

Security in an 'Always-On' World

April 2000



How the world shares ideas.

Security as a Revenue Opportunity

As small-medium enterprises (SME), small office/home office (SOHO), and mass-market consumers take advantage of broadband access for cost savings and efficiency, they will face the security challenges of an 'always on' connection environment. Broadband service providers need to provide the necessary security to protect their subscribers' corporate and personal assets. To address this mass-market demand for broadband access and security, the service provider has an opportunity to offer security as a value-added service, increasing revenue while meeting the demand for such a critical service. According to a 1999 Ovum report, "...worldwide revenue from next generation services will grow from \$74 million in 2000 to \$40 billion in 2006." According to Ovum, application services alone will comprise \$20 billion of that revenue.

Service providers who take advantage of this opportunity to offer security services can maintain their competitive advantage by offering differentiated services, and develop a *sustainable* core competency in a service that will only grow in demand. Now, with the introduction of Broadband Service Nodes such as the Nortel Networks Shasta 5000 Broadband Service Node (BSN), service providers have the tools to offer broadband security, and in an economically feasible and revenue-generating way. The Shasta 5000 BSN is designed to provide security to the mass-market, enabling the device owner to increase revenue by providing security as a value-added service (Figure 1).

Why Security in an 'Always-On' World

With traditional dialup access, subscribers dial in through their Internet Service Provider (ISP), conduct their business, and log off. This transitory nature of dialup gives hackers a limited window of opportunity to exploit any security holes. Therefore, security incidents with dialup access are limited and have not been widely reported. On the other hand, businesses with dedicated access connections (T-1, frame relay) are protected, but the high cost of these dedicated connections has made them less viable for the small and medium business markets. With broadband Internet access, the landscape changes. Broadband connections are always on and permanently connected to the Internet. Yet today, most DSL and cable subscribers are permanently connected to the Internet without firewalls and are vulnerable. This issue poses a real threat for *all* broadband service providers.

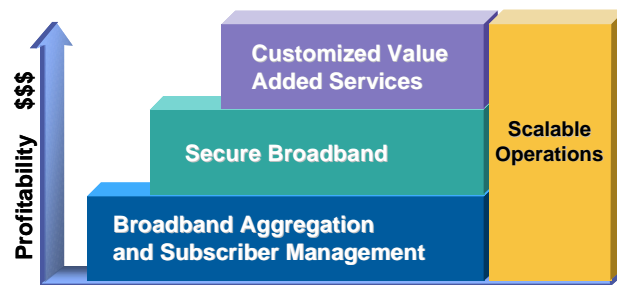


Figure 1 Profitability will increase as service providers scale their networks to go beyond broadband aggregation to provide value-added services.

Security Market in Today's Market

As more businesses and consumers have come to leverage the public Internet to conduct monetary, company-sensitive, and other transactions, the market for security products and services has grown, and will do so even more with the more vulnerable nature of always-on connections. According to a 1999 Yankee Group study, one of the top two Internet concerns of small to medium businesses was security. The growth in public Internet use and the security issues that exist has created a strong demand for firewall products, in particular. According to Frost and Sullivan, the U.S. firewall market alone grew 59 percent in 1999 and is predicted to grow at 38.7 percent annually over the next few years.

For businesses, security can be provided in-house or outsourced, and the customer's decision depends largely on the size of their business. Large enterprises, the Fortune 500, who have the skill set necessary to maintain security for their own company and have stringent security requirements, tend to purchase and maintain their own firewalls and other security products. The small and medium enterprise (SME) and SOHO markets, referred to as the 'Fortune 5,000,000', much like the consumer market, generally do not have the skill set necessary to maintain their own security and are more likely to outsource the security of their networks and connections to either service providers or consulting companies (Figure 2). The latter will either specialize in security or have a strong staff of security specialists. The service provider can capitalize on the demand for such security services, particularly for those customers for whom they already provide access and corporate connectivity. Security consulting is predicted to reach \$14.8 billion by 2003, up from \$6.2 billion in 1999, according to IDC. Businesses are now paying from \$1000 for basic security services up to \$15,000 per month to meet their security needs, noting that in many cases it is still less expensive than hiring and maintaining appropriately-skilled security experts within their staffs. Security software vendors are offering such services to service providers, who often bundle access and hardware charges with their security offerings.

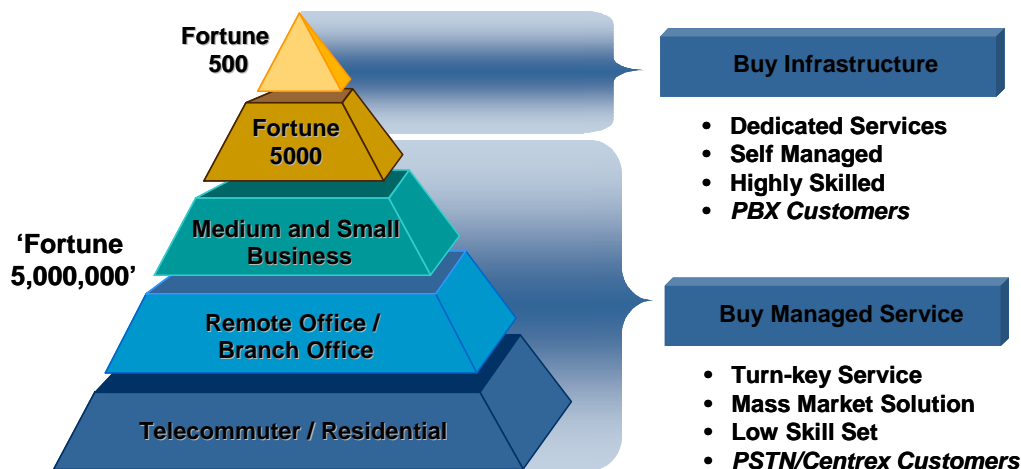


Figure 2 – Different business segments have different network requirements. The Fortune 5,000,000 will turn to their service providers for managed services, including security.

