

We secure the world's largest networks.

URL Filtering

URL filtering is the blocking of user access to forbidden Web sites. In enterprises, it tends to be used in cases where companies sense a dramatic loss of employee productivity and an increase of liability risks due to unsanctioned Web surfing. In service provider environments, it has great value as an add-on to Internet services where it may be used for parental restriction of child Web surfing or on behalf of businesses that may have an inherent distrust of Internet content.

Network security operations at the application level tend to be algorithmically intensive and complex and require a significant investment in hardware to scale performance to a desired level. URL filtering – the blocking of user access to forbidden Web sites – is one such operation.

Crossbeam products, with highly parallelized operations, are uniquely suited to the scalable delivery of URL Filtering in both enterprise and service provider environments.

Requirements for URL Filtering

The biggest issues with the deployment of URL filtering are:

- Performance – how do you restrict access to certain sites while maintaining a great (fast) user experience of legitimate sites?
- Scaling – how do you prevent the URL filtering infrastructure from getting out of hand as your employee or user base grows?
- High availability – how do you prevent failures in the blocking system so that the medicine is not worse than the disease?

The World's Highest Scaling URL Filtering

To solve the inherent complexity of delivering scalable URL filtering, Crossbeam incorporates the market-leading filtering engines from Secure Computing and Websense. Secure Computing and Websense run as OPSEC applications, which means they require and leverage Check Point Firewall-1 technology. The totally integrated solution eliminates the need

for load balancers, switches and separate high availability software required to make current URL filtering systems scale. It also adds a significant layer of protection on top of the firewall itself.

These engines are state-of-the-art, providing the industry's most complete databases of categorized suspect sites and the ability to customize and add to the databases for company-specific policies. Management of the system is automatic – as new, unauthorized sites are discovered they are added to the database. A rich palette of administrative controls provides managers with access to full-featured reports.

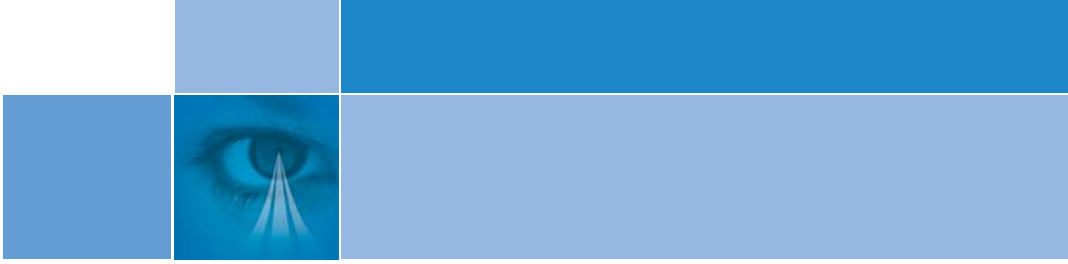
X-Series URL Filtering Solution

For large data centers, the Crossbeam X40 provides scalable URL filtering performance, single and dual box high availability and the ability to integrate with other best-in-class security solutions, such as firewall, intrusion protection, VPN, and anti-virus systems.

The Websense engine is combined on up to ten Crossbeam X40 Application Processing Modules (APM). The unique parallel processing architecture of the X40 allows Websense to run either on the same blade as the firewall or on a separate blade. This is because the X40's ultra-fast switch fabric introduces no latency in the communication channel between the firewall and the URL filtering engine. Performance scales linearly as APMs are added to the system.

How it works

The front-end Network Processing Modules (NPM) perform an initial flow classification and load balancing function, distributing traffic to the least loaded APM running Firewall-1. Firewall-1 then communicates with Websense using a TCP/IP message based API called "UFP" (URL Filtering Protocol). When a user requests a Web page, Firewall-1 intercepts the HTTP request and sends the requested URL to Websense for analysis. Websense looks up the URL in its Web site classification database and decides what action (or actions) to take based on administratively defined policies. Possible actions include block, log, continue, defer, authenticate, etc.



As with the X40 firewall solution, the need for high availability software is eliminated since it is built-in – all connections are stateful and state is maintained across modules (both NPM and APM). In addition, the NPMs are unaddressable and do not report any fingerprinting information nor do they respond to port scans. Initial packet verification occurs at this level and frees the firewall for more processing. Up to 4096 VLANs are supported, meaning that the X40 integrates easily into any network environment. Interface options on each NPM are 1GE+8FE (10/100) or 2GEs.

Administration of the system is performed through an entirely separate switched control plane. Gigabit logging ports on this same out-of-band network also ensure that data traffic is not affected by management traffic. On the X40, sixteen administrative levels are supported along with GUI and command-line configuration options.

About Crossbeam Systems

Crossbeam Systems, Inc., is a leading global developer of total security solutions required for safer, simpler networks. Crossbeam enables companies to consolidate their security infrastructures while preserving their security policies, resulting in significant savings in capital and operational expenses. Crossbeam's patent-pending architecture integrates best-in-class security engines such as firewall, virtual private networks, intrusion detection, and content security into high-performance, highly available, self-healing security services switches. The company has tailored solutions for global enterprises, carrier networks, and medium-sized businesses. More information is available at www.crossbeamsystems.com.



www.crossbeamsystems.com

Corporate Headquarters
200 Baker Avenue
Concord, MA 01742 USA
p: [+1] 978-318-7500
f: [+1] 978-287-4210

European Headquarters
E. Space, Bat C.
45 allée des Ormes
06250 Mougins – France
p: [+33] (0)4 92 28 89 89
f: [+33] (0)4 92 28 72 60

Asia Pacific Headquarters
80 Raffles Place
Levels 36 UOB Plaza 1
Singapore 048624
p: [+65] 6248 4684
f: [+65] 6248 4988