PRODUCT REVIEW

Kerio Control

Reviewed by Brien M. Posey





Introduction

Network security tools are notorious for being complex. Many such tools require a steep learning curve, even for seasoned IT pros. However, GFI is bucking the trend with its Kerio Control. Kerio Control is a comprehensive network security application for the SMB, that has been specifically designed to be easy to use.

O1 The Deployment Process

Kerio Control can be downloaded as an ISO file, or as a VMware or Hyper-V virtual appliance (physical appliances are also available). For this review, I opted to use the Hyper-V option. The download consisted of a virtual hard disk file (in VHD format). I simply created a Hyper-V virtual machine, and then attached the VHD file.

Once the VM had been set up, I booted it and was presented with a message telling me where to point my browser in order to access the administrative interface. If you look at the figure below, you can see that there is a message stating that you can press Enter to access the console. I used this option so that I could assign the VM an IP address that fell within the range used on my virtual network.

When I opened a Web browser on another machine and navigated to the specified URL, I was presented with the server's Activation Wizard. The activation process consisted of specifying a language, accepting the license agreement, and setting an initial password.

Once I had completed the Activation Wizard, I was taken to the Configuration Assistant. As you can see in the figure below, the Configuration Assistant helps with all of the initial configuration tasks, such as registering your license and configuring Internet connectivity. I found the process of configuring Internet connectivity and registering the product to be simple and intuitive.

With Kerio Control fully configured, I decided to turn my attention to its firewall. The Kerio Control firewall can be configured through a series of traffic rules. One thing that I especially like about Kerio Control, is that it displays the traffic rules in a simple and unambiguous way that should make sense to anyone who has basic networking knowledge. You



This is the screen that you see when you boot Kerio Control.



The Configuration Assistant helps with the initial configuration tasks.

definitely don't need to be a networking expert to configure the traffic rules. In fact, the most essential rules exist by default. GFI even went so far as to color code the rules to help illustrate what they do. You can see the traffic rules in the figure below.

Ē.	🗄 📋 Traffic Rules - Kerio Con 🗙 🗏	+ `	/										-	0)	
\leftarrow	O ŵ A Certificate error https://192.168.0.10/admin/#trafficRules D ŵ														
	🖂 Dashboard 🍦 🔋 Traffic Rules											Admir			
\Diamond	Interfaces		Search: 🖉 🗍 🐨 Test Rules 🖓 Restore View												
	🖡 Traffic Rules		Rame		Source	Destination	Service	IP version	Action	Translation	Last used	Valid Time			
الد الد	Intrusion Prevention		Remote administration	💬 👛 Internet Interface	Internet Interfaces	💙 Firewall	2 TCP 4081	Any	Allow						
	🕐 Security Settings	_		VPN Services		Any	💙 Firewall	IPsec services	Any	Allow					
	Bandwidth Management and QoS		Web Services		Any	💙 Firewall	() HTTP	Any	Allow						
F	Y Content Filter	- Web Service			A iiy	Vincence	6 HTTPS	,							
	Proxy Server		Internet access (NAT)	Trusted/Local Interfac Guest Interfaces VPN clients	. 👛 Internet Interfaces	Any	Any	Allow	NAT Balancing per host	22 minutes ago					
	🔗 Antivirus														
	PHCP Server		V Local traffic		🗸 💙 Firewall	💙 Firewall	Any	Any	Allow		just now				
	🔁 IPv6 Router Advertisements			me Trusted/Local Interfac.	📹 Trusted/Local Interfac Contents										
	🚠 DNS				All VPN tunnels	All VPN tunnels									
	迄 Routing Table		Firewall traffic		🗘 💙 Firewall	Any	Any	Any	Allow		just now				
	log Accounting and Monitoring		Guests traffic		Guest Interfaces	💙 Firewall	Guest services	Any	Allow						
			Block other traffic		Any	Any	Any	Any	😮 Drop		just now				
	Advanced Options														
	igh Availability														
	Users and Groups														
	Users														
	and Groups														
_	졅 Domains and User Login														
KerioControl	Definitions														
	SSL Certificates														
	🛃 IP Address Groups														
×	🕵 URL Groups														
	🚫 Time Ranges		Add Remove	More	Actions -							Apply	Rese	t.	

