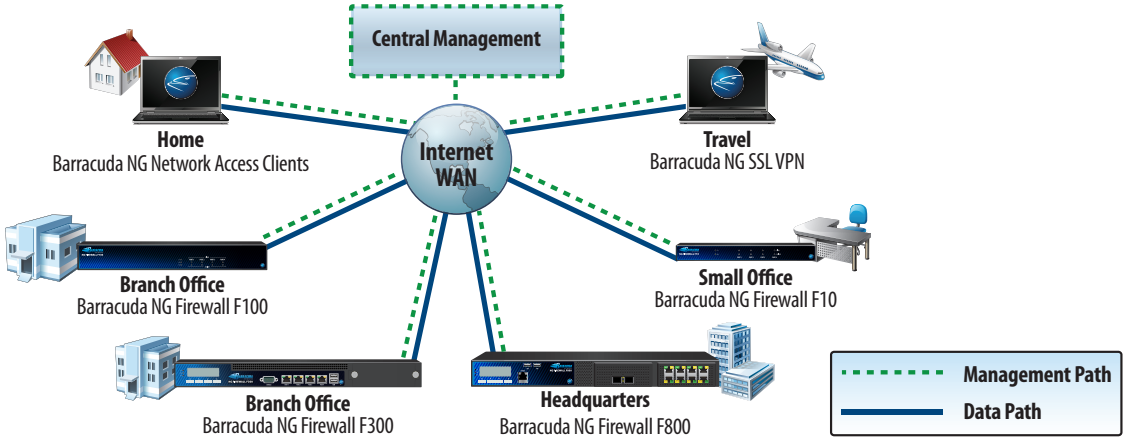
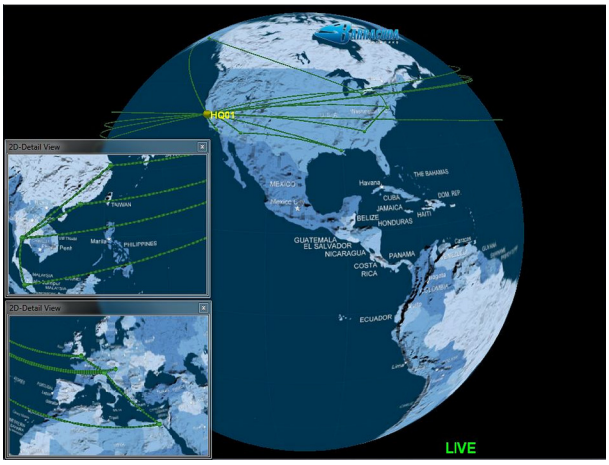
Barracuda NG Firewall Technology

The Barracuda NG Firewall is a family of hardware and virtual appliances designed to protect network infrastructure, improve site-to-site connectivity and simplify administration of network operations. Beyond its powerful network firewall and VPN technologies, the Barracuda NG Firewall integrates a comprehensive set of next generation firewall technologies, including Layer 7 Application Control, intrusion prevention, Web filtering, anti-virus, anti-spam and network access control.



The Barracuda NG Firewall offers a new and holistic approach to next generation firewall technology. Unlike other best-of-breed next generation firewalls, the Barracuda NG Firewall is designed and optimized for distributed environments where dozens or even thousands of locations need to be networked, protected and managed, and where employees must connect through virtual private network connections remotely from home offices or while traveling. The Barracuda NG Firewall enables cost effective management and enforcement of security policies throughout the entire Wide Area Network (WAN). Beyond advanced security mechanisms, Barracuda NG Firewalls provide application-aware traffic management and prioritization across the WAN. This includes fast and intelligent adaptive routing based on network traffic conditions and link status. If a quality WAN line goes down, a backup line is activated automatically and an alternate traffic shaping QoS policy is applied to make sure business-critical applications are assigned enough bandwidth. Optionally only a subset of networks or users might be serviced to make sure the most critical workstations or kiosk style terminals remain productive.



The Barracuda NG Earth provides graphical real-time 3D network monitoring of all VPN site-to-site tunnels and appliance status.