Shasta 5000 BSN: Providing Security at the Network Edge

Sophisticated, yet easy to deploy, the Shasta 5000 BSN sits at the edge of provider networks and can provide the necessary firewall and other security capabilities for all broadband technologies: DSL, cable, and fixed and mobile wireless. The subscriber edge is the mitigation and aggregation point in the service provider's network where the subscriber meets the network. Consequently, it is the only point in the network where the service provider has complete knowledge, control and visibility of the subscriber and their traffic flows for added granularity. Beyond this point, traffic flows from multiple subscribers get aggregated over high-speed connections to backbone or core routers that transport such aggregated traffic over high-speed backbones and lack the visibility into each individual subscriber's traffic flows. Therefore, the only viable point in the network where a service provider can apply any form of control over the subscriber's traffic is at the subscriber edge. The service provider gains economies of scale by spreading capital costs across as many as 32,000 customers per platform. This security is available without the need for customer premise equipment (CPE), saving the service provider precious resources for truck rolls and equipment maintenance costs at individual customer locations.

Shasta 5000 Security Services Overview

The Shasta 5000 BSN integrates an advanced policy-based state aware firewall capability and anti-spoofing security services in its IP Services Operating System (iSOS), together with Remote Authentication Dial-In User Service (RADIUS) authentication support, activity logging, encryption, and support for content filtering. The security services can be provided to subscribers as a complete package or individually on a per-subscriber basis.

Centralized Provisioning

Providing the security to such a large subscriber base does not have to be complicated. Because it is located at the edge of the network, the Shasta 5000 BSN enables the service provider to apply security policies across each and every subscriber through one interface. With its Subscriber Creation System (SCS), the service provider can apply policies through the use of templates and easily customize individual security policies for each customer or groups of customers. The policies can be bulk provisioned and applied to ports, interfaces, or virtual circuits. For example, the wholesaler and/or retail service provider can differentiate, if desired, security offerings among different customer markets such as residential, SOHO, and small-medium businesses, or through differentiated tiering with other value-added services through gold, silver and bronze service offerings.

The Shasta 5000 BSN templates leverage an edge router's knowledge of subscriber address spaces to create generic addressee objects such as subaddressee, peer addressee, and Virtual Private Network (VPN) addressee. It allows abstract objects to be used as template placeholders for required address information for Web, mail and DNS servers. It further allows subscriber-specific definition of object values to resolve the abstract objects in the templates. This allows a customer to quickly provision thousands of subscribers at one time, with similar policies. Individual rules are used to build policies, which are then applied to the individual or groups of subscribers (Figure 3).

The Shasta 5000 BSN captive portal technology enables the service provider to steer customers to a portal for self-provisioning of the services and tiered offerings. Self-provisioning enables faster time to market while still allowing some level of customer control of their security options.
































| # | Source | Destination | Service | Action | Log | Remark |
|---|---|--|--|--|---|--------|
| 1 |  Any |  WebServer |  http  https  ftp |  accept | | |
| 2 |  Any |  MailServer |  smtp |  accept | | |
| 3 |  Any |  DNSServer |  domain-udp |  accept | | |
| 4 |  Any |  Any |  Useful_ICMP |  accept | | |
| 5 |  SubAddr |  Any |  Any |  accept | | |
| 6 |  Any |  Any |  ident |  reject | | |
| 7 |  Any |  Any |  Any |  drop |  brief | |

Figure 3 An example business policy with specific destinations and 'services' (protocols) set to accept, reject, or drop.

Firewalling

Firewalls work as a form of perimeter defense to allow acceptable traffic, as defined by the enterprise or service provider, and drop all other traffic before it enters the network. Firewalls perform this defensive function by monitoring packets and sessions, making decisions based on the established rules in order to determine the appropriate action to take.

There are various firewall products, from large enterprise firewalls to PC-based personal firewall products. Enterprise firewalls sit at the edge of a corporate network or between corporate campuses or divisions and support very specific functions for that enterprise. Such firewalls support a multitude of functions for a single enterprise and as such, have more granular functions pertinent to an enterprise environment. In most cases, to support such granularity, they must employ extra processing power such as the use of a virtual machine in the kernel, and are therefore slower than the Shasta 5000 BSN firewall, and typically cost from \$40 to \$80 per enterprise user.

