

WHITEPAPER

Making the most of your Kerio Control trial



GFI™

Aurea SMB Solutions

Introduction

Kerio Control is much more than just a simple firewall. It is a feature rich, Unified Threat Management (UTM) gateway that defends your network against attacks on multiple fronts. Best of all, Kerio Control brings enterprise class security features to smaller organizations, but without the excessive cost and complexity that is so often associated with enterprise products.

As you evaluate Kerio Control, there are a number of different features that you should be sure to look at. These features include things like firewall rules and intrusion prevention modules, as well as bandwidth management and VPN features.



Traditional Firewall Rules

One of the first things that you should look at when evaluating Kerio Control is its firewall. You can access the firewall by logging into the Kerio Control administrative console and selecting the Traffic Rules tab. As you can see in the figure below, Kerio Control includes several built-in firewall rules that are designed to help keep your network secure by default.

Name	Source	Destination	Service	IP version	Action	Translation	Last used	Valid Time
<input checked="" type="checkbox"/> Remote administration	Any	Firewall	Kerio Control W...	IPv4	Allow		just now	
<input checked="" type="checkbox"/> Remote administration	Internet Interfaces	Firewall	TCP 4081	Any	Allow			
<input type="checkbox"/> VPN Services	Any	Firewall	IPsec services Kerio VPN	Any	Allow			
<input type="checkbox"/> Web Services	Any	Firewall	HTTP HTTPS	Any	Allow			
<input checked="" type="checkbox"/> Internet access (NAT)	Trusted/Local Interfaces Guest Interfaces VPN clients	Internet Interfaces	Any	Any	Allow	NAT Balancing per host	just now	
<input checked="" type="checkbox"/> Local traffic	Trusted/Local Interfaces Trusted/Local Interfaces VPN clients All VPN tunnels	Trusted/Local Interfaces Trusted/Local Interfaces VPN clients All VPN tunnels	Any	Any	Allow		1 minute ago	
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any	Any	Any	Allow		just now	
<input checked="" type="checkbox"/> Guests traffic	Guest Interfaces	Firewall	Guest services	Any	Allow			
<input type="checkbox"/> Block other traffic	Any	Any	Any	Any	Drop		just now	

Kerio Control includes built-in firewall rules.

Rather than requiring you to configure a list of obscure port numbers as so many other firewalls do, Kerio Control presents the firewall rules in a very intuitive way. The red color indicates an inbound rule, while the green color indicates an outbound rule. Rules can be enabled or disabled by selecting or deselecting the corresponding checkbox. The Source, Destination, and Service fields explain exactly what the rules apply to.

