.19.10	10.10.10.20 (junaid_pc)	Google APIs	0.012	6	1
185.33.221.89	10.10.10.20 (junaid_pc)	AppNexus[*.adnxs.com]	0.002	2	1
23.222.31.126	10.10.10.20 (junaid_pc)	Index Exchange	0.001	2	1
213.19.162.31	10.10.10.20 (junaid_pc)	Magnite[*.rubiconproject.com]	0.001	2	4
52.119.187.0	10.10.10.20 (junaid_pc)	Amazon Ads[aax-fe-sin.amazon-adsystem.com]	0.001	1	3
172.217.19.3	10.10.10.20 (junaid_pc)	Google Trust Services[ocsp.pki.goog]	0.001	1	2
18.140.156.106	10.10.10.20 (junaid_pc)	Nielsen Services[*.imrworldwide.com]	0.001	1	1
172.217.21.35	10.10.10.20 (junaid_pc)	Google Shared Services	0.000	1	1
93.184.220.29	10.10.10.20 (junaid_pc)	DigiCert[ocsp.digicert.com]	0.000	1	2
185.29.134.248	10.10.10.20 (junaid_pc)	MediaMath[*.mathtag.com]	0.000	1	2
172.217.19.164	10.10.10.20 (junaid_pc)	Google Shared Services	0.000	1	2
142.250.181.142	10.10.10.20 (junaid_pc)	Google Analytics	0.000	1	2
74.125.140.157	10.10.10.20 (junaid_pc)	Google Ads	0.000	1	2
151.101.2.219	10.10.10.20 (junaid_pc)	Speedtest[*.speedtest.net]	0.000	1	2
192.124.249.24	10.10.10.20 (junaid_pc)	GoDaddy[ocsp.godaddy.com]	0.000	0	1
172.64.155.188	10.10.10.20 (junaid_pc)	Sectigo[ocsp.usertrust.com]	0.000	0	1



Traffic Analysis - Users - Applications | Range: Last 60 Minutes 07/Jun/2022 11:25AM - 07/Jun/2022 12:25PM

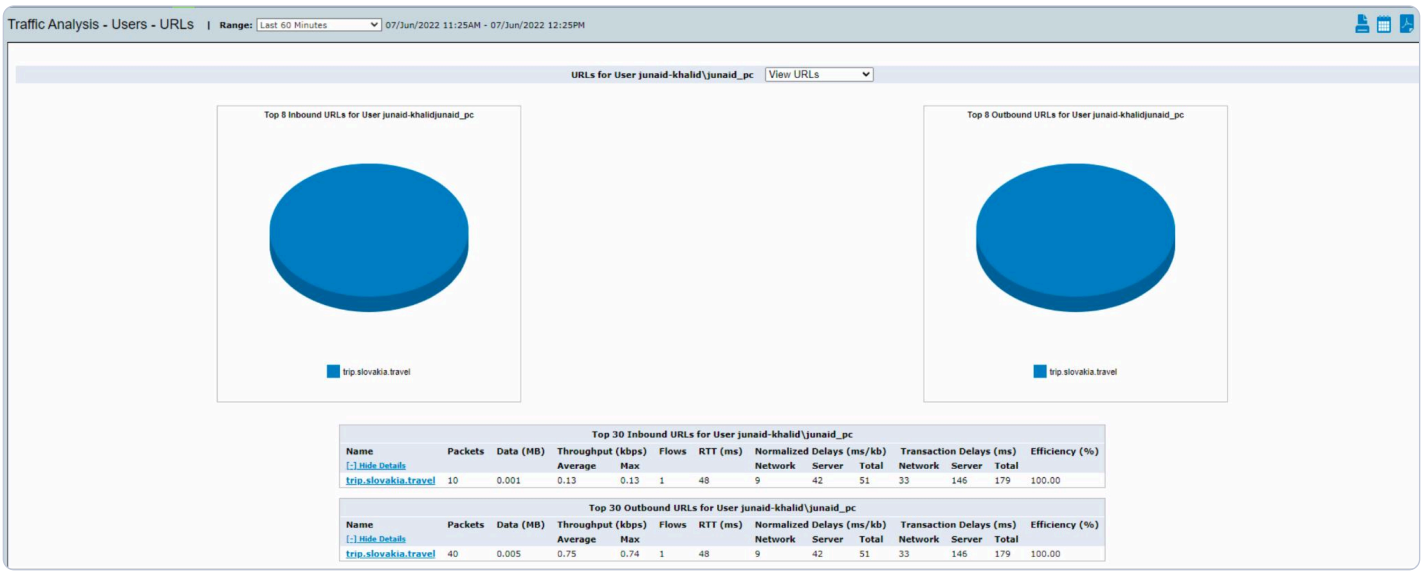
Applications for User junaid-khalid\junaid_pc View Applications

