Barracuda

QPCSS LTD.
QUEENS PARK
CyberSecurity Solutions Ltd.

Choosing a Network Firewall: Five Questions to Help You Avoid Costly Mistakes

White Paper

RELEASE 1

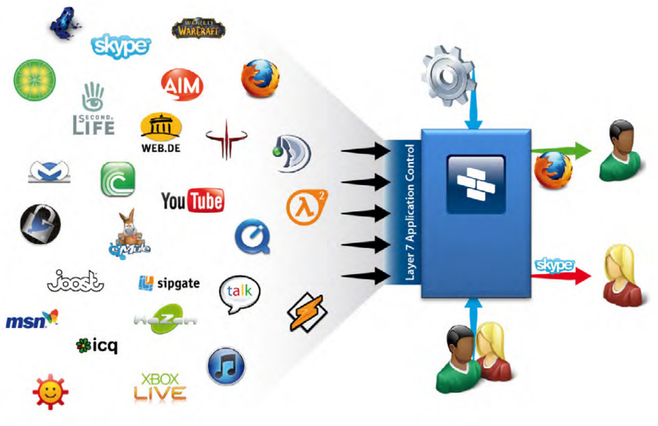
Not all firewalls are created equal

From the smallest startup to the largest global enterprise, all organizations face the same basic security challenges. It's critical to invest in a network firewall that meets those challenges cost-effectively. Choosing the wrong firewall can result in security gaps, excessive management complexity, and the need for additional investment to close feature gaps. Key security considerations include:

- An evolving threat landscape that includes a growing number of attacks disguised as ordinary web or application traffic, or designed to bypass traditional port designations
- Growing dependence on Internet applications for daily business operations, leading to greater bandwidth demands and making it harder to isolate business usage from leisure usage
- Increasing throughput requirements to maintain high performance, straining the capabilities of firewalls and Unified Threat Management (UTM) solutions
- Ever more mobile users and remote locations, which require fast, reliable, and secure connection to network resources at all times

These issues are especially challenging for organizations that lack the extensive IT resources of enterprise-scale businesses. For these organizations, putting the right network firewall in place is critical. When making a purchase decision, they must look beyond immediate cost, to also consider the five questions to be discussed below. A firewall vendor that can answer "yes" to all five of them is likely to deliver a solution that will cost-effectively address important security issues both now and over the long term.

1. Can this firewall provide visibility and regulation of application traffic and user behavior?



For a firewall to be effective, it must be able to identify and regulate application traffic. It was once adequate to simply block ports or services on the network to fulfill application control requirements. But traditional port-based firewalls are ineffective against today's evolved applications.

Port-based firewalls are ineffective against today's evolved applications.

Modern applications such as YouTube, DropBox, and Cisco WebEx are able to pass as web traffic, which is typically unblocked on port-based firewalls. Even blocking based on source and destination is unreliable because applications like Skype and peer-to-peer tools are able to obfuscate their source and destination, while using multiple ports. An even greater risk arises when malware and viruses mimic applications to gain access to your networks.

The ability to identify and block application traffic – regardless of which port it uses – is necessary but not sufficient. Because many of these applications have legitimate business uses, it must also be possible to regulate them precisely – for example, you may wish to allow only marketing personnel to use Facebook at any time, but to block the use of Facebook games or Facebook chat, while allowing all employees to use Facebook without restrictions during the lunch hour.

The Barracuda Firewall goes beyond traditional network firewalls and UTMs by providing granular, Layer 7 application controls and user-identity awareness. A comprehensive library of hundreds of applications is pre-defined on each Barracuda Firewall and updated regularly. Based on these fingerprints, administrators can configure a flexible set of actions, including allowing, blocking, resetting, and redirecting connection attempts and traffic. Administrators can easily view all active connections using an intuitive interface, and can take real-time action to either end a connection or regulate its bandwidth.

2. Can this firewall provide granular regulation and filtering of web traffic?

The use of network resources for nonproductive web browsing can reduce overall productivity, as well as have a significant impact on bandwidth – leading to real costs in terms of infrastructure investment. In addition, web traffic is an increasingly important vector for the introduction of malware, viruses, and spyware to your network.

For these reasons, it's important to install a firewall that enables granular regulation of web traffic, along with robust content filtering to keep Internet-borne threats at bay.

Unlike other next-generation firewalls, the Barracuda Firewall integrates transparently with the cloud-based Barracuda Web Security Service. This technology allows administrators to create custom block-lists, as well as choose from more than 95 predefined content categories for blocking. Policies may be defined and enforced based on individual users or groups, times, and other parameters.

In addition, incoming web traffic is filtered based on content, to block viruses and other malware. Because this filtering takes place in the cloud, threats are neutralized before they ever touch the network – and there is no demand placed on your network compute resources, preventing the performance lag typically associated with web content filtering.

Web traffic is an increasingly important vector for the introduction of malware, viruses, and spyware to your network.

3. Can this firewall increase the reliability of my network and reduce downtime?

Today's organizations are increasingly reliant on continuous connection to the Internet, and even a brief loss of connectivity can be very costly. A firewall that integrates link balancing, automatic link failover, and traffic prioritization functions ensures uninterrupted connectivity with far lower cost than a standalone link balancing solution. For additional flexibility, many firewalls today also offer a 3G modem to provide backup connectivity.