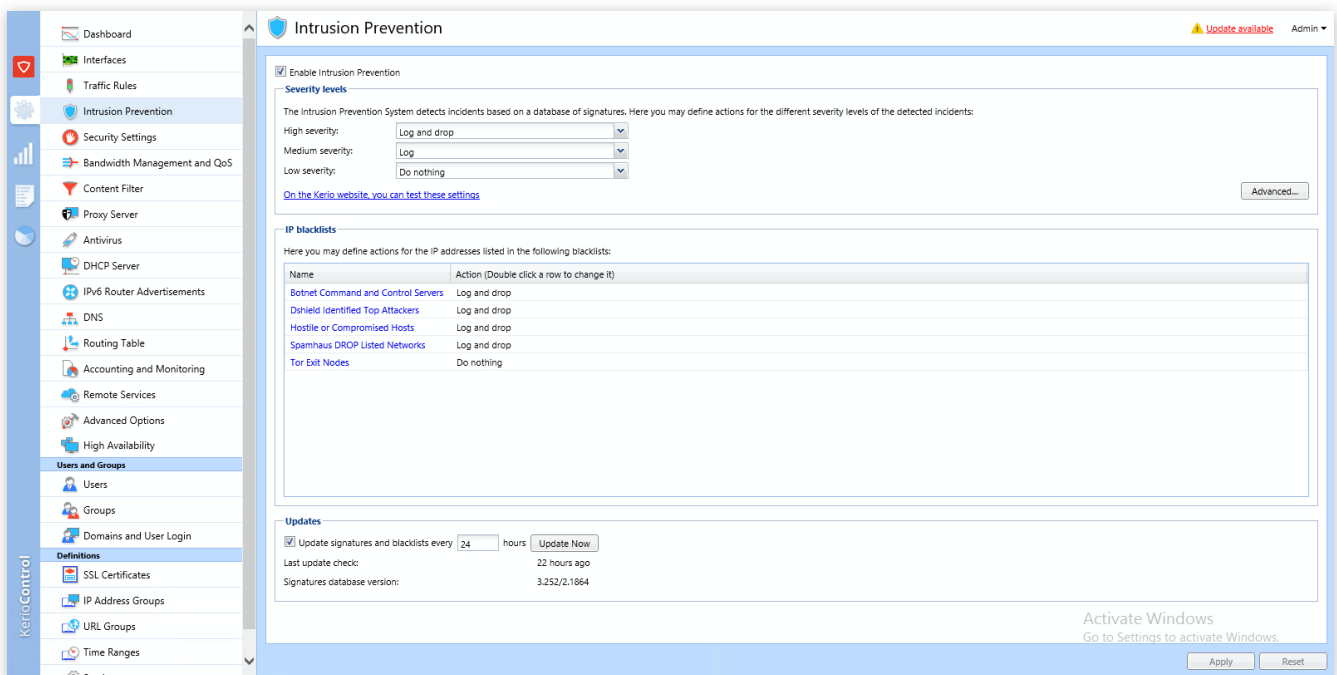
As you look at the previous figure, you will also notice that one of the traffic rules is named Internet Access (NAT). This rule, which exists by default, allows Kerio Control to act as a NAT router, shielding your internal network from the Internet.

Another thing that you may have noticed in the traffic rules is that there is a rule called Guest Traffic. This rule, which exists by default allows guests to access the Internet. In doing so, guests do not require a Kerio Control username and password, and guests are not counted as licensed users.

The Intrusion Prevention Module

Kerio Control is more than just a firewall. It comes equipped with a full featured intrusion prevention module with an underlying snort-based packet analyzer. This packet analyzer is designed to protect your network against known threats. The entire analytical process happens behind the scenes, meaning that you do not have to deal with the complexities involved in examining raw packets of data.

As you can see in the figure below, Kerio Control is equipped with an attack signature database that allows it to automatically detect various threats. These threats are categorized by severity, and you can configure how Kerio Control responds to detected threats based on how severe they are. You can access these settings from the management console's Intrusion Prevention tab.

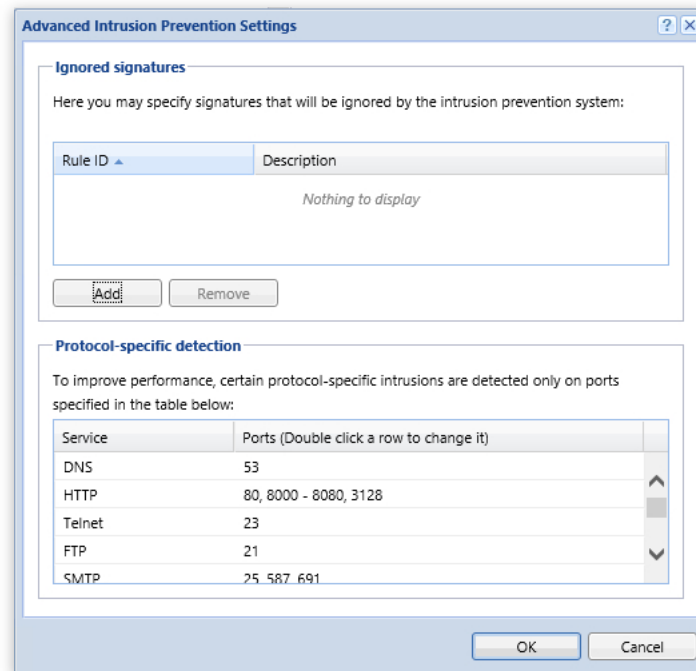


Kerio Control uses a signature database to detect malicious activity.

