Overcoming Common Firewall Limitations

Improving your first line of network defense
with firewall technology that makes your network more secure and easier to manage

This whitepaper addresses the inherent flaws and limitations of most existing firewalls and how enterprises can use the Lucent VPN Firewall Brick® to create a next-generation firewall which delivers:

- Full-featured bridging
- Packet processing capability through secure Inferno™ OS
- Comprehensive security capabilities
- Centralized management through Lucent Security Management Server
- Native virtual firewall and resiliency
- IP Quality of Service
- Disaster recovery and continuity of business planning
- Attractive overall total cost of ownership

Lucent Technologies
Bell Labs Innovations



Contents

Summary....3

Inherent flaws in most firewalls....3

Limitations of software-based firewalls....4
Common hardware firewall limitations....4
Limitations of all-in-one systems....5
Other issues: cost, management and operation....6
Compromised security needs new thinking....7

Next-generation firewall capabilities....8

Summary....10

Next-generation features, today:
Lucent Technologies VPN Firewall Brick®....10

Full-featured bridging....11
Secure Inferno™ OS adds to packet processing capability....12
Comprehensive security capabilities....12
Centralized management through Lucent Security Management Server....13
Native virtual firewall and resiliency....14
IP Quality of Service....15
Disaster Recovery and Continuity of Business Planning....15
Attractive overall total cost of ownership....16
Conclusion....16

Summary

Firewalls, intrusion detection systems and other security devices play a vital role in securing corporate networks against malicious traffic from untrusted networks. Nevertheless, most firewall systems contain inherent design flaws and limitations that hinder even the most diligent efforts of IT staff. These weaknesses often exist because the firewall has been created by stretching the capabilities of another device, which was not originally designed for network security. As a result, vulnerabilities remain, which hackers can exploit as they continue to develop new techniques to cripple or break through corporate networks. The limitations of these firewalls also add to capital and operating costs, as IT staff puts in additional time and effort — and purchases additional equipment — to compensate for inhernet flaws.

To ease security concerns and lower costs, IT staff need to take advantage of key next-generation firewall features today. The crucial capabilities include: bridging instead of routing, powerful packet processing, high availability, robust security, Quality of Service (QoS) and full support for virtual firewalls. With these features in place, firewalls can reduce design and management time and minimize the total cost of ownership of a security infrastructure. Enterprises from healthcare to financial institutions can achieve savings from shorter installation time and fewer management hours to keep their network protected at all times.

This paper provides a detailed look at the limitations of most firewalls and their business and security implications — and discusses key capabilities needed to overcome security issues. It also outlines how Lucent's VPN Firewall Brick® product line meets the challenge of providing next-generation firewall capabilities today.

Inherent flaws in most firewalls

Today, the challenges of choosing, implementing, managing and upgrading a security infrastructure are daunting — whether a network security staff facing hectic day-to-day responsibilities of protecting enterprise data or the exhausting rollouts of a managed security service provider.

To keep untrusted traffic out, corporate IT staff employ wide-ranging efforts — implementing comprehensive security policies through a combination of firewalls, anti-virus and URL content filtering servers, along with secured VPNs deployed at key points in the network. Nevertheless, today's corporate networks continue to face serious security threats. Hackers work tirelessly to develop new techniques designed to degrade and compromise any available network. To protect against the ever-changing face of malicious attacks, security staff must regularly install patches or upgrades to their firewalls, which only protects the network until the next attack comes along to exploit remaining vulnerabilities.

In this challenging environment, IT staffs are hindered by the fact that most firewall systems currently exhibit weaknesses and disadvantages and they:

- Contain unrecognized security holes
- Take significant time to configure and install
- Require additional capital costs to add more features and functions

These issues arise in both software-based firewalls — which operate on top of Linux® or UNIX® or Windows® NT platforms — and hardware products that are either standalone or part of a larger switch/router element. Some limitations are inherent because most firewalls were originally built for other purposes. Vendors then pushed the existing design parameters of their appliances to provide more advanced security features.

All-in-one dynamic-router/firewall/VPN-gateways, essentially a router with firewall/VPN code enabled, control access at a network level, but is slower, less secure and less resistant to attack than a dedicated firewall.