Personal firewalls are typically software that applies firewall policies to a particular PC, and can be complementary to network-based firewalls. Some come bundled with additional services such as virus scanning for added layers of security. Personal firewalls unfortunately can also complicate the user's experience. In many cases, they necessitate some higher-than-average level of subscriber knowledge to set up and maintain. They can further complicate the service provider's network by increasing the price per subscriber for truckrolls, software updates, or network complexity, particularly if these products are offered from the provider. In a scenario in which the provider does not offer the firewall as part of their service offering, it is highly unlikely that the provider can support trouble calls nor validate whether the source of subscriber problems (such as lack of requested videostreams) is due to network problems or the subscriber firewall configuration. In a scenario in which a service provider does provide personal firewalls, the provider will need to maintain records on individual firewall settings and version numbers deployed, and will be responsible for updating subscribers with the latest versions of the client software. Personal firewalls for individual computers are priced from \$30-60, but can also be offered as free downloads for those interested in these firewalls.

Network-based firewalls, such as that of the Shasta 5000 BSN, sit at the point where the subscriber meets the service provider network and support firewall capabilities across a number of subscribers (Figure 4). Such firewalls are cost effective for the service provider to deploy as they can be priced at a reasonable cost and spread across thousands of subscribers for economies of scale. A typical Shasta firewall costs approximately \$1-\$25 per subscriber site or virtual circuit. For example, for a SOHO environment serving up to 5 individual users, a firewall license will cost \$5 per user. The Shasta 5000 BSN further negates the need for customer premise equipment (CPE) and therefore saves money on truckrolls and IT staffing necessary for maintaining extra equipment, and answering trouble calls for CPE-based problems. Finally, while the Shasta 5000 BSN is complementary to enterprise and personal firewalls, the maintenance of network-based firewalls is easier and less complex than that of its counterparts. It can be completely configured and maintained by the service provider, at their premises, through one single interface.

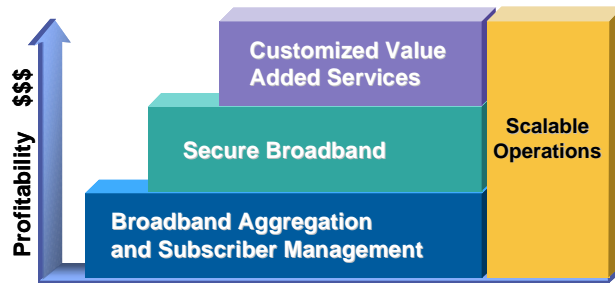


Figure 6 The Shasta 5000 BSN firewall sits at the point where the subscriber meets the service provider network.

Advanced Firewall Capabilities

Firewall technologies have advanced from traditional packet filters to more sophisticated state-aware packet filtering firewalls. Traditional packet filters operate within routers or standalone devices and work by comparing every packet against a set of rules and execute matched rules on those packets. They are generally simple to implement, requiring little logic or memory. They are typically found as a built-in capability to network routers. However, packet filters require an all-or-nothing approach that is problematic in today's business environment and, in some cases, in the residential market.

The rules must filter out certain protocols entirely, for example, and therefore may lessen productivity. On the other hand, to allow common protocols can also open a customer's network to vulnerabilities that certain protocols are known to have. In addition, packet filter rules can become cumbersome and complex to maintain the appropriate number of filters. They can also affect the speed of the network, as they must rerun rules on every packet, having substantial performance impact.

Firewalls can also operate by proxying network traffic to a proxy server prior to hitting the customer network. In this scenario, every connection is terminated at a proxy server, which then initiates a new connection to the intended network, acting as a intermediary. Proxying can be a more expensive solution; requiring full servers dedicated to the firewall function and also requires termination and initiation of layer four sessions. For this reason, proxies can be limited in throughput and scalability. The number of connections per second can be a significant bottleneck. The packets go up and down the operating system stack, and new connections cause multiple system calls and context switches. In addition, only protocols for which proxies are written are supported, limiting the use of proxies for some types of new traffic. Some applications, such as a VPN client, cannot use a proxy by definition, which further complicates the task for service providers who wish to provide a suite of IP services to their customers. Most firewalls today are a hybrid of proxies and packet filters, are available as software or as a combination of hardware and software.

The Shasta 5000 BSN State-Aware Firewall

The Shasta 5000 BSN goes beyond traditional packet filtering and negates the need for application proxies by implementing a full state-aware packet inspection capability. A state-aware firewall is much more advanced than simple access lists available on first generation devices. State-aware firewalls can recognize and track application flows that use not only static TCP and UDP ports like telnet or http but also applications that create and use dynamic ports, such as ftp, audio and video streaming. The Shasta 5000 BSN iSOS software goes a step further and creates a separate firewall process for each subscriber, giving the service provider the flexibility and power to customize security policies for each individual or group of subscribers.

The Shasta 5000 BSN firewall intercepts packets at the network layer and begins analysis on the protocols. It extracts state-related information required from all application layers for the security decision and interprets the IP 'conversation', associating packets to 'conversations'. The software is regularly updated to support the latest popular protocols.

Built from the ground up to provide firewall capabilities as a fundamental part, and not an add-on feature of its platform, the Shasta 5000 BSN is able to firewall with no detriment to overall performance. Through the use of multiple processors and dynamic state tables, the Shasta 5000 BSN maintains all current state information for all subscribers can add additional services and keep near wire-rate performance. This contrasts to traditional routers in which performance diminishes as services are added. The Broadband Remote Access Switches (B-RAS), with their few processors duplicate the architecture of traditional routers and therefore suffer the same problem (Figure 5).