Kerio Control also uses several IP blacklists to keep your users and your network safe. As you can see in the previous figure, blacklists exist for botnet servers, hostile and compromised hosts, TOR exit nodes, Spamhaus DROP listed networks, and more.

Both the IP blacklist databases and the intrusion prevention database are automatically kept up to date. By default, Kerio Control updates the attack signatures and the IP blacklists every 24 hours. However, you can easily adjust the update frequency based on your own needs.

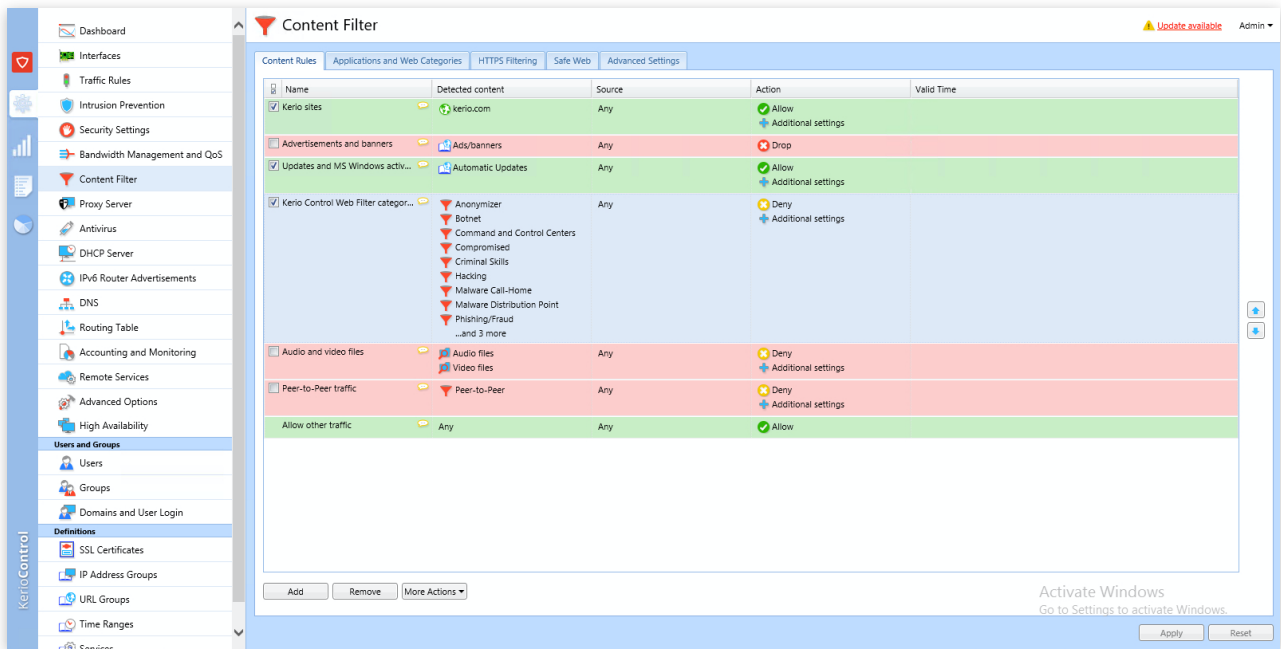
Kerio Control has been designed for reliability and was specifically engineered to avoid false positives. In the unlikely event that false positives do become an issue however, the administrator has the ability to ignore any signatures that are determined to be problematic. Simply click on the Advanced button, shown in the previous screen capture, and then click on the Add button shown below to add the signature that you want to ignore.



Kerio Control is designed to prevent false positives, but gives you the ability to ignore signatures if necessary.

