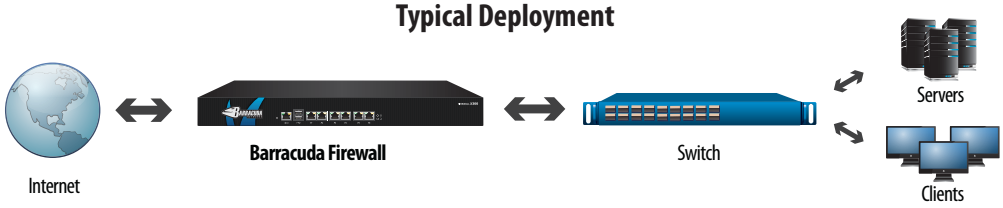
Barracuda Firewall Technology

The Barracuda Firewall is an application-aware network firewall appliance that leverages cloud resources to extend next-generation security and networking beyond the capabilities of legacy UTM products. Barracuda Firewall offers enterprise-grade security technology—including application control, user awareness, secure VPNs, link optimization, and advanced malware protection—but is designed for unsurpassed ease of use, and priced competitively. The Barracuda Cloud Control centralized management portal makes it easy and intuitive to deploy, configure, and manage the Barracuda Firewall from any location, and is included at no extra cost.

Complete Next-Generation Network Security

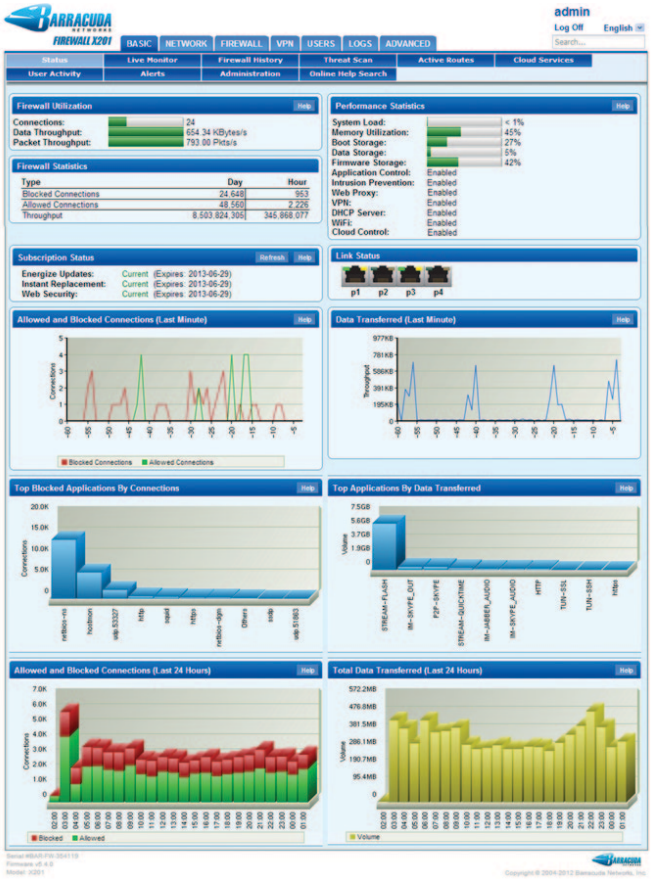
With integrated application and user visibility, along with support for multiple authentication methods and an optional local user database, the Barracuda Firewall enables highly granular policies defined by port, protocol, application, user, and time/date. For example, you might allow Skype chat at all times for everybody, but only allow Skype video at a certain time or for a certain user group. In addition, all models of the Barracuda Firewall protect unlimited IP addresses, and include an advanced intrusion prevention engine (IPS), as well as unlimited site-to-site and client-to-site secure VPN licenses.

Typical Deployment



Link Optimization Technology

The Barracuda Firewall includes advanced link balancing and traffic shaping capabilities to optimize business continuity and 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 if a disaster cuts all the landlines.



Future-Proof Investment Protection

By leveraging effectively limitless cloud resources for content filtering and malware protection, even smaller Barracuda Firewall units are able to scale easily as traffic and user numbers increase. The Energize Updates subscription service ensures that definitions and signature libraries are always up to date, and cloud-delivered firmware updates deliver new capabilities as required to address a constantly evolving threat landscape—no matter when you purchase your Barracuda Firewall, you'll always have the latest version.

Simple Pricing with No Surprises

Every Barracuda Firewall unit is delivered with all features and capabilities fully enabled. Content filtering and advanced malware protection in the cloud is offered as an affordable per-box subscription. Neither the Barracuda Firewall nor the Web Security Service have any associated per-user license fees—once you purchase the box and the service, you can scale up to the appliance's maximum capacity at no further cost. And the simple, intuitive Barracuda Cloud Control management portal is included free of charge.