Complete Next Generation Firewall Capabilities:

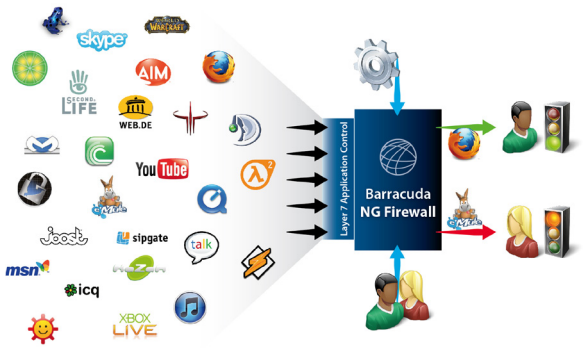
Network security threats have changed, and the old approach to network security is broken. Such new threats as social networking worms, botnets, shortened and obfuscated links, and other sophisticated attacks have changed the network security game. With increasing bandwidth demands, new Web 2.0 application architectures, and personal devices entering corporate networks, there has been a change in how protocols are used and how data is transferred. For normal firewalls, all traffic on port 80 and port 443 looks the same - the traditional firewall approach of defining proper port/protocol usage and stopping attacks looking for vulnerable servers or known bad signatures is insufficient for defending today's network. IPS techniques are not capable of identifying applications, let alone blocking them, disabling some of their features, or preventing their misuse. Moreover, enterprises today are tasked with re-architecting their network defensive postures around application-aware, next-generation firewalls augmented by adding multiple uplink redundancy, bandwidth control and identity-awareness.

BARRACUDA NG FIREWALL TECHNOLOGY

APPLICATION AND IDENTITY AWARENESS

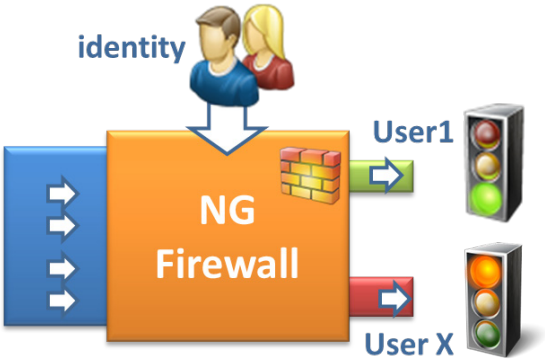
LAYER 7 APPLICATION CONTROL

Next generation firewalls utilizing Layer 7 Application Control can identify and enforce policy on more sophisticated applications, which may hide their traffic inside otherwise "safe" port/protocols such as HTTP. As an example: Skype and peer-to-peer (P2P) applications are particularly evasive protocols, requiring Layer 7 Application Control for policy enforcement. The Barracuda NG Firewall integrates Layer 7 Application Control into its core firewall functions, enabling enforcement of policies based on application, user ID, security posture, location and time of day. Policy actions include blocking, allowing, throttling, or even enabling or disabling specific application features. Layer 7 Application Control is embedded deep inside the kernel of the Barracuda NG Firewall, using a combination of deep packet inspection and behavioral analysis to reliably detect more than 800 applications even if they use advanced obfuscation and encryption techniques



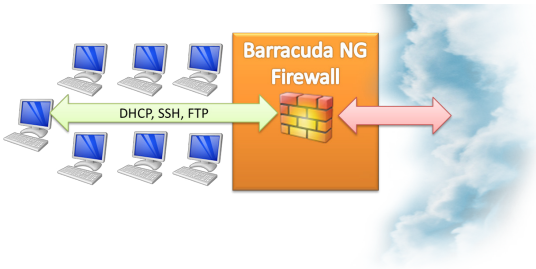
IDENTITY AWARE NETWORKING

Network users should not necessarily be treated equally. Most often there are business policies requiring access to the network shares for certain authenticated users, and not others. Allocation of more available bandwidth for preferred users or user groups and reduction of available bandwidth for others is a common task requiring the network device to know what user an IP actually belongs to. Barracuda NG Firewalls are user identity aware by linking a user to IP address mapping. Any role assignments that result from identity and device posture checks can be used within the firewall to facilitate role based access control (RBAC). Barracuda NG Firewalls support authentication of users and enforcement of user-aware firewall rules, Web filter settings and Layer 7 Application Control using Active Directory, NTLM, MS CHAP, RADIUS, RSA SecurID, LDAP/LDAPS, TACACS+ as well as authentication with x.509 certificates.