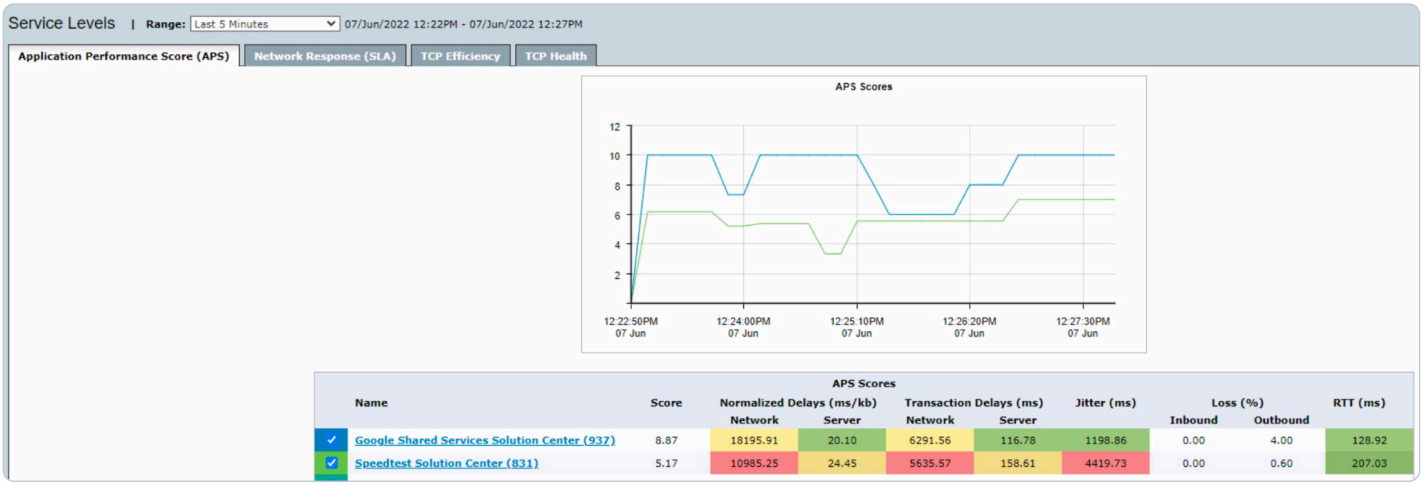
Top 8 Inbound Applications for User junaid-khalidjunaid_pc