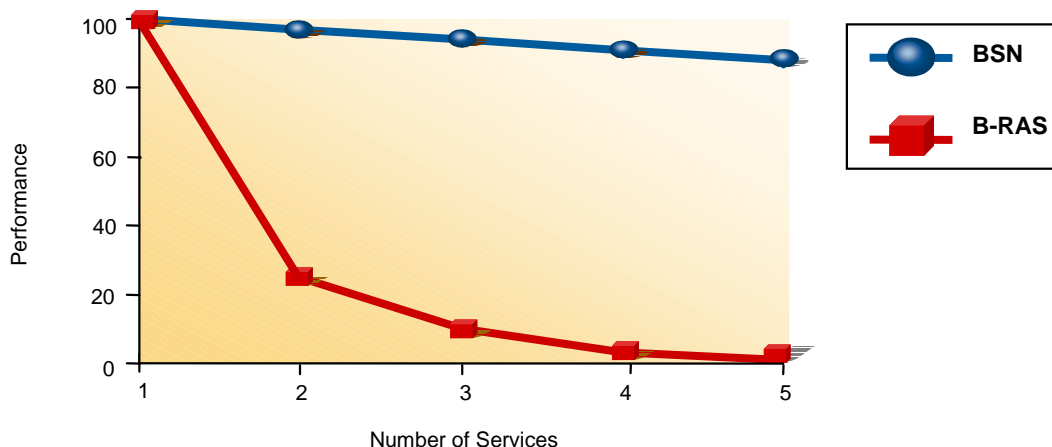


Figure 5 Due to its added processing power and memory, the Shasta 5000 BSN can add additional services and keep near wire-rate performance.

The Shasta 5000 BSN state-aware firewall examines incoming and outgoing packets, which are run against a common security policy, such as that shown in Figure 6.

| Rule Number | Source (Client) | Destination (Server) | Service (Application) | Action |
|-------------|-----------------|----------------------|-----------------------|--------|
| 1 | _SubAddr | Any | Any | Allow |
| 2 | Any | Any | Any | Drop |

Figure 6 A typical security rule for specifying how incoming and outgoing packets, per service type (http, ftp, etc.) are treated.

The following represent two specific examples of how the Shasta 5000 BSN follows conversations through state-aware inspection:

- http (TCP) connection from subscriber to popular Web site:
The first packet of the connection does not belong to any previous "conversation", so it initiates a new one. The conversation (which uses the IP parameters of its initiating packet) matches the first rule, and is allowed. Since it is TCP, packets in the reverse direction (from the Web site port 80 to the originating port number on the originating IP addresses) would be considered part of the same conversation, and when response packets arrive from the Web site, they match an existing conversation that matched rule #1, and are therefore allowed. The same IP response packets would not be allowed if the subscriber did not initiate the original connection.
- File transfer protocol (ftp) (TCP control, additional TCP data):
Similar to above, the initial TCP connection, including initiator and response packets, match the first rule. However, ftp uses the initial connection to negotiate new TCP connections, with potentially random ports numbers, for any data transfer (GET, PUT, DIR, etc.). The Shasta 5000 recognizes the initial control connection as ftp, and parses all the data connection negotiation over it. It then derives the new *expected* TCP connection information from this parsing, and associates all packets in those connections with the same overall "ftp conversation", applying the original rule (#1) to them.

The design of the Shasta 5000 BSN state-aware firewall achieves optimum performance as a result of the following techniques:

- Powerful packet-processing capability in each subscriber service card (SSC), which contains processor arrays that perform the high touch services and policy operation, including the packet filtering and inspection on a per subscriber basis. Each SSC can contain up to 16 subscriber service processors (PowerPC 740), thus a fully loaded Shasta 5000 BSN may contain 112 processors (42,000 MIPS).
- Advanced memory management techniques such as caching and hash tables unify multiple object instances and efficiently access data. Each SSC contains up to 1 GB of memory.
- Optimized packet inspection such that only the first packet of a connection examines the full rule set. Remaining packets in the same connection pass through an accelerated hash match (utilizing the Shasta 5000 state following logic) that does not depend on the number of rules.

The Shasta 5000 BSN can firewall at full line rate on all ports with 64 byte packets. This assumes that the system is configured with the correct number of subscriber service cards (SSC), and that subscriber traffic is somewhat distributed between subscribers. The Shasta 5000 BSN can support one firewall instance for every single subscriber on the chassis. Thus, a single Shasta 5000 BSN can support up to 32,000 firewall instances simultaneously. It is estimated that there are an average of less than 25 rules per firewall instance. The IP Services Business Unit enterprise security experience shows that most businesses will be covered by 6-10 rules. The number of rules on packets per second, bytes per second or latency does not affect the performance of the firewall.

Anti-Spoofing

Spoof attacks involve sending traffic that appears to be a legitimate source IP address and therefore acceptable to the firewall, but the source address has been hijacked and used illegitimately. Even the most advanced firewalls can and have been spoofed by the serious hacker. The Shasta 5000 BSN can prevent spoof attacks from getting through to the subscriber's network as it incorporates advanced anti-spoofing capabilities that can be applied to each individual subscriber. The Shasta 5000 BSN firewall filters traffic going to and from the subscriber, and prohibits the end-user from generating spoofed packets and from forwarding other subscribers' traffic.