The following sections provide a more detailed look at these concerns and their business implications.

Limitations of software-based firewalls

Patching. Software firewalls run on top of an operating system that is not optimized for security and may exhibit open ports. To compensate, firewall vendors incorporate software to harden these operating systems — and block open ports and repel attacks that can lead to buffer overflow and denial of service (DoS). Keeping this software secure requires regular patches and updates that add to maintenance time and expense.

Limited performance. Because these operating systems are neither designed nor optimized for the functions of a firewall, they have minimal capacity to perform packet inspection and policy administration — or manage large numbers of sessions. Without the ability to support a large number of sessions, with encrypted connections for VPN and reliable high throughput, the systems can offer only mid-level performance that requires additional firewalls to scale. This weakness calls for careful capacity planning and adds to the cost of network growth.

Insecure routing stacks. Another inherent problem of software firewalls is their reliance on the network stacks of popular operating systems that are built for PCs and servers, not network devices. Using these sub-optimal and insecure routing stacks, these firewalls attempt to filter packets intercepted between the hardware level and the network level in the OS, while remaining vulnerable to any unrecognized flaws — as packets are shuttled back and forth between Ethernet cards.

Common hardware firewall limitations

Inflexibility. Current hardware firewalls have eliminated some of the problems found in software-based systems. For example, they use a thinner OS that helps accelerate packet processing. However, most hardware firewalls exhibit a key weakness that leaves them open to attack or makes installation cumbersome — they use layer 3 routing.

Placing a firewall within a functioning network demands serious consideration: How will the firewall affect routing? How can routing and hardware changes be made with minimal service impact? How will the firewall restrict network growth? Most of these challenges are affected by the historical development of firewalls as packet filtering routers. Although these devices are now more secure and more feature-rich than simple access control lists on routers, they leave heavy footprints on a network. They hamper network topologies by tying firewalls to routing, segmentation of the network and interface gateway configuration. With this rigidity, it becomes difficult for a security staff to provide depth of defense throughout their network, and adding firewalls to new network segments remains an overwhelming task. This inflexibility translates into increased design and implementation costs.

Low degree of stealth. Even after all this dedicated effort, the segmentation that makes routed firewalling possible offers a low degree of stealth. This leaves networks vulnerable to common scanning techniques. Bridging offers a better alternative but some firewall vendors have reduced feature sets for their bridging mode. Bridging firewalls that can't accept Virtual Local Area Network (VLAN) tags, provide QoS or operate in dynamic addressing and address translation environments do little to ease the headaches of network security staff.

Limitations of all-in-one systems

Less resistant to attack

Some routers, web proxy caches, and even monitoring systems claim to provide firewall and security gateway functions in addition to their primary purposes. However, these all-in-one hardware and software systems have well-known, published vulnerabilities that make them less resistant to attack than dedicated firewalls and detrimental where mission-critical network resources are at stake. These vulnerabilities can be exploited, allowing penetration and easy access to network resources.

Router-based firewall software is designed to limit these published vulnerabilities but often offer only subsets of needed attack resistance features. Adding needed protective features such as TCP sanity, IP header validity, flood resistance, and fragment reassembly verification would quickly consume router memory resources needed for routing. These features are standard in dedicated firewall appliances.

Lengthy failover

When switching traffic and providing network security at the same time, all-in-one routers may experience ten or more seconds of failover, as their networks converge. This impacts existing sessions and becomes a network choke point. Firewalls that bridge or switch traffic (i.e., in transparent mode) can achieve sub-second failover since they use virtual MAC addresses with specialized algorithms for health checks and sharing of state tables.

Higher latency

When vendors add firewall functionality to their routers, they rarely accompany the software upgrade with new processors, or do so at additional cost. Firewall functions such as packet inspection and forwarding decisions increase packet latency through the router firewall and undermines its ability to perform its primary task -- moving valid traffic through the network while keeping unwanted traffic out, when under attack. This higher latency makes it difficult for router firewalls to achieve wire-speed operation, impacting their use in the network perimeter.