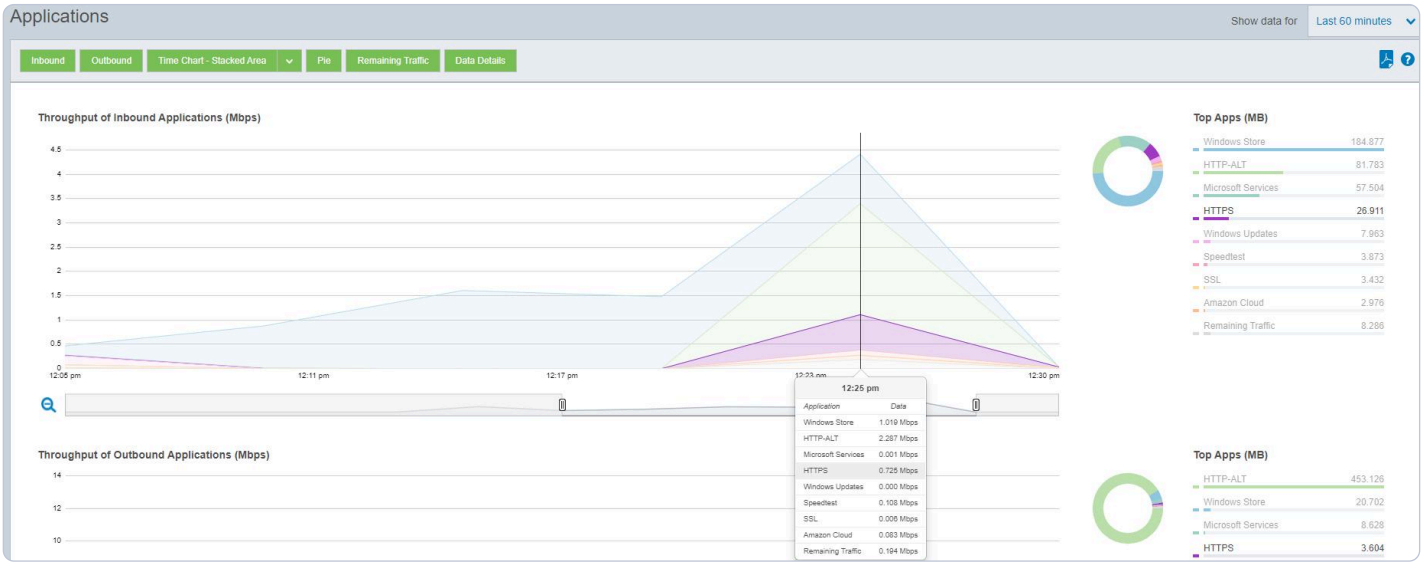
Top 8 Outbound Applications for User junaid-khalidjunaid_pc

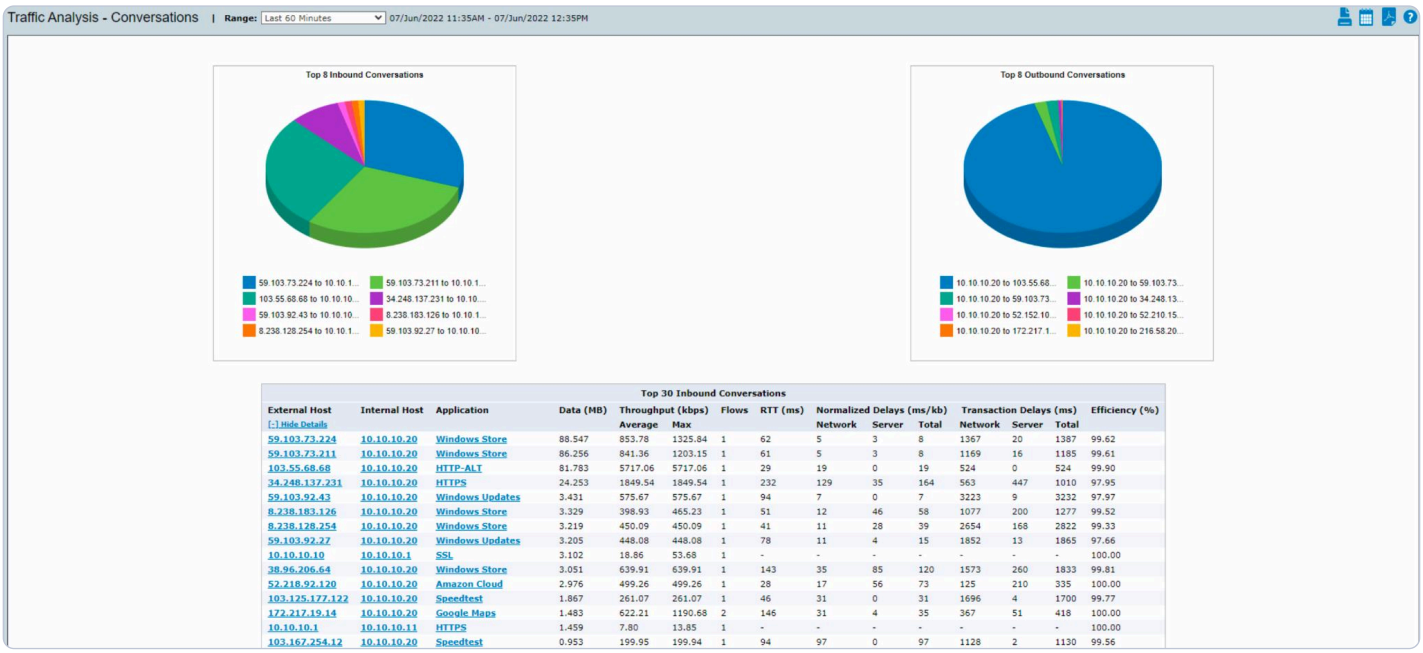
Top 30 Inbound Applications for User junaid-khalid\junaid_pc