APPLICATION PROXIES

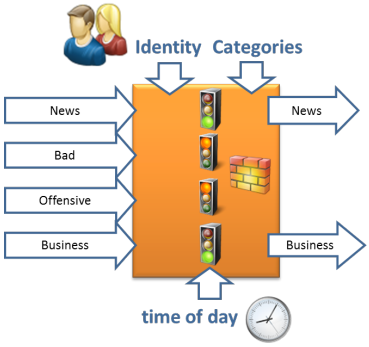
Typically companies aim to consolidate networking and security functions into fewer devices to save on management and infrastructure overhead. To aid in this, the Barracuda NG Firewall includes dedicated application proxies for FTP, SSH, DHCP, DNS, SMTP and POP3. The SSH proxy may be used with authentication enforcement, so the users have to identify themselves to the Barracuda NG Firewall prior to connecting to the desired remote target. Target access can be customized via easy to configure access lists on a per user basis and session activity can be recorded on request.



CONTENT SECURITY

WEB FILTER

The Barracuda NG Firewall protects user productivity, blocks malware downloads and other Web-based threats, and enables compliance by blocking access to unwanted Web sites and servers. With more than 100 million Web sites cataloged in 95 categories, Barracuda NG Web Filter is one step ahead of the latest unwanted Web content. The underlying database is constantly and automatically updated with up to 150,000 new Web pages every day. Internet access protected by the Barracuda NG Web Filter can easily be customized to match Internet access policies as it allows defining access rules by user, time frame and resulting action. Options range from simple performance restrictions, time-of-day regulations, posted warnings and complete blocks.

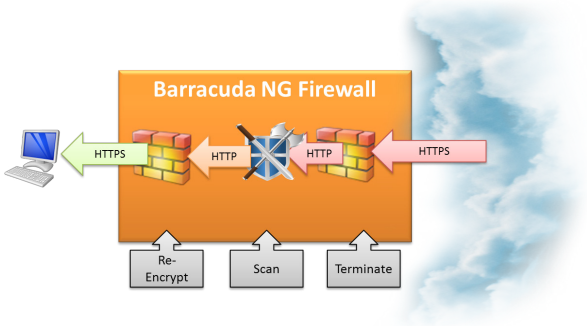


MALWARE PROTECTION

The Barracuda NG Malware Protection shields the internal network from malicious content through scanning of Web content (HTTP and HTTPS), email (SMTP, POP3) and file transfers (FTP) via two fully integrated anti-virus engines. Malware protection is based on regular signature updates as well as advanced heuristics to detect malware or other potentially unwanted programs even before signatures are available. The Barracuda NG Malware Protection covers viruses, worms, trojans, malicious java applets, and programs using known exploits on PDF, picture and office documents, macro viruses and many more, even when using stealth or morphing techniques for obfuscation.

SECURE WEB PROXY

The Barracuda NG Secure Web Proxy extends the reach of the Barracuda NG Web Filter and the Barracuda NG Malware Protection to cover even SSL encrypted HTTPS traffic. It effectively allows organizations to extend their security policies to also cover SSL traffic, allowing virus scanning and URL filtering on SSL encrypted Web sites. HTTPS traffic is decrypted temporarily for machine scanning purposes and never leaves the appliance as long as it is in plain text HTTP. The Barracuda NG Secure Web Proxy also checks for revoked certificates and prevents end-users from accidentally visiting malicious sites or connecting to malicious servers by blocking stolen or invalid certificates already at the network perimeter.



ENTERPRISE-CLASS FIREWALL AND IPS: NETWORK SECURITY

INTRUSION PREVENTION SYSTEM (IPS)

The Barracuda NG Firewall provides easy to use and immediate out-of-the box protection based on thousands of signatures covering a vast number of exploits and vulnerabilities in operating systems, applications and databases, thus preventing network attacks such as:

- SQL Injections and arbitrary Code Executions
- Access Control Attempts and Privilege Escalations
- Cross Site Scripting &Buffer Overflows
- Denial of Service (DoS) and Distributed Denial of Service (DDos) Attacks
- Directory Traversal and Probing and Scanning Attempts
- Backdoor Attacks, Trojans, Rootkits, Viruses, Worms and Spywares

Signature updates are delivered at least on a weekly schedule or on an emergency basis in order to ensure that the Barracuda NG Firewall is constantly up-to-date. For centrally managed units pattern updates are conveniently distributed by the Barracuda NG Control Center.