Less nimble in responding to emerging threats

Routers are in the choke points of the network so their high-availability needs to be assured. All-in-one firewall routers require additional quality assurance than dedicated firewall appliances. The software patches needed to protect against new attacks are often tied to normal router software releases so protection can be delayed, compromising network security.

Other issues: cost, management and operation

Both software-based and hardware firewalls have other drawbacks that can add to the overall management cost and time. These issues include:

- Licensing fees that apply when expanding user services and capacity
- Management focused on individual devices, rather than centralized management of the whole security infrastructure
- Ineffective support for virtual firewalls, so security policies cannot be tailored efficiently by user groups

Added fees. The pricing structure imposed by firewall vendors significantly affects the total cost of ownership. As an installed system needs more functionality, firewall vendors add on new charges. For example, fees might apply when adding support for more IP addresses or virtual firewalls — or increasing the number of client users.

Management limitations. When the corporate network grows large enough to need firewall management, the IT staff may face the challenges of purchasing and administering a separate database. Today, most management designs focus on firewall devices, instead of devices and management servers as part of a whole. The result is a lack of scalability. As companies add firewall devices, they generally need to install additional management servers, driving up total costs.

Ineffective support for virtual firewalls. Today, virtual firewalls offer an important management device that can streamline implementation of corporate security policies, while providing the flexibility to assign different security profiles to defined classes of employees, known as "user groups." Network traffic is then classified into management units based upon the IP addresses defined for the user groups. Ideally, each virtual firewall would have its own set of content filters, authentication and access policies; and this segmentation of employees and security policies should be friendly to layer 2 environments that use VLAN tags.

When these requirements are supported, virtual firewalls efficiently enable each user group to have the data access it requires, and no more. For example, sales management could view sales servers and finance servers within the trusted network or from across the Internet, while sales staff would be restricted to sales servers only. Unfortunately, most firewalls now provide only low to medium-duty support for virtual firewalls.

Compromised security needs new thinking

The inherent flaws and weaknesses of most firewalls add time and expense to the process of securing enterprise networks. While an IT staff often experiences overtime and stress in order to manage corporate security policies, their effectiveness is still constrained by the limitations of the devices they typically rely on, as summarized in Table 1.

Software Firewall Limitations	Hardware Firewall Limitations
High capital costs resulting from licensing fees for added features and functions	Higher operating costs, due to intensive network design for proper installation
Additional code required to harden third-party OS, along with patches to minimize security holes	Bridging mode unavailable, or feature set is reduced
Additional costs of PCs and maintenance	Non-stealthy operation
Medium-duty packet processing performance requires more systems	Feature-weak virtual firewalls limits flexibility when applying security policies
Unsecured routing stack on third party OS used to route between configured Ethernet ports	Increased capital cost, when database software licensing fees apply
Non-stealthy operation	Device-centered management minimizes scalability

Table 1: Summary of Inherent Firewall Limitations

For increased effectiveness and lower costs, network professionals need a fresh view of security, along with systems that offer next-generation firewall capabilities today. By incorporating crucial advanced features, leading-edge firewalls can eliminate typical vulnerabilities, yet still meet the cost of ownership rules imposed by corporate budgets.

Next-generation firewall capabilities

To provide security beyond the constraints of most existing software and hardware firewalls, networks need the following cost-effective, high-performance capabilities:

- Support for full-feature bridging, allowing in-depth network installation and stealth
- High-performing packet processing to support large numbers of sessions and encrypted connections
- Robust security capabilities to repel attacks
- Centralized management — from ten systems up to a thousand
- High availability
- Support for QoS and security policy segmentation through VLANs and virtual firewalls
- Comprehensive VPN support
- Superior total cost of ownership without onerous licensing schemes and time-consuming installation and management