Name	Packets	Data (MB)	Throughput (kbps)		Flows
[+] Show Details			Average	Max	
Windows Store	131832	184.854	721.24	1325.84	12
HTTP-ALT	100843	81.783	5717.06	5717.06	1
HTTPS	19769	25.608	111.88	1849.54	47
Windows Updates	4691	6.643	371.50	575.67	5
Speedtest	3123	3.872	66.28	261.07	12
Amazon Cloud	2210	2.976	499.26	499.26	1
Ookla	1388	1.836	85.58	384.50	4
Google Ads	2288	1.627	14.07	84.05	21
Google Maps	1371	1.548	99.88	1190.68	6
Microsoft Services	1252	0.705	3.10	15.56	31
Mozilla Services	976	0.522	2.16	92.45	12
Google Analytics	711	0.516	9.84	59.83	10
Google Shared Services	611	0.393	8.46	70.08	8


Traffic Analysis - Users - URLs
Range: Last 60 Minutes
07/Jun/2022 11:25AM - 07/Jun/2022 12:25PM
URLs for User junaid-khalid\junaid_pc
View URLs
Top 8 Inbound URLs for User junaid-khalidjunaid_pc
trip.slovakia.travel
Top 8 Outbound URLs for User junaid-khalidjunaid_pc
trip.slovakia.travel
Top 30 Inbound URLs for User junaid-khalid\junaid_pc
Name Packets Data (MB) Throughput (kbps) Average Max Flows RTT (ms) Normalized Delays (ms/kb) Network Server Total Transaction Delays (ms) Network Server Total Efficiency (%)
[-] Hide Details
trip.slovakia.travel 10 0.001 0.13 0.13 1 48 9 42 51 33 146 179 100.00
Top 30 Outbound URLs for User junaid-khalid\junaid_pc
Name Packets Data (MB) Throughput (kbps) Average Max Flows RTT (ms) Normalized Delays (ms/kb) Network Server Total Transaction Delays (ms) Network Server Total Efficiency (%)
[-] Hide Details
trip.slovakia.travel 40 0.005 0.75 0.74 1 48 9 42 51 33 146 179 100.00


Service Levels
Range: Last 5 Minutes
07/Jun/2022 12:22PM - 07/Jun/2022 12:27PM
Application Performance Score (APS)
Network Response (SLA)
TCP Efficiency
TCP Health
APS Scores
12
10
8
6
4
2
12:22:50PM 07 Jun
12:24:00PM 07 Jun
12:25:10PM 07 Jun
12:26:20PM 07 Jun
12:27:30PM 07 Jun
APS Scores
Name Score Normalized Delays (ms/kb) Network Server Transaction Delays (ms) Network Server Jitter (ms) Loss (%) Inbound Outbound RTT (ms)
Google Shared Services Solution Center (937) 8.87 18195.91 20.10 6291.56 116.78 1198.86 0.00 4.00 128.92
Speedtest Solution Center (831) 5.17 10985.25 24.45 5635.57 158.61 4419.73 0.00 0.60 207.03