Authentication

Service providers use identity verification in order to validate users requesting access to their networks. The authentication mechanisms will take many forms and the identification information will typically reside in a RADIUS or other Authentication, Authorization, and Accounting (AAA) server. Authentication mechanisms include, but are not limited to, username and password, SecureID tokens, and biometric devices such as fingerprint scanners.

The Shasta 5000 BSN supports several forms of authentication, dependent upon the access mechanism and protocol. For PPP end-user authentication, the Shasta 5000 BSN supports both PAP and CHAP password authentication and, for Captive Portal and PPP authentication, also supports the use of Secure ID cards.

The Shasta 5000 BSN provides a single point of integration with existing back-office systems and supports RADIUS with an interface to these systems. In PPPoE, PPPoA, and L2TP, the Shasta BSN acts as a RADIUS proxy (see RFC 2138). In 1483 bridged and routed environments, RADIUS is not used. Instead, users can be authenticated through captive portal, in which sessions are redirected to a captive portal server at the service provider premises. In this captive portal mode, the Shasta 5000 BSN takes a user http connection and directs authentication to a Web page where users then authenticate using userid and password or SecurID card. The captive portal Web server then signals to the Shasta 5000 BSN when authentication succeeds.

For administrator access to the Shasta 5000 BSN, authentication is currently password-based.

For VPN authentication, pre-shared keys are used for Internet Key Exchange (IKE) authentication, as defined in Internet Protocol Security (IPSec), an IETF standard that provides encryption, host authentication, and data integrity for TCP/IP. (For more on the Shasta 5000 VPN capabilities please see the Nortel Networks Shasta 5000 BSN VPN whitepaper.)

Network Address Translation

Network Address Translation (NAT) is a tool used to protect private network IP addresses from the public Internet by translating a publicly available IP address into a private network IP address or addresses. While NAT can be used as a security tool, it is also used to reduce the network costs by reducing the number of public IP addresses necessary for a subscriber network. It also helps expand a network while protecting the current IP-based account scheme for that given network.

As of v2.0, the Shasta 5000 BSN supports a many-to-one translation by allowing up to 254 private IP addresses to be assigned to a publicly visible IP address. The Shasta 5000 BSN Service Creation System (SCS) maintains the assignments and does so for each "real" individual subscriber, rather than for a template subscriber. Therefore each subscriber must be mapped individually. NAT can be configured as shown in Figure 7. The source address, "_privateAddr" is resolved at runtime when the service is applied to a specific subscriber.

| SrcAddr | DstAddr | Service | Action |
|-----------------------|---------|---------|-------------------|
| ----- | | | |
| _privateAddr | Any | Any | Map to publicAddr |
| <any number of rules> | | | |
| Any | Any | Any | None |

Figure 7 SCS action for mapping a public address to an individual private address.

Activity Logging

Activity logging helps track activities within and at the edge of a network to determine if rejected traffic represents a threat or forms a pattern. Such information can later be used to enhance the security features of the network or track illegitimate users.

The Shasta 5000 BSN SCS provides a powerful, and easy-to-use GUI for the creation and definition of the previously mentioned security services. With this service, the SCS provides a log manager that displays every logged event per subscriber and per service. The log information is stored on the Subscriber Service Gateway (SSG) and delivered to the SCS in binary form. All events, including acceptance and reject of packets, can be recorded in a log based on actions specified within the SCS and are time-stamped by the SSG at the time they are generated.

The Shasta 5000 BSN log manager enables the analysis, filtering and searching of the log in a variety of different ways through the customer's use of third party applications, so that information can be extracted quickly and efficiently. All packets that are dropped due to nonconformance of a protocol's 'normal' behavior can be logged in the Log manager for later analysis.

Encryption

To provide the security necessary for VPNs, encryption can be applied between the network endpoints. Such encryption requires compatible algorithms and encryption keys at all end devices for encryption and decryption. The Shasta 5000 BSN currently supports IPSec for secure network connections between Shasta 5000 network devices offering end-to-end tunnels independent of any interior topology or networking technology. The Shasta 5000 BSN employs TripleDES and 56-bit DES through the use of dedicated hardware co-processors for encryption (up to 4 per SSC/line card) for optimum performance, with Internet Key Exchange (IKE)-based keying through pre-shared keys. (For more on the Shasta 5000 BSN VPN capabilities, please see Nortel Networks' [Broadband Service Node: IP-Based Virtual Private Networks](#) whitepaper.)

Content Filtering

Content filtering is a way to control incoming Internet content into any environment---residential and business. Such filtering is done through pre-determined filters used to block URLs meeting certain pre-defined criteria or categories for the particular environment or circumstance. With the advent of pornography, hate crime, and other violent content on the Internet, as well as more benign but inappropriate content to certain environments, such as job seeking in a corporate environment, the demand for content filtering is growing. Corporations are moving to control the availability of job seeking information for their employers during the workday, while parents are actively screening the Web sites their children visit while online. Businesses dedicated to maintaining such URL lists now exist to help service providers cater to their customer's desires for more control over incoming Internet content. Most filtering is then administered through a proxy in which a service provider's customer's Web requests are sent to a proxy which checks requests against a list of 'denied' URLs and blocks any incoming content from those URLs meeting the customer's predetermined criteria.