AID	Org	Scan Result
IPS Severity Critical (3)		
	FWD	RPC Windows RPC DCOM Interface exploit - 135
	FWD	EXPLOIT Ipswitch Imail IMAP server LOGIN stack overflow
	FWD	EXPLOIT eSignal v7.6 remote buffer overflow
IPS Severity High (533)		
IPS Severity Informational (1)		
	FWD	POLICY HTTP Proxy Server access attempt
IPS Severity Low (5)		
	FWD	VULN Protocol Telnet (ms telnet) S
	FWD	VULN Protocol ICMP (ms ping) S
	FWD	VULN Protocol HTTP (get request) U
	FWD	VULN Protocol HTTP (get request) S
	FWD	VULN Protocol FTP (multiple put) S
IPS Severity Medium (8)		
	FWD	WEB http ..\ directory traversal
	FWD	WEB http directory traversal
	FWD	WEB http ..%5C directory traversal
	FWD	WEB Sql injection command 1=1 attempt
	FWD	EXPLOIT Microsoft ASN.1 DoS -4
	FWD	DNS zone transfer TCP attempt

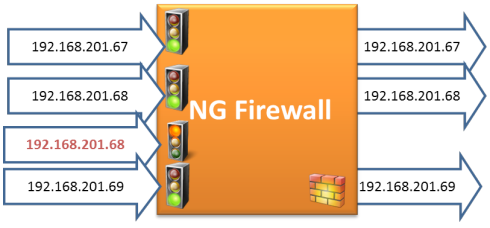
DENIAL OF SERVICE (DOS) PROTECTION

In today's world of omnipresent botnets, one of the main tasks of perimeter protection is to ensure ongoing availability of the network for legitimate requests and to filter malicious denial of service attacks. With TCP SYN Flood Protection, the Barracuda NG Firewall effectively functions as a generic TCP proxy, forwarding only legitimate TCP traffic to the inside of the network.

Additionally RESOURCE EXHAUSTION PROTECTION allows definition of a rate limit that is applied to the maximum number of sessions per source address handled by the firewall. Packets arriving at a rate faster than allowed will simply be dropped.

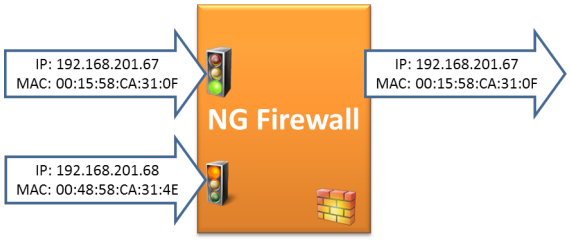
IP SPOOFING PROTECTION

To prevent IP spoofing, the reverse routing path (RRP) to the packet's source IP address is checked. Based on the routing table, the reply from the network interface has to leave the firewall in order to reach the sender. If the check results in a mismatch between the incoming and reply interface, the packet is dropped. Settings can be customized on a per rule basis. This protection mechanism is available for all protocols.



ARP SPOOFING PROTECTION

The Address Resolution Protocol (ARP) is a well-known attack point for infected machines trying to bring down a network. The Barracuda NG Firewall employs several ARP security mechanisms to prevent ARP spoofing, ARP cache flooding, and ARP cache trashing by immediately alerting suspicious behavior.



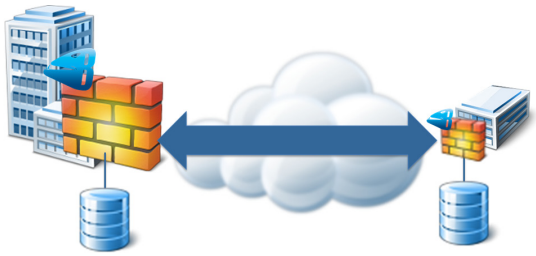
ADVANCED VPN CAPABILITIES

WAN OPTIMIZATION

Integrated Application Layer control makes sure only allowed traffic passes the firewall all while reaction times are optimized and WAN compression reduces bandwidth load by applying one or a combination of the following:

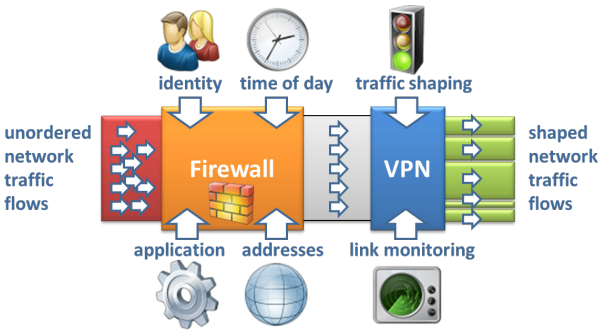
- Byte level caching (data deduplication) to the traffic stream inside the VPN tunnel between two Barracuda NG Firewall units.
- Built-in stream as well as packet based traffic compression.
- Caching of frequently accessed web content on the web proxy.

