Application-layer security: Enabling the next generation of security services with application switching
Introduction

In today's world of increasingly sophisticated cyber attacks, application-layer security threats are top of mind with many network administrators, security consultants, and CIOs. The loss of network and application access can cost enterprises dearly in lost revenue and employee productivity. Today's security infrastructure must address the new wave of application-layer security attacks and application abuse. The solution is a layered security strategy that protects the network at all points of attack. In this fight, Nortel Networks Application Switches offer administrators an invaluable tool that is uniquely positioned to provide application-layer security by leveraging highly specialized deep-packet inspection capabilities.

The application-layer security need

Attacks on corporate networks are increasing at a dramatic pace. The number of security incidents reported in the first two quarters of 2003 (76,404) is close to equaling the total (82,094) for all of 2002 (CERT). Last year, incidents increased 56 percent over 2001. If incidents continue at their current pace, 2003's total will be an 86 percent increase over 2002.

Network security is at the top of every IT manager's hit list and must be considered in the design of every network, server, and application deployment.

An alarming trend is the use of sophisticated new application-layer attacks. Application-layer attacks are very attractive to a potential attacker because the information they seek ultimately resides within the application itself, whether it be a database application, financial reporting tool, ERP system, CRM system, etc. If disruption is their goal, the service disruption is ultimately evidenced by loss of service to an application. The application layer also provides fertile ground for attacks because it supports many protocols, allowing for greater opportunities for application vulnerabilities and access points. All this variability makes application-layer attacks very hard to defend against.

Traditional firewalls have long been able to enforce security policies based on who or what is allowed to connect to a specific service or machine. However, the content of the packets allowed to pass through a firewall has typically been invisible to the firewall. Firewalls generally look only at header information. The header information is described as Layer 2 (e.g., MAC addresses), Layer 3 (e.g., IP addresses of the sender and the receivers), and Layer 4 (e.g., TCP and UDP port numbers that indicate requested applications). Standard firewalls have limited ability to block attacks based on the content of a packet.

Many new application-layer attacks utilize viruses, worms, malicious code, and buggy applications. A great example of an application-layer vulnerability is the weakness enabled by the standard practice of opening services such as HTTP (TCP port 80) and HTTPS (TCP port 443) through most firewalls. Many applications and protocols, both legitimate and illegitimate, can use these openings to tunnel through firewalls by connecting over standard TCP port 80 (e.g., Code Red virus) or encapsulating in SSL tunnels (HTTPS). Packets aimed at these services pass through the firewall without being identified.

Another level of complication is the use of stateful inspection by traditional firewalls to increase throughput. With stateful inspection the firewall performs inspection on the first packet in a session and compares it to a rule set to make a decision to allow or deny the complete session. The resulting decision is applied to all subsequent packets in the session. By not inspecting all the packets in a session, a firewall can increase its ability to process a larger number of sessions and improve traffic throughput. This poses a significant problem when protecting against application-layer attacks because the data or “payload” of subsequent packets in a session is not inspected for attack signatures. If the first packet in a session is initially inspected and declared “clean,” then a later packet in the same session could pass through the firewall un-inspected and initiate an attack. An example of this problem is Web Services (SOAP, XML) traffic that can contain unique application commands in each packet of a single session. Therefore, Web Services traffic must typically have all packet payloads in a session inspected. Only inspection of all packets at high speed can adequately protect against application-layer attacks without adding latency to the network.

The same application vulnerabilities that enable application-layer attacks are also now being utilized by Peer-to-Peer (P2P) file sharing applications to avoid detection. With over 60 percent of Internet traffic now being originated by P2P, these applications can rob network bandwidth and leave the majority of users with a poor network/application experience (NetworkWorld 7/03). Many enterprises want to limit the use of P2P applications because they can be significant bandwidth hogs and are often associated with the transfer of illegal copyrighted files (music, movies, etc.). While not traditionally considered a security breach, P2P application use can be a significant network abuse problem.