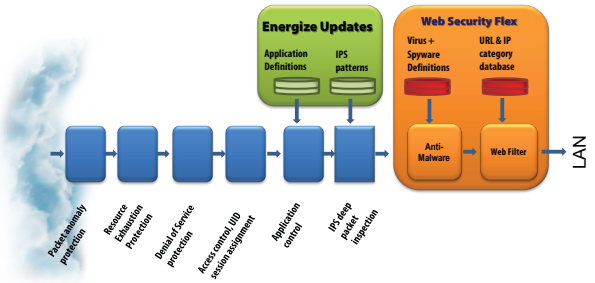
BARRACUDA FIREWALL TECHNOLOGY

MODEL
X200
X300
X400
X600

ADVANCED NETWORK SECURITY

In today's world of omnipresent botnets and other advanced threats, one of the main tasks of perimeter protection is to ensure ongoing availability of the network for legitimate requests and to filter out malicious denial of service (DoS) attacks. Barracuda Firewall achieves this via a series of advanced techniques:

- Barracuda Firewall DoS protection uses generic TCP proxy forwarding so that only legitimate TCP traffic gets into the network.
- Rate limits are applied to limit the number of sessions per source handled by the firewall. Packets arriving too quickly will simply be dropped.
- To prevent IP spoofing, the reverse routing path (RRP) to the packet's source IP address is checked. If the check uncovers a mismatch between incoming and reply interface, the packet is dropped.

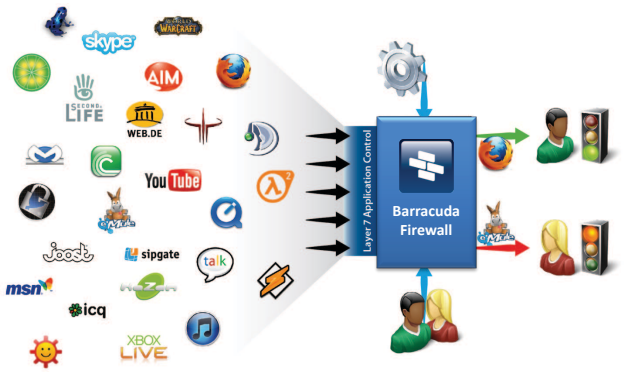


APPLICATION CONTROL

Barracuda Firewall can identify and enforce policy on sophisticated applications that hide their traffic inside otherwise "safe" port/protocols such as HTTP or HTTPS.

For example, Skype and peer-to-peer (P2P) applications are particularly evasive, requiring advanced application control for policy enforcement. Barracuda Firewall enforces policies based on application, user, location, and time/date. Actions include blocking, allowing, throttling, or even enabling or disabling specific application features.

Application control is built into the kernel of the Barracuda Firewall, using a combination of deep packet inspection and behavioral analysis to reliably detect more than 900 applications.

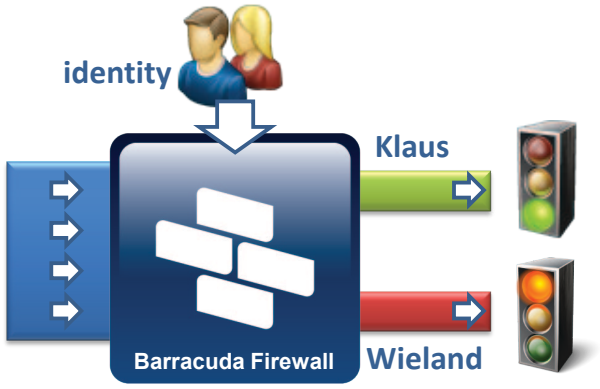


IDENTITY AWARENESS

Within any organization, different individuals or groups require access to different resources and applications. For example, marketers may need to use Facebook for their work, while for other groups it will only waste time and bandwidth.

To enforce policies that control access to resources and allocation of bandwidth, Barracuda Firewall identifies users based on IP address mapping. Role assignments based on identity and device posture checks can be used within the firewall to facilitate role-based access control (RBAC).

Barracuda Firewall supports authentication of users and enforcement of user-aware firewall rules, content inspection, and application control using Active Directory, NTLM, MS CHAP, RADIUS, RSA SecurID, LDAP/LDAPS, TACACS+ as well as authentication with x.509 certificates.



INTRUSION PREVENTION SYSTEM (IPS)

The Barracuda Firewall IPS is tightly integrated in the firewall architecture. It enhances network security by providing comprehensive real-time network protection against a broad range of network threats, vulnerabilities, exploits and exposures. It also keeps spyware and worms out of the corporate network in order to prevent fraud and to maintain strict privacy.