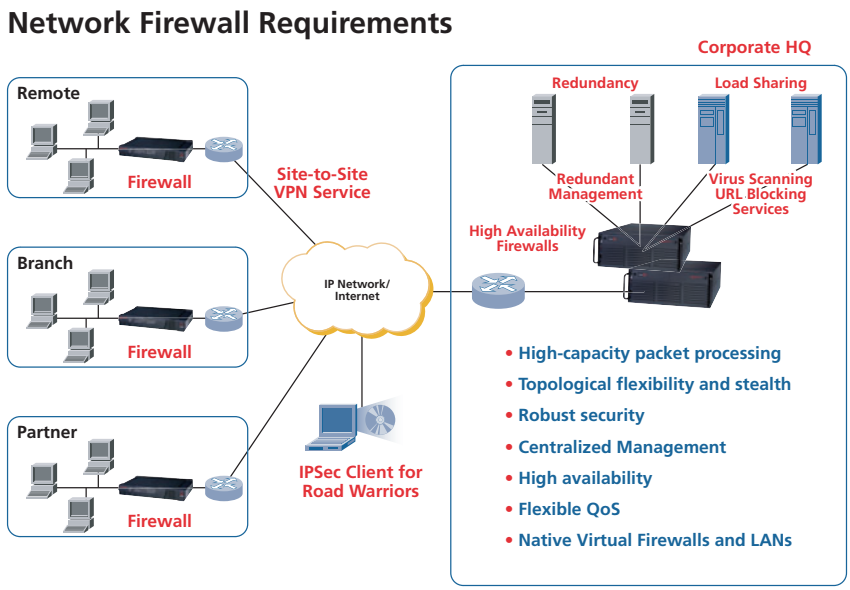

Diagram 1: Network firewall corporate needs

Bridging. Firewalls built with bridging capabilities can overcome some key limitations of typical hardware firewalls. Most importantly, they can be installed between any layer 3 devices without affecting routing. By separating the firewall from the routing process, the firewall remains a pure packet processor, free from any vulnerability connected to routing topologies or dynamic routing protocol attacks. Often, the bridging firewall can be installed as fast as a physical connection can be made. Since a bridging firewall does not require dedicated network segmentation, the security infrastructure can deliver a depth of defense previously unachievable. A firewall can be placed anywhere in the network that has an available IP address, where it can be managed in the same way as any Ethernet switch that has an IP address.

Stealth. Because the bridging firewall remains a layer 2 device, it offers a much higher degree of stealth than its layer 3 predecessors.

Security capabilities. Internet Protocol (IP) was never designed for secure transport on public networks. It was designed to provide a redundant communication path on military networks that were already secure and totally private. Protecting information systems has always been a challenge of risk management — limiting losses to an acceptable level, warranted by the gains of centralizing or broadening access to resources. Almost every level of the Open System Interconnection (OSI) model contains vulnerabilities: lines can be tapped, Address Resolution Protocol (ARP) caches can be poisoned, addresses can be spoofed, packet fragments can be offset, half-open connections can be cast and viruses and malicious code can commandeer unsuspecting systems to launch attacks for hackers.

Applications themselves pose challenges. For example, voice-over-IP (VoIP) sessions use multiple ports for signaling and data, which leaves pinholes in firewall policies that lack application awareness. A firewall must offer remedies that meet the challenges of today's increasingly vicious and ingenious hackers — and offer no vulnerabilities of its own.

Processing. To support today's resource-hungry processes, a firewall must process packets fast enough to maintain the network's performance.

Centralized management. Because firewalls impact network processes to a profound degree, they need scalable centralized management to minimize the cost of ownership. Without centralized control over policies, reports, monitoring and authentication, managing a firewall infrastructure is nearly impossible. The time it takes to add non-integrated services saps the budget of any IT staff.

Secure communication. Centralized management must be accompanied by a secure communication protocol to the management server. This built-in protocol can also optimize resources by using peer-to-peer key distribution algorithms to save time on re-keying, symmetric encryption algorithms for efficient encryption of data and digital signatures for integrity and authentication. As soon as the ideal firewall boots, based upon configuration information, it will contact its management server and proceed to download and update policies, report device and network status, perform authentication and make reports on transactions that cross the device. This centralization of management tasks reduces time and resource requirements.

Scalable management. Centralized management capabilities must include the ability to support growth cost-effectively. That means it must be able to manage just a few devices or up to a thousand devices. Without this scalability, the purpose of centralized management is lost altogether.

Resilience and high availability. Rapid failover for the synchronization of state tables at the session level is mandatory to maintain the vitality of network applications that rely upon the security services of a firewall. And NEBS™ Level III adds to the reliability for critical data center applications. The firewall's management application should also failover to another device in response to network or power outage, or even physical destruction. With the capability for active/active or active/passive failover, not only can network services be maintained, but a security infrastructure can endure beyond an isolated destructive event.