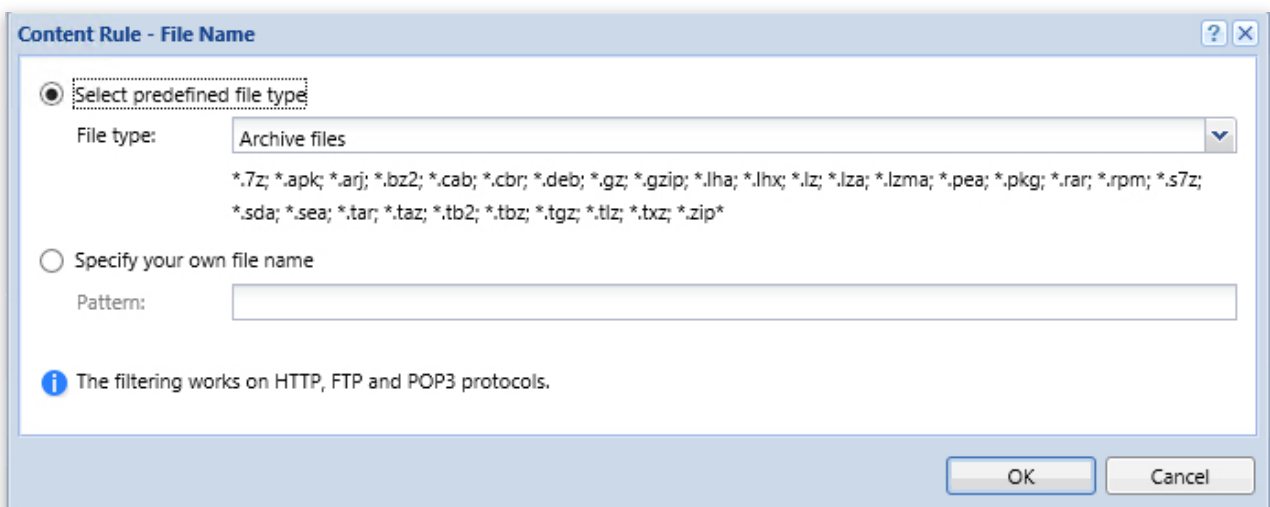
Content Filtering

Kerio Control's content filter helps to protect organizations against the threat of users accessing objectionable Internet content. Like the Kerio Connect firewall, the content filter is color coded, and includes several default rules. As you can see in the next figure, the rules shown in red are designed to block content, while rules shown in green allow content. Rules can be based on URLs or on automatically detected content categories. For example, Kerio Control's default rules block ads and banners, malicious Websites, audio and video files, and peer to peer networks.



The content filter blocks objectionable Web traffic.

You can access the content filtering rules shown above through the console's Content Filter tab. You can use the Add or Remove buttons at the bottom of the screen to create and delete rules as necessary. You can also modify existing rules by double clicking on the rule. Doing so gives you the ability to specify file names and extensions, as shown below. You also have the option of setting time ranges within which the rule should be enforced.