These are the default traffic rules that are built into Kerio Control.

Because these rules exist by default, I didn't have to do anything special to make Kerio Control function as a NAT router. Once I configured the machines on my test network to use the Kerio Control server as a default gateway, those machines received Internet access without any issues.

02 Anti-Virus

One of Kerio Control's most noteworthy features is its antivirus capabilities. Whereas legacy antivirus products often focus on scanning files to determine whether or not they contain malicious code, Kerio Control is able to scan network traffic. As you can see in the next figure, Kerio Control is able to scan both HTTP and FTP traffic. Additionally, the software can check inbound email for malware through SMTP and POP3 protocol scanning.

	🖂 Dashboard	â 🥔 Antivirus	Admin -
	📰 Interfaces	Kerio Antivirus HTTP, FTP Scanning Email Scanning	
	🖡 Traffic Rules	Antivirus	
*	intrusion Prevention	V Use Kerio Antivirus	
	🕐 Security Settings	🕗 The antivirus is running.	
at	⇒ Bandwidth Management and QoS	Updates	
Ð	Y Content Filter	Check for update every 8 hours Update Now	T
E -	Proxy Server	Last update check: 2 hours ago	Bitdefender
\bigcirc	i Antivirus	Current virus database updated: 2 hours ago Threat definitions count: 12928389	
Ŭ	DHCP Server		
-	R IPv6 Router Advertisements	Protocols	
-		Enable HTTP scanning To Enable FTP scanning	
	Routing Table	Enable SMTP scanning (for inbound connections only)	
		SHTP scanning is not compatible with grey/isting.	
	Accounting and Monitoring	C Enable POP3 scanning	
-	Remote Services	Settings	
	Advanced Options	☑ Scan only files that are smaller than:	
	幊 High Availability	4096 KB	
	Users and Groups		
	🧟 Users		
	angle Groups		
Kerio Control	🚁 Domains and User Login		
	Definitions		
	🖹 SSL Certificates		
	📑 IP Address Groups		
	🕵 URL Groups		
	🕑 Time Ranges	v	Apply Reset

Kerio Control is able to perform network level malware scanning.

03 Web Content Filtering

Another key capability found within Kerio Control is its ability to filter Web content. The content filter interface is nearly identical to the interface used for managing traffic rules, but allows admins to regulate the types of Internet traffic that are and are not allowed within the organization. As you can see in the next figure for example, Kerio Control is configured by default to block advertisements and banners, audio and video files, peer to peer traffic, and traffic related to hacking and malware. As such, the content rules are not merely designed to prevent users from accessing inappropriate content, but they can also be used as a tool for shielding the organization from attack.

	📉 Dashboard	Content Filter					Admin		
	Interfaces	nterfaces Content Rules Applications and Web Categories HTTPS Filtering Safe Web Advanced Settings							
	🕴 Traffic Rules	8 Name	Detected content	Source	Action	Valid Time			
*	힌 Intrusion Prevention	Kerio sites	Skerio.com	Any	🕗 Allow				
al	🔭 Security Settings				💠 Additional settings				
	⇒ Bandwidth Management and QoS	Advertisements and banners	Ads/banners	Any	😮 Drop				
	Y Content Filter	Updates and MS Windows activ	Automatic Updates	Any	Allow Additional settings				
-	👽 Proxy Server	Kerio Control Web Filter catego		Any	🔁 Deny 💠 Additional settings				
	🥔 Antivirus		Gonet Command and Control Centers Compromised Criminal Skills Hacking Malware Call-Home Malware Oldribution Point Phishing/Fraud and 3 more						
	P DHCP Server								
	😢 IPv6 Router Advertisements	Audio and video files Peer-to-Peer traffic							
	🚠 DNS						*		
	💺 Routing Table								
	Accounting and Monitoring		Audio files Video files	Any	Deny Additional settings				
	Remote Services								
	😥 Advanced Options		Peer-to-Peer	Any	🔁 Deny 💠 Additional settings				
	啦 High Availability	Allow other traffic	P Any	Any	Allow				
	Users and Groups								
	🗟 Users								
	angle Groups								
-	🛃 Domains and User Login								
tre	Definitions								
Control	SSL Certificates								

