

Barracuda NG Firewall - A Modern Approach to Security Management

Security management - The key to more security and efficiency

The success of Internet-based business processes has, for many companies and managed security providers, resulted in the steady growth in the number of network gateways used over many years. Commensurate with the growth in the number of gateways has been the growth in management overhead.

Any gains made by vendors to simplify the installation and maintenance of a single gateway is no longer of any significance – the pure volume of systems alone demands enormous expense in terms of time and staff. In addition, infrastructures which have grown gradually over time are now becoming overly complex. The proliferation of various kinds of security systems, connectivity systems and WAN optimization systems, have resulted in increasingly divergent infrastructures with uncountable interactions between devices.

With its unique gateway management approach, the Barracuda NG Firewall delivers a compelling response to the demands of modern security architectures. Even the most complex infrastructures can be managed transparently and efficiently with the Barracuda NG Firewall. With minimal resources, administrators can manage their gateways at all locations – from the headquarters to the smallest branch office – all from a single interface.

Barracuda NG Firewall Management

The Barracuda NG Firewall presents a unique approach toward the management of similarities, convergence and integration of security and networking, and audit control.

Management of similarities

The core requirement for efficient management of security systems can be illustrated by one simple example: when a new apartment complex is built, the units are initially all identical. In an environment like this, it is very simple to make general decisions as to how the complex will be built because there are no special circumstances to be considered. As soon as tenants move in, however, the units are “in operation” and individual requirements have to be integrated. Perhaps the bathroom fixtures will be changed for some while others will have new windows fitted. In any case, the units do not stay identical for long. Instead they are “customized” by their inhabitants – the users.

General policies which affect the entire complex require much more planning and have to consider the particular circumstances in the units. Despite these differences, the units do not differ fundamentally and far-reaching similarities are still to be found in many areas. If these similarities are neglected then each of the units must be viewed as an individual, completely different unit in its own right. On the other hand, the common ground is no longer sufficient for all units to be treated identically.

A new management approach for large firewall clusters

If the insights from the example above are transferred to security management, then it is apparent that conventional approaches are overtaxed with the management of similarities.

Purely profile-based management focuses on the common ground and ignores the individual characteristics of the gateways. Device-based management, on the other hand, reflects the peculiarities, but is rather expensive especially for complex infrastructures.

Based on technology from next-generation firewall provider phion AG, the Barracuda NG Firewall was designed from the ground up to protect the overall corporate network. One of its first projects was for the Allgemeine Rechenzentrum (ARZ) in Innsbruck, a centralized IT and hosting service provider for the Austrian banking sector. In 1999, the customer wanted to extend its firewall infrastructure and decided to use the opportunity to optimize customer security and management at the same time. However, the financial institutions they provided services for also had their own individual guidelines for Internet and network usage by their staff that had to be taken into account – all at a reasonable management expense. Each branch office was to be protected with its own firewall (i.e., 650 firewalls for 650 branch offices). A network of this scale was unique at the time and demanded a new architecture for centralized management.

RELEASE 1

FEBRUARY 2010

phion AG departed from obsolete concepts and developed a unique combination of profile and device-based management, which is still an integral part of the Barracuda NG Firewall management today. On one hand, this approach allows the mirroring of individual requirements on the gateways, and on the other hand it facilitates the efficient and overall management of similarities. In this way, Barracuda NG Firewall management combines the advantages of profile and device-based management while avoiding the inherent disadvantages. The Barracuda NG Firewall approach proved to be immediately successful at ARZ, and continues to benefit customers around the globe with similar, distributed environments.

There are numerous specialized systems in modern company networks. Alongside commodity systems like switches and routers, network traffic is filtered, encrypted and optimized by firewalls, VPN gateways, Web and mail content security gateways and dedicated WAN optimization gateways. These isolated products are expensive in terms of maintenance and management, and they also make the network extremely complex. Introducing consistent work processes in this confusing environment is anything but simple and often fails because of the many interrelations and incompatibilities among disparate security and networking products. It is also extremely difficult to document network security thoroughly under such circumstances, as is required by various legal rules and regulations.

Integration of Security and Connectivity

Barracuda NG Firewalls integrate the core requirements for both a security and connectivity infrastructure:

- **Security** - The constantly growing flood of refined attack methods is countered by a combination of high-performance next generation firewall and VPN capabilities, including content security, Layer 7 application profiling and network access control.
- **High availability** - All Barracuda NG Firewalls deliver out-of-the-box support for high availability configurations, both active/passive as well as active/active. Customers no longer have to install additional systems and integrate them into the network.
- **Traffic Intelligence** - Barracuda NG Firewalls provide application-aware traffic intelligence across the wide area network (WAN). They are able to identify connectivity disruptions and divert traffic to alternative connections. All current standard line types are supported. Using traffic intelligence, companies can ensure the seamless communication between different locations – even under difficult and unpredictable circumstances.
- **WAN optimization** - Barracuda NG Firewalls include capabilities that optimize application data traffic across the WAN to reduce bandwidth loads and shorten response times. The Barracuda NG Firewall incorporates complete capabilities in models for even the smallest branch offices, enabling consistent security policy of multiple security services across the enterprise.