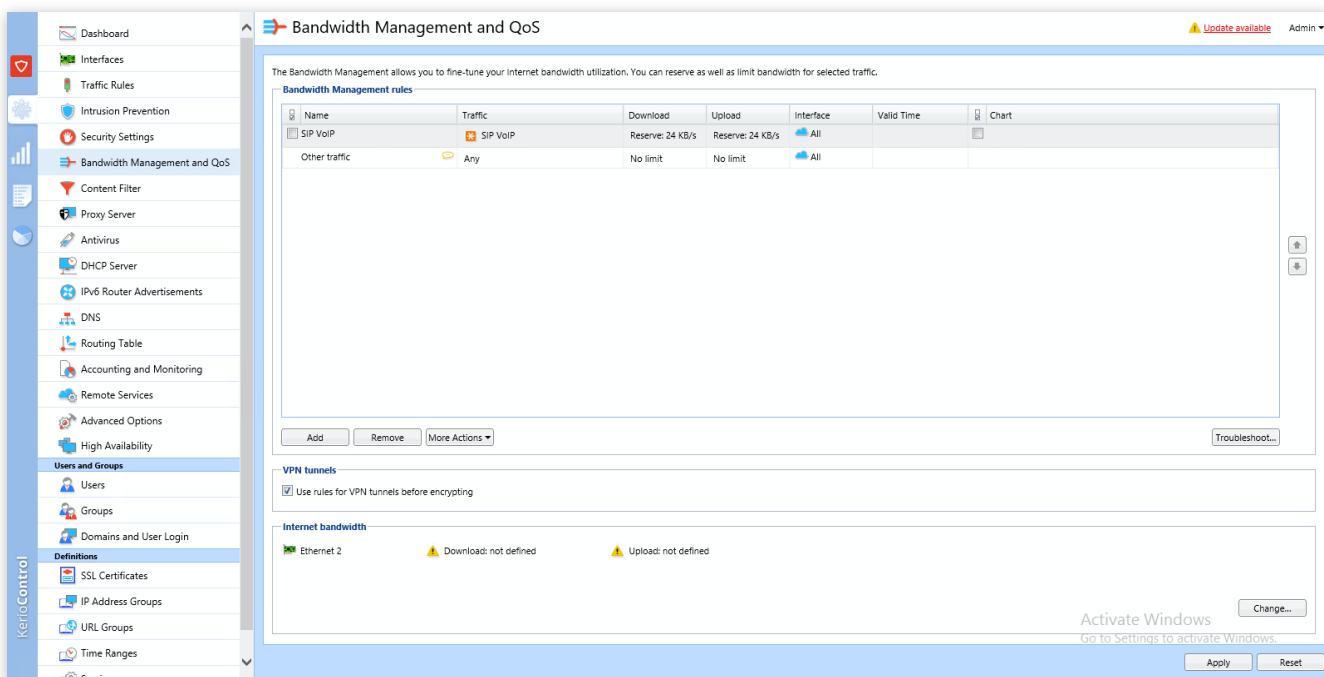


You can base rules on specific file names or extensions.

Bandwidth Management

One issue that almost all organizations struggle with from time to time is insufficient Internet bandwidth. When users place too much of a demand on an organization's Internet connection, critical services can suffer. For instance, VoIP calls may be dropped or may suffer from audio distortions. Similarly, SaaS applications may become slow and unresponsive.

Kerio Control helps to keep mission critical applications running smoothly during periods of heavy Internet use by providing organizations with the ability to prioritize Internet traffic. You can access these controls by selecting the Bandwidth Management and QoS tab shown below.



The screenshot displays the 'Bandwidth Management and QoS' configuration window. The main area contains a table of 'Bandwidth Management rules' with the following data:

Name	Traffic	Download	Upload	Interface	Valid Time	Chart
SIP VoIP	SIP VoIP	Reserve: 24 KB/s	Reserve: 24 KB/s	All		
Other traffic	Any	No limit	No limit	All		

Below the table are buttons for 'Add', 'Remove', and 'More Actions', along with a 'Troubleshoot...' button. The 'VPN tunnels' section includes a checked checkbox 'Use rules for VPN tunnels before encrypting'. The 'Internet bandwidth' section shows 'Ethernet 2' with two warning icons and the text 'Download: not defined' and 'Upload: not defined'. At the bottom right, there are 'Apply' and 'Reset' buttons, and a 'Change...' button next to the 'Activate Windows' watermark.

Kerio Control provides tools for prioritizing Internet traffic by type.

Kerio Control includes a number of predefined traffic categories, thereby making it easy to restrict or prioritize traffic by type. In the figure for instance, you can see a rule that reserves Bandwidth for use by VoIP applications.

In addition to being able to restrict or prioritize traffic by type, you can also manage traffic by user or group. You can even apply quotas if necessary.

VPN Features

Finally, Kerio Control can be configured to act as a VPN providing remote user access and / or site to site connectivity. The VPN is compatible with the IPSec protocol, meaning that communications can be IPSec encrypted. Additionally, GFI offers clients for Windows, MacOS, and Debian and Ubuntu Linux.

You can download the VPN clients at:

<https://www.gfi.com/products-and-solutions/network-security-solutions/kerio-control/resources/other-downloads/vpn>

For more information on how to configure and manage VPN with Kerio Control, check out these video demos:

<https://www.gfi.com/sites/keriocontrol/how-to-install-and-manage-your-vpn>



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.