Content Rules allow you to regulate Web content within your organization.

In addition to the content filtering capabilities shown in the figure above, Kerio Control can also enforce the use of safe search, and block pages containing various words or phrases. The software also contains a whitelist option that can be used to override the filters for sites that are known to be safe.

O4 Additional Infrastructure and Reporting Features

Kerio Control includes a number of infrastructure components that can help to make life a bit easier for smaller organizations. For example, the software provides DNS caching, which can help users to experience more responsive browsing. There is also a built-in secure VPN functionality, and the Kerio Control server can even be configured to act as a DHCP server.

One of the things that impressed me about Kerio Control is that it can be configured to map groups and user accounts from the Active Directory. By doing so, it becomes possible to keep track of activity on a user by user basis. The software includes reporting capabilities that allow you to track which sites users are visiting, and how much network traffic users are generating, among other things. You can see an example of this in the figure below.

文 Kerio Control		My Account Logout
Summary Report Individual		 ♦ 8/18/2019 ■
Al Overall Users by Traffic	<u>Visited Sites</u> Web Categories Ap	plications
Website microsoft.com windows.com live.com google.com kerio.com gstatic.com akamaized.net bing.com doubleclick.net msn.com	Visits 68 27 21 21 7 7 6 4 4 4 3 3 3	
Details microsoft.com - 68 visits windows.com - 27 visits	not logge	Name Visits not logged in (unrecognized users) 68 Name Visits

Kerio Control provides rich reporting capabilities.

If Kerio Control is mapped to an Active Directory, the report shown in the figure above will show you which specific users accessed which sites. It is even possible to block Web access to users who are not logged in, so as to prevent users from acting anonymously.

05 Pricing

Pricing for a Kerio Control virtual appliance like the one that I based my evaluation on starts at \$320 per year (covering the minimum of 10 licenses). Prices decrease per user at higher volumes. The Deluxe edition, which includes antivirus and web filtering capabilities costs \$380 per year, again for the minimum 10 users. GFI offers several different Kerio Control hardware appliances with prices ranging from \$575 to \$1,599 per year, plus required software licenses.

You can find the full pricing information, and a listing of the various plans that are offered at: https://www.gfi.com/products-and-solutions/network-security-solutions/kerio-control/pricing

06 The Verdict

I always wrap up the reviews that I write for this site by assigning a numerical score to the product that I am evaluating. These scores range from zero to five stars, with five stars being the highest possible score. With that said, I decided to give Kerio Control a score of 4.9, which is a gold star review.

Throughout my evaluation, I consistently found Kerio Control to be completely intuitive. That's quite an accomplishment for a network security tool. So many of the competing tools that I have used in the past seem needlessly overcomplicated.



The other thing that really impressed me about Kerio Control is the sheer number of features that it includes. As you may have gathered from the screen captures, its feature set goes far beyond what I am able to cover within a review.

Kerio Control is clearly an excellent choice for any small or medium sized business that needs a reasonably priced network security suite, that is reasonably priced and not overly difficult to use.



Get your FREE Kerio Control trial



All product names and companies mentioned may be trademarks or registered trademarks of their respective owners. All information in this document was valid to the best of our knowledge at the time of its publication. The information contained in this document may be changed without prior notice.