The Shasta 5000 BSN currently has the ability to support such proxy services through the captive portal's redirection capability to such content filtering server sites, usually within the service provider point of presence (POP). Through the Shasta 5000 BSN policy-forwarding capability, rules can be established to forward the subscriber traffic to content filtering server(s), which then do the filtering on behalf of the customer. Most content filtering servers can handle less than 5,000 concurrent sessions and therefore are not presently appropriate for inclusion within the Shasta 5000 BSN architecture, which handles up to 32,000 users. (See also **Nortel Networks Commitment** for information on content filtering partnership).

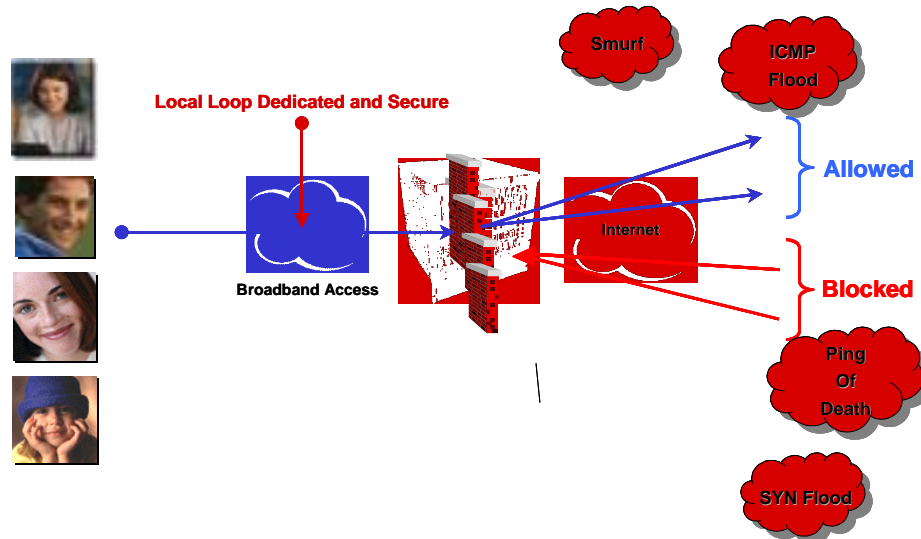
Shasta 5000 BSN and Denial-of-Service

In the fifth annual survey on computer crime and security, the FBI and Computer Security Institute polled 640 corporations, banks and government organizations on the subject. Denial-of-service attacks showed losses up to more than \$8.2 million, prior to the February 2000 attacks on Yahoo!, eBay and others, up from \$77,000 in 1998. More than six high-visibility Web sites were attacked and 150 sites hacked and used as 'slaves' to launch the attacks.

Denial-of-Service and Distributed Denial-of-Service Attacks

Denial-of-service (DoS) attacks prevent a target server or victim device from performing its normal functions through the use of flooding of or irregular sizes of certain types of protocols, such as 'ping' requests aimed at the "victim" server. Normally these attacks are launched from a *single* machine to a specific server to overload the processor or monopolize the bandwidth for that server so that legitimate users cannot use the resource.

Distributed denial of service (DDoS) attacks operate much the same way, however, they are launched from *multiple* machines for the same intentions. Most of the DDoS attacks are done through pre-positioned code on the offending machine, also known as a 'slave', so that the remote or 'master' machine can command the 'slave' to launch the attack at any time.



Tools

Given the far-reaching nature of the Internet, tools to launch such attacks are widely proliferated across the Internet and available to even novice attackers. Many tools posted to hacker Web sites now help hackers automate such attacks; therefore the likelihood for such attacks only increase with time.

In most cases, because many attacks are bandwidth attacks, very few solutions are available to *avoid* such an attack. The attacks continue until all bandwidth or server resources are monopolized and no further traffic is permitted through.

Because the 'slave' is normally used through the pre-positioning of active code, some attacks can be prevented through proactive security policies such as strong authentication and authorization to machines. In addition, to lessen the attack's intended result – to deny server access to others – proactive analysis of logs for servers can help catch the attack early and reset the server for faster turnaround and less downtime.

Shasta 5000 BSN---Enhanced Protection Against DoS and DDoS Attacks

In general, the Shasta 5000 BSN high-bandwidth capabilities make it difficult for such attacks to quickly consume the entire bandwidth. But the Shasta 5000 BSN also includes several features which raise the bar against denial of service attacks (Figure 8). Anti spoofing, in which source and destination addresses are checked and validated for authenticity, i.e. that the address matches the link, is performed in both ingress and egress directions. This helps lower the probability that rogue code from illegitimate network users can be planted on potential 'slave' machines. To prevent 'ping of death' attacks to subscribers, the Shasta 5000 BSN firewall can be set to deny all ICMP 'ping' requests from other than legitimate network servers. In addition, the Shasta 5000 BSN has the capability to verify the length of ICMP packets to ensure correct ICMP packet size and drop malformed packets.