This effectively allows compression rates up to 95%, significantly reducing the bandwidth needed at remote locations while increasing network responsiveness.



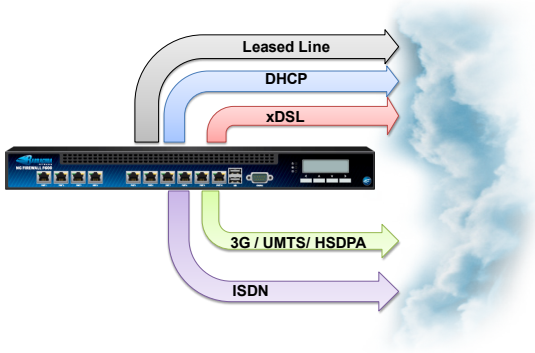
TRAFFIC SHAPING AND QOS

Limited network resources make bandwidth prioritization a necessity. The Barracuda NG Firewall enables traffic shaping which takes a number of factors - including time of day, application type and user identity - into account and prioritizes network resources accordingly. Traffic shaping is available inside VPN tunnels as well for the link outside the VPN tunnel to make sure remote locations are assigned enough bandwidth for business critical Web applications.



MULTIPLE UPLINK SUPPORT

To ensure the best and most cost efficient connectivity, the Barracuda NG 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. Further, traffic intelligence mechanisms make sure the next defined uplink is activated on the fly and all traffic is rerouted to make full use of the remaining lines. In the event that backup lines provide less bandwidth, traffic shaping automatically prioritizes business-critical applications, networks or distinct endpoints.



VPN WITH CUSTOMIZABLE ENCRYPTION

The secure remote connectivity of remote locations is a must-have in today's distributed business world. For this reason Barracuda NG Firewalls include unlimited site-to-site and client-to-site VPN functionality. VPN clients are available for Windows, Linux and Mac OS X. The Barracuda NG Firewall provides resilient site-to-site connectivity even across third party firewalls and network address translation devices. VPN tunnels are protected by heartbeat monitoring and auto reconnection in case of line loss. Encryption algorithms include a wide range of standards including AES128, AES256, DES, 3 DES, Blowfish etc. Optionally, customers may integrate their own encryption algorithms via a publicly available API.

VPNC CERTIFIED
Basic Interop

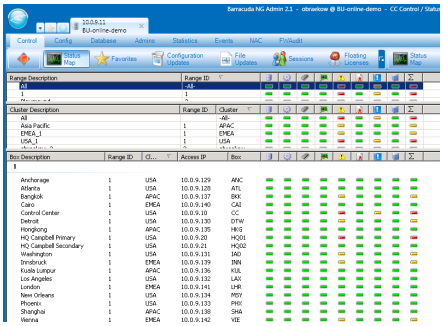
CENTRAL MANAGEMENT

Industry Leading Central Management:

Barracuda Networks provides a cost-effective solution for medium to large enterprises and service providers. The heart of this advanced functionality is the Barracuda NG Control Center that enables role-based central management for unlimited administrators on an unlimited number of appliances. The Barracuda NG Control Center allows administrators to configure all appliances, set and administer security and network access policies, control firmware, update revisions and manage user settings all from one easy-to-use central location.

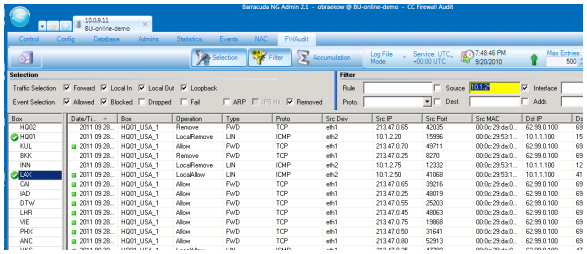
TEMPLATE-BASED MANAGEMENT

One of the main features that saves time for administrators is the ability to create reusable templates. Template-based configuration and globally available security objects enable efficient configuration across thousands of locations without the need to redefine the same settings over and over again. Via template-based central management, administrators need only define a setting once and can then create a referral link from multiple appliances to this setting in the template repository. Changes to templates at the Barracuda NG Control Center are available immediately throughout the network without further actions from the administrator.