Virtual firewalls. Because they can allot network privileges on the basis of user groups and categories, virtual firewalls have become an indispensable tool for implementing security policies. Whether they are used to segregate departments within an enterprise or separate hosts in a data center, linking policies to virtual firewalls simplifies management. Virtual firewalls that incorporate the definition of user groups within policies can simplify administration even further, because network objects can be added or deleted conveniently from the user group rather than the policy rule. Some virtual firewalls even add the flexibility of accepting VLAN tags, so filtering can be applied to networks anywhere in a layer 2 switched environment.

Quality of Service (QoS). With VLANs, QoS has become a critical application. At the most basic level, it is necessary because IP is naturally bursty and attempts to consume available bandwidth, compromising other sessions. More importantly, malicious attacks often attempt to flood a network or specific firewall devices with erroneous traffic to deny network service. Without the ability to control and limit bandwidth to network segments, devices, applications and sessions, IT infrastructure becomes vulnerable.

Comprehensive VPN support. Today's enterprises require secure connections that allow off-site PC users, remote offices and branch offices to gain safe access to the corporate network. Consequently, the ideal firewall must offer the capacity and security to build VPNs using available access methods. This capability should include LAN-to-LAN and client-to-LAN connections — with cryptographic support for protocols. such as Diffie-Hellman, 3DES, SH-1, MD-5, PKI and Secure ID. It also requires the processing power to handle thousands of sessions per second. Secure IPSec tunnels at high throughput rates offer the necessary performance to keep efficiency and productivity up.

Summary

Firewalls can combine the greatest security and cost effectiveness when they incorporate key next-generation capabilities, including: bridging instead of routing, powerful packet processing, high availability, robust security and QoS. With these features, the devices can reduce the time required for design and management and minimize the total cost of ownership for a security infrastructure.

Next-generation features, today: Lucent Technologies VPN Firewall Brick®

A major issue for IT staff is the lack of time to create a secure corporate environment. They are frequently overworked and deal with constant security challenges while implementing corporate policies and attempting to prevent network vulnerabilities. The Lucent VPN Firewall Brick® optimizes the efforts of IT staff by reducing time to service, minimizing operational and capital costs — and offering superior security capabilities, high availability and integrated centralized management.

In other words, Lucent's VPN Firewall Brick® offers valuable next-generation capabilities for today's networks. These key features make it more secure, more flexible and easier to manage than other VPN firewall products, and it offers greater capacity as well. More specifically, the Brick:

- Supports full-featured bridging for depth of defense network deployment and stealth
- Supports comprehensive security features
- Uses the slender, highly secure Inferno™ OS, which enables powerful packet processing
- Offers high-device-count centralized management for ease of deployment, operation and support
- Maintains resilient operation, with high availability throughout the security infrastructure
- Includes native support for virtual firewalls

The Brick's capabilities stem from a superior network firewall paradigm. Most firewalls were originally built as packet filtering routers with access control lists. Vendors then attempted to force-fit these appliances to provide advanced feature sets. The Brick was built, from day one, as a hybrid bridge/router with virtual firewalls — a data management structure in the packet processing model that correlates a set of IP addresses to policies or VLANs. As a result, the Brick offers greater topological flexibility, as well as the following rich features that span the Brick portfolio.

Full-featured bridging

With its native bridging ability, the Lucent VPN Firewall Brick® remains stealthier than routed firewalls. Even if the Brick sits between hosts and a gateway router, the ARP cache of each device still looks to the router as its default gateway — because the Brick can bridge. Consequently, it remains very difficult to scan for the Brick. In some cases, it is completely invisible to any device not on the same segment. And hackers can't attack what they can't see.

As another benefit of bridging, the Brick can be implemented wherever the network has a free IP address — just as soon as a physical connection is made. There's no need to re-segment a network or worry about downtime as the network tries to converge to a new topology or wait as hosts are redirected to a new gateway. As soon as an Ethernet cable is snapped in, the Brick is in business. The Brick also provides native Ethernet switching that handles 802.1q VLAN tags. Yet it continues to support all features — unlike other appliances whose features may not work with either bridging or VLAN tags. With this kind of flexibility, enterprise or managed security service provider rollouts can be streamlined.