In general, the Shasta 5000 BSN state-aware filtering enables only *solicited* TCP, UDP or ICMP packets onto the network--that is, those that arrive in response to traffic explicitly initiated from within the premises. This helps protect the subscriber base from falling 'prey' to most network-based direct infiltration attack scenarios. For example, to protect against SYN floods, the Shasta 5000 BSN drops all unsolicited SYN requests. For 'land' attacks that force victim machines into an unending loop, the Shasta 5000 BSN prevents such attacks by disallowing any packets with the same source and destination addresses. In release 2.0, the Shasta 5000 BSN has been updated to provide even better resiliency against typical SYN flood attacks.

To protect against vulnerabilities through broadcast, the Shasta 5000 BSN does not forward any IP-directed broadcast packets for directly connected subnet addresses. It forwards directed broadcasts if they are part of subscriber reachability. If a subscriber has reachability, they have CPE within their network, which can be configured to not forward directed broadcast for their internal network.

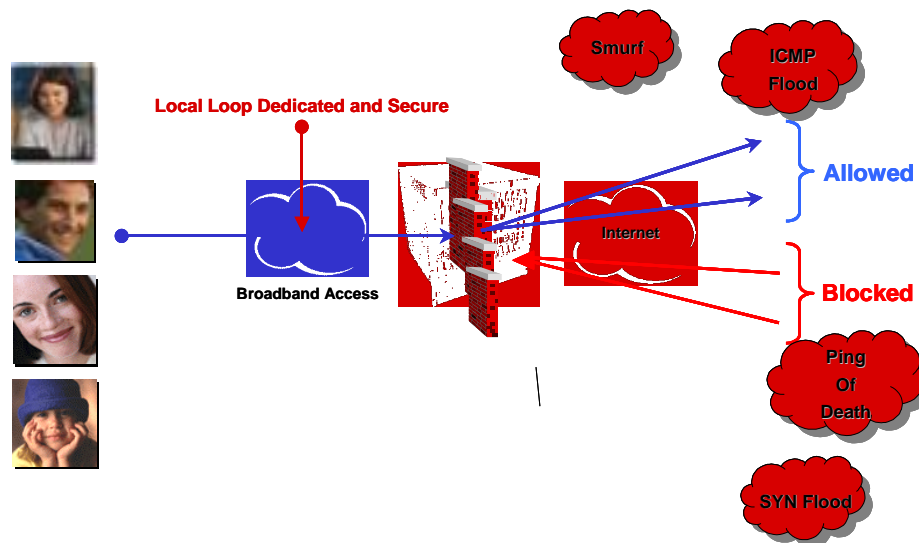


Figure 8 The Shasta 5000 BSN enables the service provider to block threatening content from their network and their subscribers.

Finally, in ftp bounce attacks in which ports are spoofed, the Shasta 5000 BSN is not vulnerable to such attack. The Shasta 5000 BSN avoids this vulnerability by the way it parses ftp control streams.

Proactive Security

There are other proactive approaches the Shasta 5000 BSN enables a network administrator to do to protect the network and its subscribers. If a machine "behind" a Shasta 5000 BSN is generating floods, a network administrator can update the Shasta 5000 BSN policies to disallow traffic from that user or in some cases, disallow the particular type of traffic. For example, network administrators can proactively update the Shasta 5000 BSN policies to filter any 'trigger commands' used in the latest DDoS attack tools, to disallow any incoming traffic of this type while allowing such commands in outbound traffic from legitimate network addresses.

The use of the Shasta 5000 BSN logs to search for and analyze suspect dropped packets can later assist network administrators in at least blocking future traffic from the offenders or may even assist in finding the culprits of such attacks.

Special Security Considerations for Cable Deployments

In cable environments it is also possible to provide a high degree of security. Unlike DSL though where subscribers have their own dedicated line, cable is essentially a shared medium. Therefore other mechanisms are required to provide security all the way to the subscriber. There are three components that make up this secure cable environment.

Firstly, there is a need for Data Over Cable System Interface Specification (DOCSIS) that provides Baseline Privacy using Private/Public Key encryption on the communication channel between the cable modems and the Cable Modem Termination System (CMTS). Secondly, at the CMTS or cable headend filters or access lists need to be applied to prevent broadcast traffic from being seen by other subscribers on the same segment. In other words all traffic needs to be forced to a specific port, which is then the connection to the Shasta 5000 BSN (A more detailed description of the various ways to do this on the different types of headend equipment is being developed). The Shasta 5000 BSN, which is the third component, then supplies the necessary security as described above for each individual subscriber.

The Nortel Networks Commitment

Implementing security goes beyond buying a product. It also involves enforcing policies to proactively defend corporate and personal assets from the growing threats of public Internet use. Having the right product must be coupled with a proactive awareness of the climate to use the product effectively. Nortel Networks goes beyond selling a product to offer tools, such as this and other collateral, and its additional partner programs to offer service providers what they need to effectively provide security.

Nortel Networks is committed to providing customers with the necessary security to meet their evolving business requirements. Through its membership in the ICSA's newly formed Alliance for Internet Security, Nortel Networks and other members hope to raise awareness on the effects of DoS attacks and to make the industry aware of some solutions which can help lessen the probability of such attacks. All members of the Alliance recognize:

- There is currently no way any vendor can entirely defend against DDoS attacks
- Attacks come from thousands of computers fooled into launching the attacks
- We can — and must — make sure our systems are not among those to perpetuate the attacks
- It is a matter of global economic security that we all take responsibility for appropriate actions

The Nortel Networks IP Services business unit has also recently established the Broadband Enabling Ecosystem (BEE) to help address service providers issues in deploying broadband services. Addressing issues such as loop qualification, coordination and installation, Nortel Networks wants to provide a direct link to solution partners for each of these areas. A large part of the BEE program is to provide complimentary security solutions to those of the Shasta 5000 BSN, such as content filtering rating databases and virus and active content scanning. Service providers will have direct Web site links to information on the vendors, their products, and solution news and white papers.