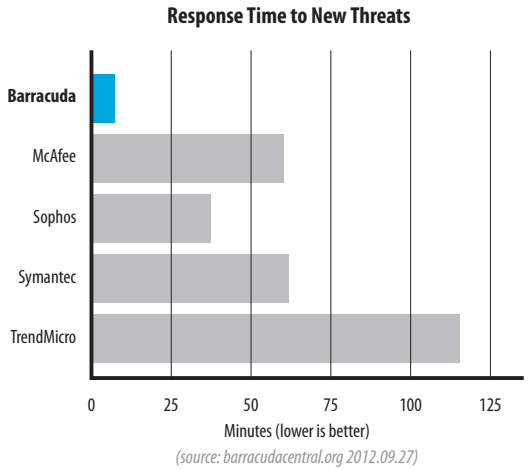
When an attack is detected, the Barracuda Firewall either drops the offending packets and sessions (while still allowing all other traffic to pass) or just logs the intrusion attempt. As part of the Energize Update subscription, signature updates are delivered in near real time as new exploits are identifies, to ensure the Barracuda Firewall is constantly up-to-date and aware of the latest threats and vulnerabilities.

The Firewall for the Cloud Era

BARRACUDA WEB SECURITY SERVICE

By moving CPU-intensive malware scanning and URL filtering tasks to the Barracuda Web Security cloud infrastructure, the Barracuda Firewall extends the capacity of on-premises compute resources. With virtually unlimited cloud resources, the Barracuda Firewall has the elasticity to scale dynamically as security needs change. Reporting is also handled in the cloud, further improving resource efficiency.

In addition, cloud integration ensures that signature libraries and threat definitions are always up to date—even as whole new threat categories emerge, your protection continues without interruption, unlike that provided by legacy UTMs, which must be replaced each time they need to defend against a new kind of threat.

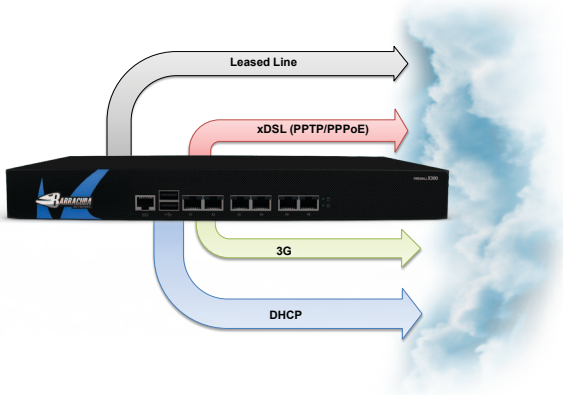


LINK OPTIMIZATION TECHNOLOGY

To ensure the best and most cost efficient connectivity, the Barracuda Firewall provides a wide range of built-in uplink options such as unlimited leased lines, up to six DHCP, up to four xDSL, and up to two ISDN and UMTS.

By eliminating the need to purchase additional devices for uplink balancing, security-conscious customers will have access to a WAN connection that never goes down, even if one or two of the existing WAN uplinks are severed.

Automatic failover ensures the next best uplink is activated on the fly, and all traffic is rerouted to make full use of the remaining links. Predefined load balancing policies make it particularly easy to share the bandwidth of multiple uplinks, and can prioritize specific application traffic or assign it to a specific link.



CENTRALIZED MANAGEMENT VIA THE CLOUD

Every Barracuda Firewall is integrated with Barracuda Cloud Control (BCC), which allows organizations to manage all their Barracuda Firewalls (along with most other Barracuda Networks solutions) through a single, consistent interface. This gives administrators a global view of all of their devices and ensures they are provisioned with the latest firmware, definitions, and security policies.

Combined with the configuration of Barracuda Web Security settings and reporting, this allows effectively all security settings to be centrally managed via one interface available on every Internet-connected device. BCC is included at no charge with every Barracuda Firewall unit. Users may also choose to manage each device directly through its own interface.

BARRACUDA FIREWALL

MODEL
X200
X300
X400
X600

Underlying Technology

Hardened Operating System

Security devices protecting the network at the perimeter need to be invulnerable to attacks. Barracuda Firewall is built on a hardened Linux operating system developed and optimized over the course of more than ten years.

A customized infrastructure layer provides the basic gateway properties and routing capabilities already in the Linux kernel. The system is protected against attacks on the system itself as well as all application functions hosted by the system via the integration of a separate Barracuda Firewall-based host firewall, inspecting all incoming and outgoing local traffic from and to the system.

Phion Core

Unlike other firewall products that simply enhance or augment standard Linux firewall packages, the core of every Barracuda Firewall is a specially developed application-controlled packet-forwarding firewall called the phion core. It is based on a combination of stateful packet forwarding, TCP stream forwarding, and application-layer gateways, enhanced by custom application plug-ins that handle complex protocols involving dynamic address or port negotiations.

The phion core technology delivers a best-of-both-worlds hybrid technology firewall that uses stateful packet forwarding as well as transparent circuit-level application proxying, and that provides generic interfaces for content scanning, bandwidth management, and VPN tunnel selection.