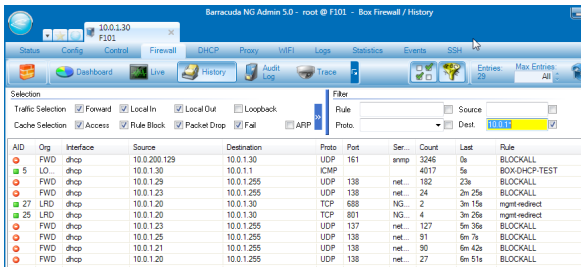
FIREWALL AUDIT

Drilling down on connectivity problems is a daily task for network administrators. Rather than relying on cryptic command lines, the Barracuda NG Control Center provides graphical data in the firewall audit view of all managed appliances and locations in real time. This gives administrators the ability to drill down on connectivity issues in a matter of seconds without the need for any command line interaction.



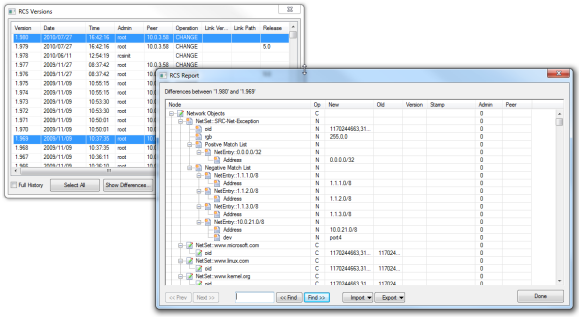
FIREWALL HISTORY

The firewall history view provides a graphical representation of current and recent active session and session requests on each Barracuda NG Firewall. By narrowing down the list quickly by Port/IP, protocol type, application traffic type, user etc., the firewall history gives administrators information about which rule has allowed or blocked these sessions.



COMPLIANCE AND REVISION CONTROL

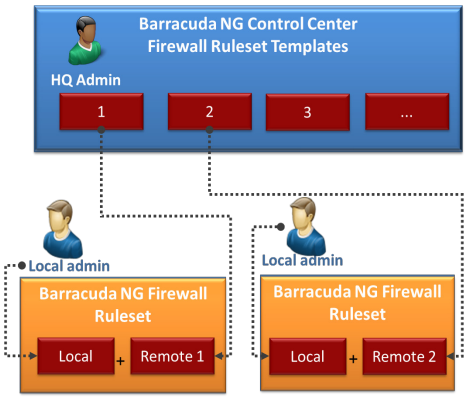
When multiple administrators manage a network of appliances for remote locations the inevitable question arises: Who changed x and why? For this reason the Barracuda NG Control Center includes a Revision Control System (RCS) that facilitates compliance and governmental regulations by tracking and documenting every single change to the system. This helps determine when changes take place, by whom, and from where with sophisticated reports.



CENTRAL MANAGEMENT

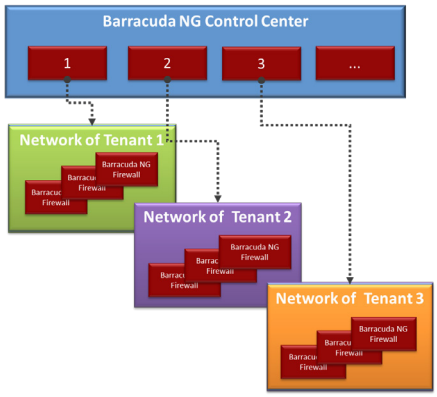
DISTRIBUTED FIREWALL

For complex, mid-size or large installations, local IT administrators usually need to have some form of authority on the network, i.e. they need to be able to manage the portion of the firewall rule set for which they are responsible. To facilitate this business need, Barracuda NG Firewalls include the option to have the overall firewall ruleset be logically divided into several distinct rule sets, each visible and manageable by appropriate administrators or linked to different centrally manageable repository entries. In distributed environments, this allows an organization to have a fixed set of firewall rules mandated via headquarters central management with a designated section inside the firewall ruleset to be managed by local staff.