Secure Inferno™ OS adds to packet processing capability

The Inferno™ OS, designed at Bell Labs by the developers of the original UNIX®, is a revolutionary operating system. Unlike most operating systems that operate on a single hardware device, a distributed OS spans many different devices in different geographic regions — while maintaining centralized management. Imagine, for a moment, that your computer could be split into parts, with its jobs distributed to different computers, and your network served as a bus. One network device would function as a file server instead of a hard disk. Another would become a terminal instead of a traditional tower or laptop, and yet another might be the CPU cycle server. This kind of OS must be highly efficient to gain the most from hardware. It must also be very small — able to run on as little as one megabyte of memory. In addition, it requires a peer-to-peer, encrypted communications protocol, so that distributed devices could communicate, along with native networking features. The Inferno™ OS has all these features and more.

Unlike server operating systems forced to pushed beyond their native design to become firewalls, the Brick was built for security from the ground up. And the Inferno™ OS makes a key contribution to the Brick's innate advantages. For example:

- There are no superfluous features for hackers to exploit, as they would with other firewalls running on an OS that needs to be hardened — at the cost of IT talent and time.
- The trim Inferno™ frees up memory that can be used to manage a remarkable number of sessions — 3,000,000 on the Brick 1100 — as well as 30,000 rules among all virtual firewalls.
- The Brick is a packet processing phenomenon — offering a capacity of 3 Gbps of clear text on the Brick 1100 and just under 1 Gbps of 3DES. It also supports 23,000 new sessions per second and 1,164,970 pps (64-byte UDP packets).
- Each VPN Firewall Brick® is built with an encrypted peer-to-peer communication protocol, so that policies, reports and monitoring of up to 1000 firewall appliances can be effortlessly managed from the Lucent Security Management Server.

These features combine to deliver heavy-duty performance from the firewall infrastructure.

Comprehensive security capabilities

The Lucent VPN Firewall Brick® also provides the following security features that deliver comprehensive security, protecting against multiple network threats:

- TCP states are rigidly enforced to deny attackers the opportunity to use common scanning techniques to map networks and identify potentially vulnerable systems.
- Malformed packets that target OS bugs, such as the land attack, are discarded before they can damage hosts.

- Floods, such as ping floods and others, are stopped in their tracks with QoS controls.
- Connection-oriented DoS attacks, such as syn-floods, are defeated at the firewall, because patented intelligent cache management technology identifies malicious traffic and then resets open connections, allowing other traffic to be processed reliably.
- Fragmented streams of traffic are reassembled and analyzed to preserve legitimate traffic — while eliminating DoS attacks, like teardrop, which attempt to fill fragment re-assembly queues and shut down services.
- Initial Sequence Numbers (ISN) are rewritten for weak TCP stack implementations.
- VoIP application awareness allows telephony applications to use multiple dynamic ports for data and signaling without leaving pinholes in traffic enforcement policies for exploitation.
- With the aid of the Lucent Proxy Agent and best-of-breed third-party applications, HTTP and SMTP sessions are inspected for: protocol attacks like URL buffer overflows; backdoors like wiz and debug; viruses and malicious code; and violations of content policy that expose organizations to loss and liability.
- IP headers are validated to protect against buffer overflows, land attacks (SrcIP = DstIP), forged IP checksums, source routing options and other assaults.

Built on a platform that uses a highly optimized algorithm for filtering packets, the Brick offers convenient implementation, as well as speed and security. It requires no Common Language Infrastructure (CLI) to apply filtering but incorporates an intuitive graphic user interface instead. Service group templates, such as HTTP, FTP, and Telnet, are preconfigured to save time, and new templates are easily added.

Centralized management through Lucent Security Management Server

The Brick's flexibility and power are efficiently directed by the Lucent Security Management Server (LSMS). Unlike some management systems that can only control subsets of functionality, the LSMS controls every feature of the Bricks' VPN, QoS, VLAN, authentication, policy, reporting, monitoring and alarm generation capabilities. Because the LSMS offers high-count device management, this level of control can be applied to as many as 1000 Bricks.