It is also highly recommended that your network firewall provide the capability to manage the performance and traffic of WAN links. With integrated link balancing, organizations have the flexibility to reserve costly, high-speed connections for high-bandwidth or latency-sensitive traffic such as Voice over IP (VoIP), while directing low-bandwidth or latency-insensitive traffic such as email, to lower-cost links.

The Barracuda Firewall includes advanced link balancing and traffic shaping capabilities to prioritize business-critical applications while throttling or blocking unproductive ones. Automatic link failover ensures uninterrupted connectivity even when a primary link fails. And with the optional Barracuda UMTS 3G modem, you'll stay connected even when wired connections are damaged or become unavailable.

A firewall that integrates link balancing and availability functions is a cost-effective option relative to purchasing a standalone link-balancing solution.

4. Can this firewall provide comprehensive security without compromising performance?

Tighter security requirements for functions such as content filtering have put an extraordinary demand on today's UTM platforms. Most UTM vendors today face challenges maintaining system performance while all features are enabled, resulting in degraded throughput, increased latency, and traffic bottlenecks, even with dedicated hardware platforms.

As you are considering your next firewall solution, be sure to evaluate its throughput and scalability when all security features – such as intrusion prevention, content scanning, VPN, and anti-virus protection – are enabled. A non-scalable product becomes costly. Often, customers who don't account for the performance degradation in UTMs are forced to upgrade to larger models, accelerating upgrade investments in network firewalls. The costs become prohibitive over time, as the amount of malware and anti-virus scanning increases.

The Barracuda Firewall's integrated cloud-based web security technology filters content and blocks malware before it reaches your network. This eliminates performance bottlenecks that traditional UTM devices incur when scanning for viruses and spyware. Using the cloud for malware scanning ensures unlimited scalability and elasticity, as well as real-time updates for continuous protection against the latest threats.

Most UTMs today face challenges maintaining system performance, resulting in degraded throughput, increased latency, and traffic bottlenecks.

5. Can this firewall help me reduce costs?

As with any technology investment, a firewall's total cost of ownership (TCO) depends on many factors. In addition to the up-front cost, buyers must consider the resources required for ongoing management and administration. In addition, fees may be charged for per-user licensing, VPN licenses, and for enabling "premium" features such as centralized management or link balancing – and if those capabilities are not provided, there are additional costs associated with separate solutions that must be purchased to fill the gaps. Finally, if the solution is not sufficiently scalable, all of these costs will be magnified over time as an organization grows.

The most cost-effective firewall, therefore, will be one that:

- Includes a full suite of key features and capabilities – secure VPN, link balancing, automated failover, application visibility, centralized management, etc. – fully enabled with no additional fees or costly add-on modules
- Makes minimal demands on organizational resources, in terms of both staff time and IT infrastructure
- Is designed for maximum scalability, without predefined user limits, and with a clear and affordable upgrade path

The Barracuda Firewall meets all these criteria, combining advanced functionality with low TCO to deliver exceptional value in a next-generation firewall. While each unit includes its own intuitive web management interface, it is also integrated – at no extra cost – with Barracuda's global cloud infrastructure for easy, centralized, "single pane of glass" management of multiple devices with minimal IT overhead. Administrators can even use mobile apps to complete device management tasks on the go.

Other key features are fully enabled with no need for extra fees or modules, including unlimited VPN licenses, link balancing, automated failover, and more. The simple interface makes it easy for small and medium-sized organizations to implement and manage their firewalls with minimal IT overhead. And because of its innovative leveraging of practically limitless cloud resources for management, content filtering, malware blocking, and reporting, scaling as requirements evolve is simple and affordable.

For less dispersed environments, a dedicated management appliance is often unnecessary and cost-prohibitive relative to the overall cost of the deployment.

Barracuda
Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
1-408-342-5400
1-888-268-4772 (US & Canada)
www.barracuda.com
info@barracuda.com

Summary

Organizations need to have application and user control, robust content filtering that does not affect performance, link balancing and failover, and bundled centralized management.

The Barracuda Firewall is an excellent choice for most small to medium-sized organizations. Its innovative cloud-based content filtering resolves the bottleneck issues typically seen in today's UTMs when the full suite of malware and anti-virus scanning is enabled. It includes free centralized management in the cloud, allowing units to be managed anywhere, anytime. Each unit comes with pre-configured QoS bands that ensure organizations can deploy and configure its QoS policies in minutes. Its next-generation firewall capabilities let administrators control bandwidth. The Barracuda Firewall is offered without per-user or per-VPN fees.

To learn more about the Barracuda Firewall, or to request a free, 30-day trial, contact a Barracuda sales engineer or your Certified Barracuda Reseller.

Queens Park CyberSecu-

8a Bravington Road,
Maida Vale,
London,
London,
W9 3AH,
United Kingdom,

02039710740,
info@qpcsl.com,
www.qpcsl.com

To learn more about Barracuda's web security solutions, please visit www.barracuda.com/products or call Barracuda for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772 (US & Canada).

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit www.barracuda.com.