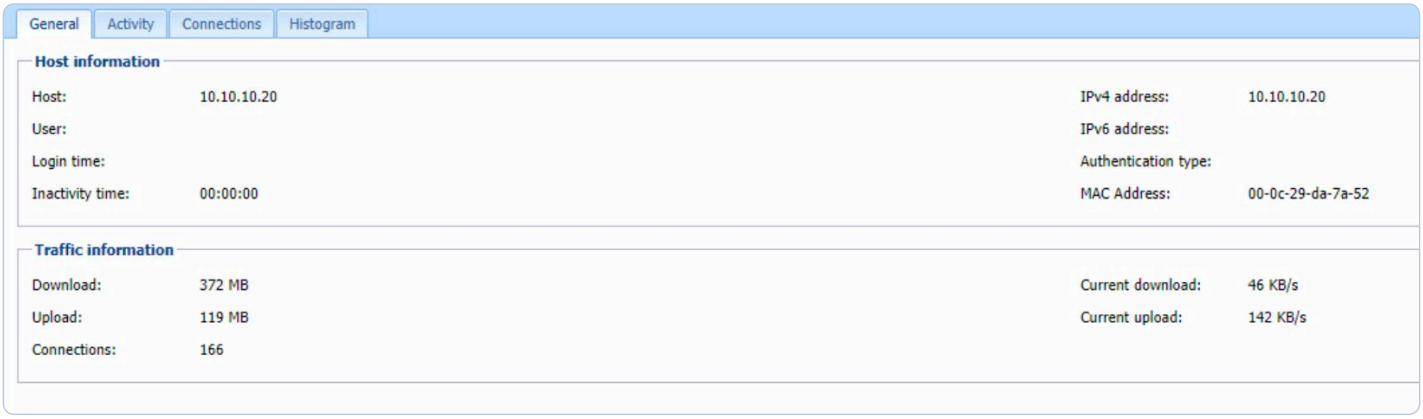

Applications
Show data for Last 60 minutes
Inbound
Outbound
Time Chart - Stacked Area
Pie
Remaining Traffic
Data Details
Throughput of Inbound Applications (Mbps)
12:05 pm
12:11 pm
12:17 pm
12:30 pm
12:25 pm
Application Data
Windows Store 1.019 Mbps
HTTP-ALT 2.287 Mbps
Microsoft Services 0.001 Mbps
HTTPS 0.725 Mbps
Windows Updates 0.000 Mbps
Speedtest 0.108 Mbps
SSL 0.006 Mbps
Amazon Cloud 0.083 Mbps
Remaining Traffic 0.194 Mbps
Top Apps (MB)
Windows Store 184.877
HTTP-ALT 81.783
Microsoft Services 57.504
HTTPS 26.911
Windows Updates 7.963
Speedtest 3.873
SSL 3.432
Amazon Cloud 2.976
Remaining Traffic 8.286
Throughput of Outbound Applications (Mbps)
Top Apps (MB)
HTTP-ALT 453.126
Windows Store 20.702
Microsoft Services 8.628
HTTPS 3.604