First-generation attempts to manage P2P traffic focused on the ports that the applications communicate over. Standard firewalls are not able to detect these P2P applications because they have evolved dynamic port hopping capabilities. By dynamically changing the ports they use, a P2P protocol cannot be restricted simply by blocking a specific port. Therefore, a unique P2P protocol signature does not appear at the Layer 4 port level, only at the application-layer 7. Many of these protocols have signatures...
that are embedded in the HTTP header and/or the data payload. Kazza, Kazza v2, eDonkey, Morpheous, iMesh, and Gnutella are examples of popular P2P applications that leverage protocols which use dynamic ports to enable client-to-client communication.

Application-layer attacks or abuse, especially the Denial of Service and P2P application subset, are surprisingly easy to initiate. This has lead to an increasing concern regarding attacks that may originate within an organization. The average employee has easy access to the majority of corporate network resources and many have intimate knowledge of corporate application vulnerabilities. A disgruntled employee may want to disrupt the corporate billing system or simply be interested in their co-worker’s salary. Given the growth of internal threats, there is a need for strong security to protect the data center as well as the corporate network perimeter. With strong application-layer security tied closely with application servers, malicious activity directed at corporate applications can be thwarted even if initiated within the security perimeter.

To leverage the Internet to enhance business productivity, enable teleworking, and increase communications with partners, sensitive corporate information must be transferred securely. IT administrators have traditionally implemented IPSec-based Layer 3 security schemes or less secure alternatives. While providing strong security, IPSec does require significant effort to support dedicated clients on each machine authorized to connect remotely to the network. Many times, the complexity of securely managing third-party access devices precludes using IPSec with business partners. IPSec remote access solutions also are unforgiving of the network architecture they run over. Firewalls often interfere with IPSec connections. DSL lines are also notorious for not being IPSec friendly.

In addition to protecting against application-layer attacks initiated from within a corporation, IT departments need to take into consideration that sensitive corporate information, normally housed on application servers with strong protection, is routinely transferred across the corporate LAN free and clear of any security. This leaves sensitive information open for employees to see what they would otherwise not have access to when secured on an application server. IPSec provides full access or no access to the network or network segment it is securing. This lack of access granularity makes IPSec ill-suited for securing communication inside a corporate network. An application-layer VPN technology can support both the need to secure communication originated from inside and outside the corporation.

Protecting applications and application data transfer

What type of payload security inspection is needed?

As application-layer attacks and abuse become more sophisticated, it is imperative that application-layer (Layer 7) deep packet inspection be performed to identify and discard offending packets. Often times, a virus pattern is a combination of multiple patterns within a packet’s payload. Therefore, a security device must be flexible enough to be configured to inspect multiple compound patterns located at different offsets within a payload. When an attack pattern is matched, the security device should treat the packet according to the security policy. This normally will mean the packet is dropped. Alternatively the policy might direct the security device to notify the administrator or set in motion a set of intrusion prevention activities. In the case of application abuse, the security device could enforce rate limiting or shaping that will allow the traffic to pass, but minimizes any abusive effects on the network or applications.

What type of application-layer secure communication is needed?

The most appropriate application-layer VPN technology today is SSL VPN. SSL VPN provides clientless access to a per-application basis that enables the granular security needed to support business productivity by restricting application access to only those with a true need for access. A great example of the power of SSL VPN is its use with channel partners that connect to a corporate network. These channel partners can be granted access to only the documentation and ordering interfaces required for them to effectively work with the corporation. Regular corporate employees that connect to the network using SSL VPN can be given access to all applications except the most sensitive. Access to applications can also be restricted based on the client computer utilized to initiate a connection (e.g., tight restriction from a public kiosk, but full access from a home PC).

