

« Web content security

# Finjan Vital Security NG-8000



**Supplier** Finjan UK  
**Price** NG-8000 chassis and four blades £19,760; 251 users with one-year web security licence £2,477 (all exc VAT)  
**Contact** [www.finjan.com](http://www.finjan.com)

The most prominent weapon in Finjan's Vital Security arsenal is its patented behaviour-blocking technology, which works at the application level to identify malicious content in web traffic. Anti.dote provides protection in the window between a new threat being identified and a patch being posted. As soon as new exploits are discovered, Finjan downloads behavioural rules to the appliance, allowing it to block them.

Anti-spyware is the third component, and Finjan employs preventative measures that include known spyware URL lists and its behavioural analysis. These form the foundation of the vendor's web security solution and they can be augmented with optional anti-virus measures and web content filtering. For the former you can choose from Kaspersky Lab, Sophos or McAfee, and the latter; Websense or IBM's Proventia.

The appliances can function either in all-in-one mode or you can use multiple appliances to spread the scanning load and have them all reporting to a central policy enforcement server. We focus on the latter method as the NG-8000 is designed to provide

these services to enterprises. At its foundation is a well-specified IBM BladeCenter server, and its 7U chassis has room for up to 14 server blades. The entry-level model comes with four dual-core Xeon server blades; one to provide policy management and the other three to act as scanning servers. It is possible to add more scanning server blades and a second policy server blade for redundancy.

You can decide what networking services you require as the blade server accepts IBM's L2 to L7 Ethernet switch blades. Load balancing across multiple scanning servers can be carried out by the switch blades but, in most cases, customer premises equipment will be used for this. One scenario is to present a virtual IP address to the network that all clients use as their proxy. The switches carry out load balancing to determine which scanning server the request is sent to. Or use multiple scanning servers, still managed by a single policy server, but each providing different security services.

Installation and deployment is simplified with a new wizard-based CLI setup for each blade. The web management interface is identical to other Finjan appliances.

More scanning servers are added by providing their IP address. The policy server pushes software, signature updates and scanning policies to them automatically. Each server is accessed so you can configure it as transparent or explicit proxy and configure upstream proxy details, proxy authentication plus ICAP integration. The policy server also

maintains a set of global default values that can be applied to each scanning server.

Scanning services are configured using policies that comprise rules and can be customised. The x-ray feature will prove useful for testing as it runs selected policies and rules passively and merely reports on what their effects would have been. Configuration is easier thanks to an interface that shows policies in a simple tree structure.

Policies use sets of rules, and we were impressed with the number on offer. An option for scanning HTTPS traffic is available where the encrypted stream is terminated at the scanning server and inspected before being passed on to the client. WCCP (web cache communication protocol) is supported, allowing Cisco's security appliances and compliant switches to forward traffic to the appliance for inspection.

Websense offers over 50 content categories, and during testing it delivered in performance. Of more interest is the behaviour-blocking technology, which normally resides near the bottom of a set of policy rules to provide a last line of defence. We pointed a client at a website with a known Trojan payload and gradually switched off each rule in our default policy.

To see the behavioural blocking in action, we disabled rules for web content filtering, anti-virus, anti-spyware, files with missing digital signatures, and suspicious file downloads. The Trojan's code



was analysed, blocked, and the log showed it was trying to terminate running processes, illicitly manage memory and run DLLs.

The NG-8000 is simple to deploy and configure and delivers tough web security measures. Ploys such as dynamic code obfuscation may fool signature-based scanners but are unlikely to get past Finjan's behavioural blocking technology, while its security policies and blade server architecture make it highly versatile.

*Dave Mitchell*

SC MAGAZINE RATING	
Features	★★★★☆
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>For</b> Greatly improved management interface, policy-based web security, extensive deployment scenarios, IBM blade-server platform, unique behavioural blocking technology	
<b>Against</b> Nothing of any significance	
<b>Verdict</b> A range of security measures deployed in a versatile blade server with plenty of expansion potential offer tough defences against web-borne threats	



securing your web

[www.finjan.com](http://www.finjan.com)