Nortel Networks Raises the Bar on Secure Broadband

The Shasta 5000 BSN—The Industry's First ICSA Certified Network-Based Firewall Solution

Service providers are increasingly required to provide robust protection and firewalling solutions to hundreds of thousands of customers with always-on broadband connections. The Shasta 5000 BSN is the first network-based firewall that satisfies the stringent requirements of the ICSA certification process that allows the mass customization and application of sophisticated security policies to users from the network via a single management system at no additional cost to the ISPs

The ubiquity of DOS/DDOS and hacking tools on the Internet has exposed the vulnerability of current always-on broadband service. Service providers are looking for the security solution that ensure that stringent security policies are in place and are being adhered to *across hundreds of thousands of subscribers*, as they work with the customer to guarantee their security needs are being met and that their network (and indirectly the corporate network they dial into) is not rendered vulnerable.

Stringent ICSA Labs' testing procedures provide the "seal" by which service providers can distinguish "best of breed" firewall implementation from brand-bound claims. ICSA certification is a mark of excellence the Nortel customer's request when evaluating solutions for the networked-based firewall. The ICSA certification is also a proof that IP Service Providers can deliver mission-critical and firewalling and security services from within their public networks: Rapid rollout of best-of-breed secure Internet connectivity at a fraction of the cost, independently of the Internet appliance and access technology used (cable, DSL, fixed and mobile wireless, Frame Relay, ATM etc.), solutions that can meet the superior cost, scaling, reliability, performance, flexibility and robustness requirements network-based solutions demand.

For more details on the Shasta 5000 BSN ICSA certification please refer to the Web site at:

http://www.icsa.net/html/communities/firewalls/vendor_only/nortel/shasta/pfd.pdf

Summary

The Shasta 5000 BSN enables service providers to reach beyond the access services market and capitalize on the new opportunities emerging in IP Services. With the Shasta 5000 BSN, service providers, regardless of their access technology, can gain economies of scale while deploying high-quality security that is less complicated and more affordable than ever, while also gaining significant revenue opportunities through its value-added services features. As one of the few platforms in its market to provide stateful inspection, antispoofing, and powerful hardware encryption and for as many users/platform, the Shasta 5000 BSN offers tremendous value in providing the *necessary* security for today's small and medium enterprises, small office home office (SOHO) and residential environments.

For more information on Nortel Networks Security Solutions please visit the Web site below.

Primetime Broadband—Scaling Secure DSL to the Mass Market

Dave Passmore, Research Director/Founder NetReference, Inc:

http://www.nortelnetworks.com/products/03/broadband/w_scaledsl.html

Broadband Service Node—Secure Cable and Wholesale Access

http://www.nortelnetworks.com/products/03/broadband/cable_layout.pdf

Secure Broadband Access—An eBusiness Requirement

<http://www.nortelnetworks.com/products/03/broadband/SecureBA.pdf>

Secure DSL

http://www.nortelnetworks.com/products/03/broadband/secure_dsl.html

A Framework for IP Based Virtual Private Networks

<http://www.nortelnetworks.com/products/03/broadband/vpn-framework.pdf>

NORTEL NETWORKS™

How the world shares ideas.

In the United States

Nortel Networks
4001 El Chapel Hill-
Nelson Highway
P.O. Box 13010
Research Triangle Park, NC
27709

Nortel Networks IP Services Business Unit

2305 Mission Park Blvd.
Santa Clara, CA 95054
Tel: (408) 565.3708

In Canada

Nortel Networks
8200 Dixie Road, Suite 100
Brampton, Ontario
Canada L6T 5P6
Tel: (905) 863-0000

In Europe

Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead, Berkshire
SL6 3QH U.K

In Asia

Nortel Networks (Asia)
Limited
151 Lorong Chuan
#02-01 New Tech Park
Singapore 556741

In the Caribbean and Latin America

Nortel Networks (CALA) Inc.
1500 Concord Terrace
Sunrise, FL 33323 USA

For more information, please contact your local Nortel Networks representative, or call
1-800-4-NORTEL (1-800-466-7835) or 506-674-5471 from anywhere in North America.

<http://www.nortelnetworks.com/ipservices>



© 2000 Nortel Networks. All Rights Reserved.

*The Nortel Networks logo, the Globemark, How the World Shares Ideas and Unified Networks, Accelar, BayStack, CVX, Contivity, Meridian, OPTera, Optivity, Passport, Preside, Shasta, Shasta 5000 and iSOS Symposium, are trademarks of Nortel Networks. Nortel Networks reserves the right, without notice, to make changes in equipment design or components as progress in engineering or manufacturing methods warrant.

All other product or service names mentioned herein are trademarks of their respective owners or authorized users.

Nortel Networks IP Services is a business unit of Nortel Networks Service Provider and Carrier Group and is headquartered in Santa Clara, California.

#94002.25/04-00