SSL VPN extends the reach of enterprise applications to mobile workers, telecommuters, partners, and customers without the need to install and maintain a VPN client on the end user’s computer. SSL VPN is highly portable given that it is embedded in every browser, and browsers are part of almost every computer OS. SSL VPN technologies have matured to the point where they support almost all the applications and features that a user needs to be productive. SSL VPNs provide strong (minimum 128-bit encryption) security, are incredibly forgiving of the network, can survive interrupted network connections (e.g., common on wireless networks), and traverse almost all firewalls seamlessly. With the per-application level of security and simple management, SSL VPN is a great complement to IPSec-based remote access and can solve many of its weaknesses, while also bringing more of the Internet’s productivity gains to the enterprise. SSL VPN is also the perfect solution...
to enable secure communication within the corporation without introducing client administration costs.

**What is the right Application-layer security platform?**

While traditionally security has been the domain of firewalls, they are ill-suited to perform the level of application-layer security required to protect a network. Firewalls, whether server or appliance-based, are typically single processor platforms that are optimized to control access to a network with performance as a secondary concern. To accomplish the task of application-layer security, a device must be able to scan deep into a packet’s payload and identify strings of data that are indicative of a security attack. This type of deep packet inspection is highly processor intensive and would bring most firewalls, and in turn the performance of the networks they protect, to their knees. Switching technology was developed specifically to inspect packets and route them with no network latency. Application switches were specifically designed to switch session traffic based on the content of packets at Layer 4-7. This functionality has been leveraged for a significant amount of time to perform content-intelligent load balancing.

The intelligent application-layer security inspection capabilities of application switches should be utilized to assist standard firewalls. Using application switches in conjunction with standard firewall perimeter security enables a layered security strategy that effectively protects networks against application-layer attacks. With their traditional set of intelligent traffic management features, application processing, and application-layer security in one platform, application switches provide an excellent network consolidation Return on Investment. A typical flow of an application switch performing application-layer security inspection is shown in Figure 1.

Application switches complement standard firewalls by leveraging deep packet inspection to detect P2P protocol patterns and restrict the traffic. Alternatively, the application switch can act as a bandwidth management device that identifies P2P traffic and provides rate limiting and shaping functionality to control the amount of the total traffic generated by these applications. This is especially useful in cable, ISP, and university networks where P2P traffic can reach as much as 70 percent of total network traffic.

Sophisticated application switches can enable application-layer security while being placed in the data center or at the edge of the network. When at the edge of the network, application switches can protect network bandwidth by blocking DoS attacks and abusive applications such as P2P traffic. In a DMZ, they can act as an SSL VPN gateway, while also performing traditional intelligent traffic management tasks for applications in the DMZ such as load balancing servers and network devices. These intelligent traffic management features enhance the reliability, performance, and utilization of the network and applications. Figure 2 shows a typical edge of the network DMZ architecture utilizing an Alteon* Application Switch as an Application-Layer Security Gateway (ALG). The switch in the DMZ is load balancing Web, FTP, DNS, Mail,
Anti-Virus, Citrix, and IDS servers while facilitating SSL VPN secure remote access and also accelerating secure communications (SSL acceleration).

As mentioned previously, an application switch in the DMZ is the perfect place to leverage it as an Application-Layer Security Gateway providing SSL VPN termination. Figure 3 provides a detailed look at how SSL VPNs are enabled using an application switch.

Application switches have long been used in the data center to enhance application performance, security, and availability. In the data center, sophisticated application switches can provide effective application-layer security that not only protects the applications from external attack, but can also be used to protect against internally originated corporate attacks. Securing internal communications with SSL VPN is very effective and efficient protection against “roving” employees. Figure 4 shows a data center architecture utilizing a sophisticated Alteon Application Switch to optimize the network for application performance and functioning as an

**Figure 2. Typical edge of the network architecture utilizing an application switch in the DMZ to perform application-layer security deep packet inspection, SSL VPN termination, SSL acceleration, DMZ server/application load balancing, Firewall load balancing, ISP link load balancing, and bandwidth management.**

**Figure 3. Application switch performing SSL VPN**

1. User establishes SSL session with the SSL VPN portal and enters login information
2. User’s credentials are checked against LDAP/RADIUS/Active Directory authentication database
3. User is presented with a Web portal interface that lists available applications/resources
4. User selects file/application/Link
5. SSL VPN authorizes user and proxies request to application
Application-Layer Security Gateway. The switch is load balancing Web, FTP, CRM, ERP, mail, intranet Web servers, etc. while accelerating SSL and facilitating SSL VPN for internal high-value communications.