The LSMS also offers greater flexibility for assigning specific role-based security privileges. A super-user, the LSMS Administrator, controls all management of the LSMS, such as creating group administrators, managing devices, setting up alarms and making reports. A group administrator can also be given full — or view-only — privileges over devices, policies and user groups. This powerful granularity allows large security infrastructures to grow without the usual challenges of scale.

For example, a trans-national corporation could create separate administration groups for each continent, or even each country where they operate. A managed security service provider could offer its customers either full or view-only privileges for each part of their security infrastructure. This might include view-only privileges for policies and devices, while full privileges would be available for users and user groups, since the company would want flexibility in the addition and deletion of employees. Data centers could offer similar capabilities to their customers. When companies are co-located behind the same VPN Brick Firewall®, they can even have administrative privileges over their corresponding partitions of the very same security device — without viewing or influencing any other data center customer.

These management roles can be accessed through the server itself — or through the LSMS Remote Navigator, a Web-based application that is encrypted by the Lucent IPSec Client. Upgrades are also managed from the LSMS, where new code can be automatically distributed through a 1000-firewall infrastructure with just a few clicks of a mouse. Administrators can even send instant messages to other active administrators through the LSMS or view real-time logs from each firewall.

Native virtual firewall and resiliency

From the outset, the Brick was designed to support virtual firewalls — data structures within the Brick's packet processing model that simplify management. They achieve greater efficiency by organizing firewall rules into units that are defined by sets of IP addresses or VLAN tags — and correspond to physical ports. These units streamline implementation of a security policy, because each virtual firewall corresponds directly to specific privileges for the devices delineated in the policy. Instead of applying one gargantuan access list to an interface, the administrator can use separate virtual firewalls to gain a clear picture of the implemented policy and update privileges without unintended consequences. Virtual firewalls can be used to divide administration privileges, as found in data centers, buildings supported by a fiber infrastructure and large enterprises.

Because virtual firewalls are defined by IP addresses or, optionally, a corresponding VLAN tag, the Brick can conveniently enforce security policies applied to entire segments of the network, since it slips into the infrastructure without disruption. Furthermore, since virtual firewalls have always been a feature of the Brick's design, all features work with virtual firewalls. No extra licensing fee is required for these capabilities, and every model in the Brick portfolio has this feature, from the Brick 20 with 20 virtual firewalls designed for Small Office Home Offices (SOHOs) to the Brick 1100 with 1000 virtual firewalls to meet the needs of large enterprises and data centers.

IP Quality of Service

Integrating QoS into a network is no longer just an issue of performance. As Distributed Denial of Service (DDoS) attacks marshal armies of zombie computers against single-server applications, like e-mail or a Web server, bandwidth limiting is as important for securing the reliability of resources as for maintaining the client experience. Here the Brick excels with granularity far beyond its peers. Unlike many firewalls and routers that do incorporate QoS but offer only tens of classifications of traffic, the Brick classifies traffic on the basis of physical interface, virtual firewall, policy rule and session. Within these categories, bandwidth can be both guaranteed and limited. These options allow for a simpler and more effective security implementation.

Disaster Recovery and Continuity of Business Planning

The redundancy features of the Brick and LSMS also offer a superior design. Each Brick can be configured — to the session level — with an identical model for active/standby high availability. This failover needs no special cables or external network reconfiguration. It combines the protection and resilience that electronic commerce and media hosts demand to sustain performance for their users. In addition, the Brick comes with NEBS™ Level III data center and managed service provider central-site versions. For added reliability, the LSMS itself can be configured for active/active or active/standby redundancy to support disaster recovery and continuity of business planning.

