Exinda for M86 Security

While the symptoms of a poorly performing network are easy to see, pinpointing the underlying causes of network issues is not nearly so straightforward. With the increased use of complex applications including peer-to-peer file sharing applications such as BitTorrent, video, online gaming, streaming media, voice conferencing, and more, ensuring that crucial administrative and education applications perform well has become a challenge. With Exinda for M86 Security, network administrators have the ability to see precisely which applications and how much of your network resources are being used by which users, so network managers can ensure they have the right security policies and controls in place to address this traffic. With Exinda, network managers can also control and optimize the traffic on their networks to ensure that adequate bandwidth is available to the ones with highest priority.

KEY BENEFITS

- Application visibility allows IT staff to visualize all traffic on the network at the application layer (Layer 7). Using an advanced application classification engine, Exinda can identify and classify over 2,000 peer-to-peer traffic, URLs and application signatures.
- Real-time monitoring and historical statistics help IT understand what applications are running on the network and how much bandwidth each application is consuming.
- Dynamic policies provide bandwidth guarantees to critical applications to ensure they receive the network resources they need in order to operate effectively. Policies also limit and constrain recreational or non-business critical applications.
- Exinda's anonymous proxy detection function senses the use of cloaking sites and software and allows network managers to limit or drop these flows as desired.
- Active Directory integration allows tracking of network usage directly to individual users. You can view traffic usage by user names and create policies to manage bandwidth for users rather than IP addresses, especially in dynamic address environments or policies can be applied to whole Active Directory groups such as the finance department or all printers.
- A library of pre-built report templates allows business and technical users to access the relevant information they need without IT staff having to spend time and effort building custom reports.
- Intelligent acceleration allows IT staff to selectively speed up both TCP and CIFS applications so end users enjoy quicker application response with less effective bandwidth clogging the wide area network.
- Asynchronous Object Memory (AOM) allows the distribution of unicast video with the bandwidth effectiveness of multicast. A YouTube video need only be downloaded once to each site in order for all users of that site to take advantage of the file by replaying the video from a local copy rather than refetching from the Internet.

THE BUSINESS ISSUES

High volumes of non-mission critical traffic on the network can drive increases in operating costs as organizations are forced to upgrade their bandwidth or invest in high capacity WAN links at data centers, HQ buildings and remote offices. Recreational internet traffic increases congestion and competes with legitimate business applications for available bandwidth, creating delays, frustration and lost productivity when students, teachers and administrators need to access applications on the network. Many customers who have opted to deploy Exinda cite recreational traffic consumption of up to 45% of the total available WAN capacity.

Many sites and applications that were once considered purely recreational – such as Skype, YouTube and Twitter – are now being used as teaching or business tools. Network managers are concerned about the leakage of sensitive data via these and other applications. Threats such as spam, phishing, viruses and malware attacks can also originate from these sites and quickly spread across the network, as many are designed specifically to evade detection and slip past corporate firewalls by port hopping or masquerading as legitimate business applications. It can be difficult for network security professionals to ensure that this traffic is handled effectively and to pinpoint the source.

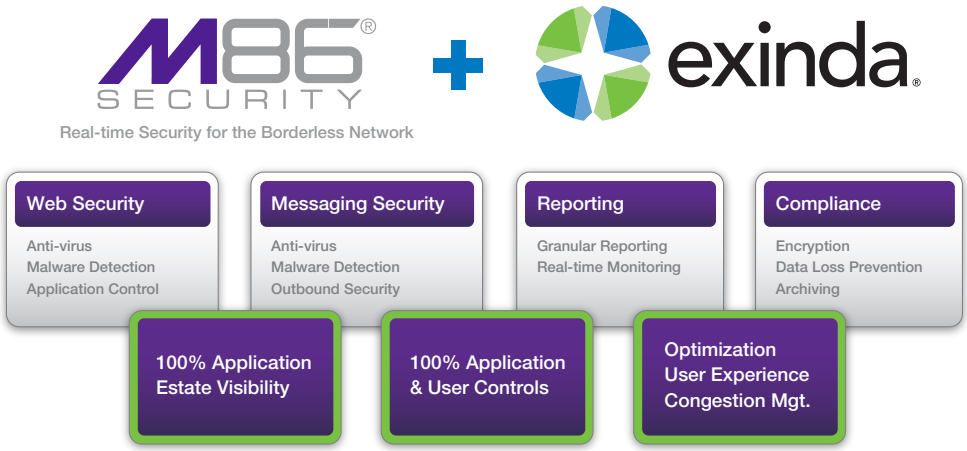
Many cloud based applications also pose challenges for network administrators. Microsoft applications including Windows file sharing, Exchange and Outlook for email, SharePoint services for portal and collaboration, database services using MS-SQL, and domain and directory services with Active Directory can be very "chatty", meaning a large number of round trip transactions are required to complete a request. Managing both security and performance concerns for these applications is a considerable challenge without the right tools.

THE SOLUTION

Exinda's WAN Optimization solutions enable network managers to get a complete view of what is happening on their WAN. Its Unified Performance Management (UPM) strategy delivers full visibility, control and optimization capabilities, all within a single solution. When coupled with M86, network managers can ensure that security policies are applied more effectively, while maximizing the performance of critical applications on the network.

Visibility ensures you have a real-time view into the applications – including recreational and unwanted traffic – and users on the network. Rich historical reporting provides trend analysis; this provides objective application performance information using application response measurements to analyze actual traffic on the network. Controls and QoS deliver bandwidth guarantees and prevent non critical applications from impacting critical applications.

With Exinda for M86 Security, administrators can give priority to applications or application groups, and can assign policies at the user or user group level. For example, schools can give priority to educational applications, while limiting or blocking access to other types of traffic and content such as Skype. By improving network performance and their ability to monitor network traffic, schools can maximize the performance of their existing networks, without compromising network security, and without the need for additional spending on their infrastructure.



ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**

Corporate Headquarters
8845 Irvine Center Drive
Irvine, CA 92618
United States

Phone: +1 (949) 932-1000
Fax: +1 (949) 932-1086

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Suite 3, Level 7, 100 Walker St.
North Sydney NSW 2060
Australia

Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899

Version 04/13/11