Converging Security Solutions

The convergence of multiple security technologies in each gateway is an important step towards limiting the complexity and facilitating the management of modern infrastructures at reasonable expense. However, beyond the simple inclusion of multiple security technologies is the requirement for full and seamless integration. The Barracuda NG Firewall is a complete solution portfolio in which all components are tightly integrated, providing a single solution for a modern security and connectivity infrastructure.

Components of a converged security solution include:

- **Perimeter Security** - Protection of network borders
- **Secure Connectivity** - Seamless branch office integration
- **Content Security** - Integrated Web filtering, malware protection and email security
- **Client Security** - Secure VPN connections

Management and Auditing

To facilitate completely centralized control of all connected systems, the Barracuda NG Control Center is available either as dedicated hardware appliances or virtual appliances. With the Barracuda NG Control Center, administrators can define global security regulations and the configuration of all Barracuda NG Firewall services.

To centralize management across many different firewalls and remote access users, the Barracuda NG Control Center enables administrators to configure security and network access policies, control firmware update revisions, and manage user settings. Template-based configuration and globally available security objects enable efficient configuration across thousands of locations.

Highly developed multi-administrator capabilities

The hierarchical management interface of the Barracuda NG Control Center sorts all managed gateways by configuration group which may be specific to departments or locations. For managed service providers, multiple enterprises / tenants (or “ranges”) can be supported independently. Highly customizable administrative roles can be defined to delegate administrative capabilities for specific configuration groups or ranges. The Barracuda NG Control Center supports multiple administrators simultaneously – even within the same configuration tree.

Audit control as requirement

Many IT departments expend considerable time and personnel resources in order to reconstruct the configuration of security gateways – because the responsible employee suddenly fell ill, because presumed “insignificant” changes were not documented or because complex object dependencies were not taken into account. While historically the lack of an audit trail was simply a costly inconvenience, the situation is no longer acceptable in today’s environment of growing regulations and increasing demands on auditability. Both traceability and audit control play a crucial role in modern security architecture management; Traceability for process and personnel management and audit controls for the preservation and recovery of configuration settings.

Unlike alternative solutions that rely on third-party auditing tools, the Barracuda NG Firewall has integrated its Revision Control System (RCS) directly into the security architecture so that the audit control cannot be circumvented either intentionally or unintentionally. The advantage lies in the absolute reliability and completeness of the recorded configurations changes, offering major benefits both for resolving faults and also providing evidence.

Auditing capabilities include:

Revision Control System

- Each individual component is versioned separately
- Each individual configuration entry is tracked separately
- Each individual configuration node can be set back to older versions
- Each individual configuration session can be tracked separately

Revision Control System

- Centralized reporting of network and user activities
- Fully automated report generation and delivery
- Simple configuration via a secure Web interface

Barracuda NG Firewall Management

The Barracuda NG Firewall offers unique capabilities to deliver an extraordinary high level of efficacy:

- A unique combination of profile- and device-based management approaches. Even very large gateway clusters can be managed economically by utilizing system similarities - without making any cuts in the depiction of individual requirements.

- The convergence of security, Traffic Intelligence, High Availability and WAN optimization also contributes to a major reduction in infrastructure complexity and enables the centralized management of important services.
- The integration of all Barracuda NG Firewalls into the Barracuda NG Control Center provides administrators with access to all functions allowing for a centralized management of globally distributed networks with a high level of audit control.

By combining these advantages, the Barracuda NG Firewall offers a unique solution for improving security and connectivity infrastructures for complex environments.

About the Barracuda NG Firewall

The Barracuda NG Firewall is a family of hardware, virtual appliances, software and services designed to protect the network infrastructure, improve site-to-site connectivity and simplify administration of network operations for enterprises and managed services providers. The Barracuda NG Firewall achieves this by tightly integrating a comprehensive set of next generation firewall technologies, including Layer 7 application profiling, intrusion prevention, Web filtering, malware protection, anti-spam and network access control. On top of these class leading next generation firewall capabilities, highly resilient VPN technology combined with intelligent traffic management capabilities allow customers to save line costs and increase overall network availability. Scalable centralized management of all aspects of the solution reduces administrative overhead and ensures policy compliance for local and remote locations.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.



Barracuda Networks

3175 S. Winchester Boulevard

Campbell, CA 95008

United States

+1 408.342.5400

www.barracuda.com

info@barracuda.com