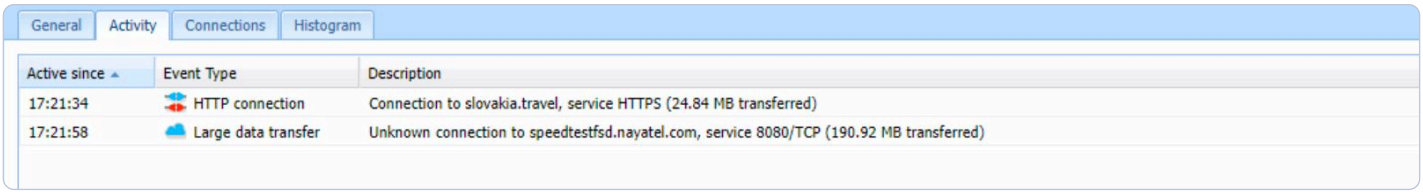


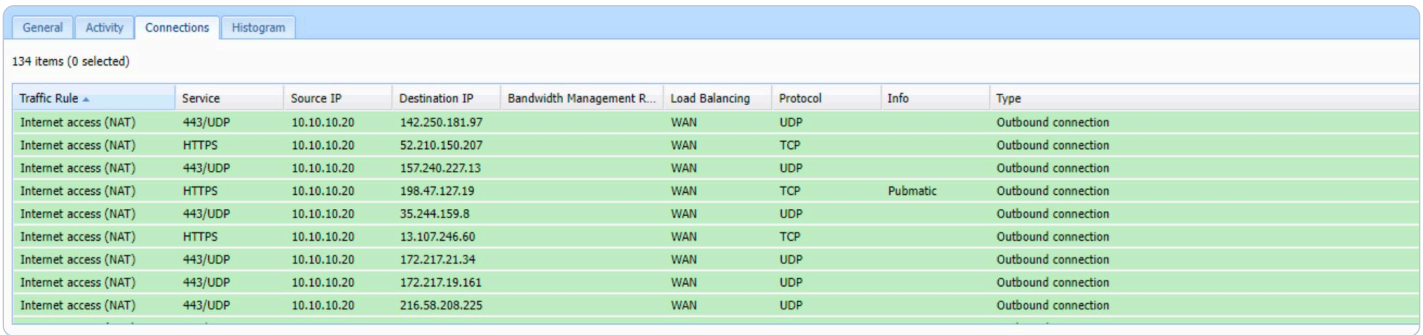
External Host [-] Hide Details	Internal Host	Application	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows	RTT (ms)	Normalized Delays (ms/kb) Network	Normalized Delays (ms/kb) Server	Normalized Delays (ms/kb) Total	Transaction Delays (ms) Network	Transaction Delays (ms) Server	Transaction Delays (ms) Total	Efficiency (%)
59.103.73.224	10.10.10.20	Windows Store	88.547	853.78	1325.84	1	62	5	3	8	1367	20	1387	99.62
59.103.73.211	10.10.10.20	Windows Store	86.256	841.36	1203.15	1	61	5	3	8	1169	16	1185	99.61
103.55.68.68	10.10.10.20	HTTP-ALT	81.783	5717.06	5717.06	1	29	19	0	19	524	0	524	99.90
34.248.137.231	10.10.10.20	HTTPS	24.253	1849.54	1849.54	1	232	129	35	164	563	447	1010	97.95
59.103.92.43	10.10.10.20	Windows Updates	3.431	575.67	575.67	1	94	7	0	7	3223	9	3232	97.97
8.238.183.126	10.10.10.20	Windows Store	3.329	398.93	465.23	1	51	12	46	58	1077	200	1277	99.52
8.238.128.254	10.10.10.20	Windows Store	3.219	450.09	450.09	1	41	11	28	39	2654	168	2822	99.33
59.103.92.27	10.10.10.20	Windows Updates	3.205	448.08	448.08	1	78	11	4	15	1852	13	1865	97.66
10.10.10.10	10.10.10.1	SSL	3.102	18.86	53.68	1	-	-	-	-	-	-	-	100.00
38.96.206.64	10.10.10.20	Windows Store	3.051	639.91	639.91	1	143	35	85	120	1573	260	1833	99.81
52.218.92.120	10.10.10.20	Amazon Cloud	2.976	499.26	499.26	1	28	17	56	73	125	210	335	100.00
103.125.177.122	10.10.10.20	Speedtest	1.867	261.07	261.07	1	46	31	0	31	1696	4	1700	99.77
172.217.19.14	10.10.10.20	Google Maps	1.483	622.21	1190.68	2	146	31	4	35	367	51	418	100.00
10.10.10.1	10.10.10.11	HTTPS	1.459	7.80	13.85	1	-	-	-	-	-	-	-	100.00
103.167.254.12	10.10.10.20	Speedtest	0.953	199.95	199.94	1	94	97	0	97	1128	2	1130	99.56

GFI Exinda AI is able to show all the connections to different servers for the Speedtest application and is also able to provide TCP efficiency for it. Furthermore, from a quick look, it can tell how well the application is performing on a scale of 1 to 10.