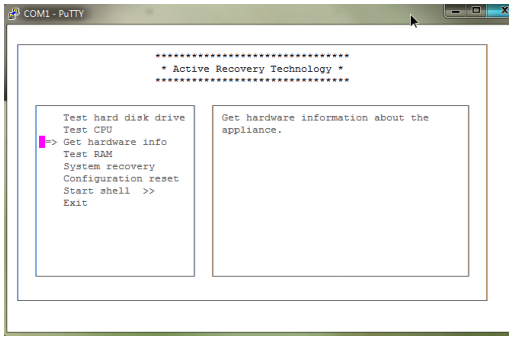
MULTI-TENANCY

Barracuda NG Control Centers provide support for multi-tenant management of remote Barracuda NG Firewalls, allowing the total logical segregation of groups of appliances within the central management user interface. This feature is especially valuable for service providers, as it allows administrators to define access to the Barracuda NG Control Center for individual tenants without the risk of allowing a client to see any information about another client. The multi-tenancy feature of the Barracuda NG Control Center effectively provides the functionality of multiple distinct Barracuda NG Control Centers within a single installation.



APPLIANCE RECOVERY TECHNOLOGY

To ensure the fast recovery of hardware or misconfiguration outages, the Barracuda NG Firewall can be restored to the last known working condition within minutes for remote connections via the embedded appliance recovery operating system. In the event setup of a spare Barracuda NG Firewall should become necessary, the included bootable USB thumb drive, and a single configuration archive, are sufficient to get the appliance up and running within a few minutes - even by untrained staff in remote locations such as point of sales shops, kiosks and small branch offices.



BARRACUDA NG FIREWALL TECHNOLOGY

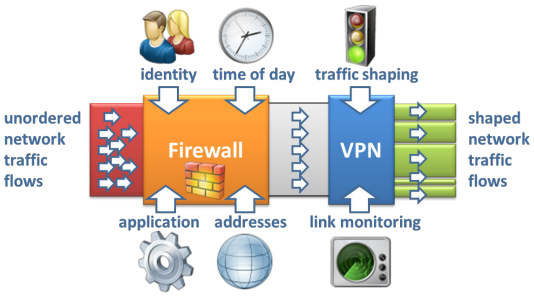
UNDERLYING TECHNOLOGY

HARDENED OPERATING SYSTEM

Security devices protecting the network at the perimeter need to be invulnerable to attacks. The Barracuda NG Firewall is based on more than 10 years of hardened Linux operating system experience. After the hardening process, a custom crafted infrastructure layer is added to provide 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 NG Firewall that inspects all incoming and outgoing local traffic.

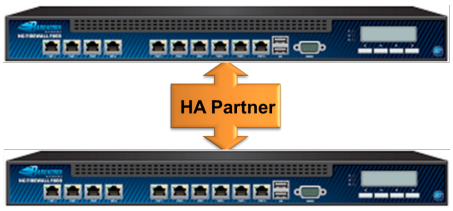
PHION CORE

Unlike other firewall products that simply enhance or augment standard Linux firewall packages, the next generation firewall in every Barracuda NG Firewall appliance is a specially developed application controlled, packet forwarding firewall called the phion core. The phion core technology represents a combination of stateful packet forwarding, TCP stream forwarding and application layer gateways which are enhanced by custom application plug-ins that take care of complex protocols involving dynamic address or port negotiations. The phion core technology implements the best-of-both-worlds: A hybrid technology firewall that uses stateful packet forwarding, as well as transparent circuit-level application proxying to provide generic interfaces for content scanning, bandwidth management and VPN tunnel selection.



HIGH AVAILABILITY AND TRANSPARENT FAILOVER

All Barracuda NG Firewalls can be deployed in tandem to provide interruption-free transparent failover to the backup system. The firewall engine on the backup system replicates the session table of the active gateway and will continue to forward traffic flows in the event the active gateway goes down unexpectedly or requires service disruptive maintenance such as hardware servicing or software updates.



BUILT IN CENTRAL MANAGEMENT

Unlike other next generation firewall solutions that offer only threat protection, the Barracuda NG Firewall has been designed from the ground up to include scalability and manageability. The management capabilities are easily replicated with the Barracuda NG Control Center, a special central management server which is also based on the Barracuda NG Firewall OS and augmented with a comprehensive set of central management services. By adding the concept of a control center, configuration tasks are accomplished through the central management server for an unlimited number of supported systems. Management specific features like template-driven objects, reusable global objects, user definable work views, and graphical representation of the global WAN network (see picture) make sure the complexity of securing distributed WAN networks remains manageable.