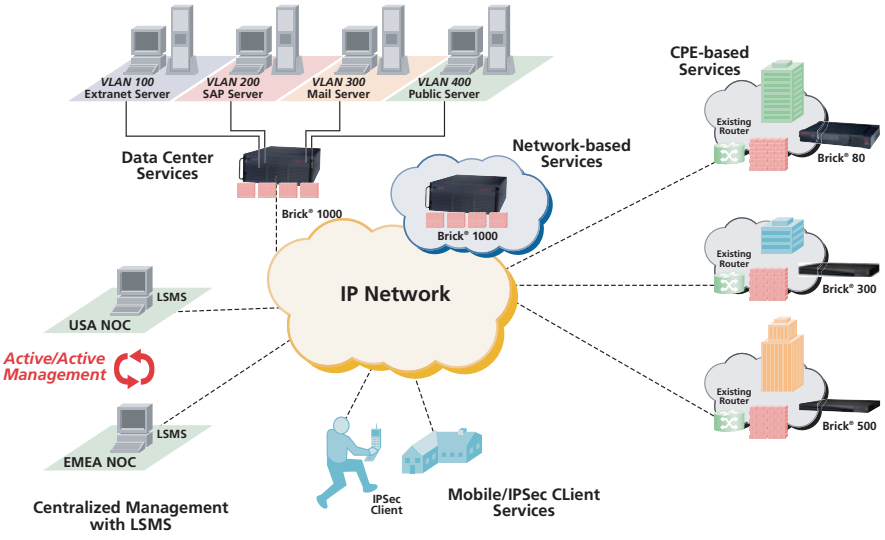

Diagram 2: Brick deployment flexibility across corporate network

Attractive overall total cost of ownership

The Lucent VPN Firewall Brick® portfolio reduces IT staff hours and shortens time to service with its full-featured bridging support and LSMS centralized management. It also decreases capital expenditures with powerful packet processing that minimizes firewall equipment needs; and it replaces costly feature-licensing schemes with a simplified, upfront pricing model. The Brick's comprehensive security capabilities and stealthy operation reduce the network vulnerabilities that absorb IT staff budget and diminish business productivity and corporate image. By providing key next-generation firewall capabilities today, the Brick offers the IT staff a budget-friendly solution and the best investment/performance in the industry.

Lucent VPN Firewall Brick®	Software-based Firewalls	Existing Hardware Firewalls
Simplified licensing model and high-packet processing keep capital costs reasonable	Costly licensing for new features and capabilities keep costs high	High database software fees often charged to add network management capabilities
Full-featured bridging and LSMS shorten time to service	No bridging support	No bridging or limited bridging mode where key features do not operate
Packet capacity and stealthy operation delivered by secure Inferno™ OS	Firewall software runs on top of common OS that needs to be hardened. Added software still has vulnerabilities.	Vulnerabilities persist. Limited stealth leads to more time-intensive operation.
Native heavy-duty virtual firewall support	Low-duty virtual firewall support	Medium-duty virtual firewall support
High-device-count management through LSMS tight integration with Bricks	Device-centric management of firewall limits scalability	Medium device-count-management

Table 2: VPN Firewall comparison

Conclusion

Networking staff face constant pressure to keep their corporate network secure — but are hindered by deploying security systems with inherent flaws and added costs. What's needed are solutions that allow the IT staff to take advantage of next-generation firewall features that support robust security, centralized and intelligent management, topological flexibility and robust packet processing with high availability.

Lucent's VPN Firewall Brick® portfolio of products offers next-generation capabilities to network security planners today. Brick products deliver reliable high performance, ease of deployment, streamlined management control and security features that keep untrusted traffic banned from the corporate network — while optimizing IT staff time and effort.

For information on Lucent's VPN Firewall Brick® models, product specifications and applications, please visit www.lucent.com/security.

To learn more about our comprehensive portfolio, please contact your Lucent Technologies Sales Representative.

Visit our web site at www.lucent.com.

This document is for planning purposes only, and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to these products or services. The publication of information in this document does not imply freedom from patent or other protective rights of Lucent Technologies or others.

VPN Firewall Brick is a registered trademark of Lucent Technologies.
Inferno is a trademark of Vita Nuova.
Linux is a registered trademark of Linus Torvalds.
NEBS is a trademark of Telcordia Laboratories.
UNIX is a registered trademark of The Open Group.
Windows is is a registered trademark of Microsoft Corporation.

Copyright © 2003
Lucent Technologies Inc.
All rights reserved

LVF v1.903

Lucent Technologies
Bell Labs Innovations