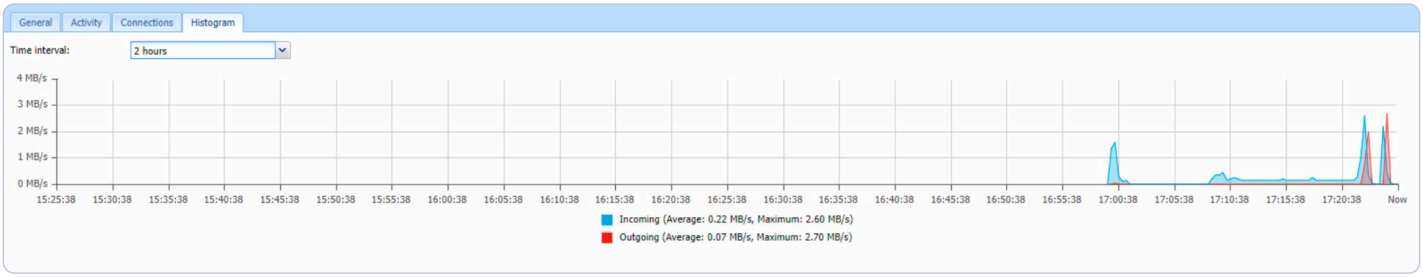
GFI KerioControl







Traffic Rule	Service	Source IP	Destination IP	Bandwidth Management R...	Load Balancing	Protocol	Info	Type
Internet access (NAT)	443/UDP	10.10.10.20	142.250.181.97		WAN	UDP		Outbound connection
Internet access (NAT)	HTTPS	10.10.10.20	52.210.150.207		WAN	TCP		Outbound connection
Internet access (NAT)	443/UDP	10.10.10.20	157.240.227.13		WAN	UDP		Outbound connection
Internet access (NAT)	HTTPS	10.10.10.20	198.47.127.19		WAN	TCP	Pubmatic	Outbound connection
Internet access (NAT)	443/UDP	10.10.10.20	35.244.159.8		WAN	UDP		Outbound connection
Internet access (NAT)	HTTPS	10.10.10.20	13.107.246.60		WAN	TCP		Outbound connection
Internet access (NAT)	443/UDP	10.10.10.20	172.217.21.34		WAN	UDP		Outbound connection
Internet access (NAT)	443/UDP	10.10.10.20	172.217.19.161		WAN	UDP		Outbound connection
Internet access (NAT)	443/UDP	10.10.10.20	216.58.208.225		WAN	UDP		Outbound connection



Even though the core traffic generated intentionally was via SpeedTest and slovakia.travel website, GFI Exinda AI shows that the majority of the bandwidth was actually consumed by the Windows Store and Services instead. Assuming there was network congestion faced at the said time, a firewall would have shown a clouded/foggy image of the network activities, hence the remediation action taken would have been weak.

That said, KerioControl is for SMB-market and its visibility cannot be compared with other enterprise-grade firewalls; those are expected to have a higher level of visibility than it. Nonetheless, based on what we have seen in product comparisons, none has the level of visibility that GFI Exinda AI offers.

Final Remarks

Firewall's key objective is network security; whereas, for GFI Exinda AI its network's performance (i.e. performance of the applications or network services). Since both process network traffic, it makes sense for vendors in each to offer some functionalities that overlap, likely added specifically for customers that only require those features at a surface level. `

GFI Exinda AI provides the ability to drop/block traffic using policies, which is essentially a feature of a firewall; however, it cannot replace a firewall because a firewall does much more than that. Similarly, the firewall can assist you in bandwidth management, but it cannot replace GFI Exinda AI, as it offers far more visibility and performance-related metrics and features.

To sum it up, the two products are complementary to each other, rather than direct competitors. It is advisable to use a firewall in tandem with GFI Exinda AI to ensure that your network is not only performing optimally but is also secure, and vice versa.

Try a GFI Exinda AI Demo free for 30 Days

Copyright © GFI USA, LLC, All rights reserved.