What are the characteristics to look for in an application switch that is to be used for application-layer security?

There are several characteristics an application switch needs to enable it to effectively provide application-layer security. The first is performance. Application switches need to be able to process not just Layer 2 and Layer 3 packets at wire-speed. They also need to sustain a similar type of processing performance while handling the more complex task of opening up a packet and inspecting the packet payload. Standard PC architecture-based switches do not have the performance required for demanding tasks such as deep packet inspection—especially when dealing with applications like Web Services that require all packets to be inspected. Application switches with network processor-based inspection engines are designed for high-speed packet processing and are best suited for the demands of application-layer security.

Application switches should support integrated and dedicated application processing. An example of this is dedicated SSL encryption/decryption capabilities paired with SSL. Key handshake overhead processing. This feature significantly increases the capacity and performance of SSL processing, which greatly enhances the user experience. By offloading the core SSL overhead processing from the primary application switch processors, application-layer VPN functionality and application-layer security inspection can function independently. This minimizes the chance that users will experience any degradation of service during an application attack or heavy SSL VPN gateway use. Given the increasing dependence on SSL in general and SSL VPN as a secure communication vehicle, dedicated application processing is a ‘must have’ in a high performance application-layer security installation.

An application switch should have a common set of basic Denial of Service attack signatures available for the administrator to easily leverage in securing their network. The switch should also be flexible enough to allow the administrator to set their own defined pattern matching policies.

Even though traffic can be secured with SSL VPN, there still is a security hole if a client computer is not adequately secured. This generates the need for assessing the security of each client system. Application switches need the ability to determine the identity and trustworthiness of the end user and deny or restrict access privileges accordingly. Should a trusted user log on to the network with unrecognized hardware, perhaps from an Internet café, the network could be configured to give the user access only to e-mail and then give full access privileges when the user returns to the network via a trusted device, such as a business-issued laptop.

Last but not least is the need for application switches to provide a broad set of features that offer layered security to complement the core application-layer security features (e.g., end-to-end SSL encryption, filtering, NAT, etc.). By also offering traditional traffic management features such as application server and device load balancing, application redirection, etc., a sophisticated application switch offers very compelling device consolidation benefits. To ensure these benefits are realized, application switches must be able to run all these features simultaneously without degrading switch performance.
To provide the level of security required without adding latency to the network, application switches need to be very robust, have the power to look deep inside a packet in real time, the intelligence to detect complex patterns and signatures at different locations within a packet payload, dedicated security application capacity, and a broad feature set.

**Alteon Application Switch—Application-Layer Security Gateway**

Nortel Networks Alteon Application Switch, utilizing a next-generation version of the proven Alteon Virtual Matrix Architecture and the award-winning application-rich Alteon OS Traffic Management Software, offers leading application-layer security and application management capabilities. This platform is key to today’s layered security infrastructure and functions as a high performance Application-Layer Security Gateway. Built from the ground up as a specialized high performance Layer 4-7 application switch, Nortel Networks Alteon Application Switch enables the broadest range of high-performance traffic management and control services available. Able to manage the traffic of any IP-based application based on header or payload information, Alteon Application Switches have the power and intelligence required to protect against application-layer attacks and perform application-layer security deep packet inspection on today’s most demanding applications (VoIP, wireless, Web services, database, etc.).

Alteon Application Switches extend Nortel Networks award-winning Alteon switching portfolio, which has been the number one fixed Layer 4-7 switch for five straight years (Dell’Oro, May ’03). Alteon Application Switches are the market’s most powerful Layer 4-7 switch with three to four times the performance of competitor switches, enabling application-layer security deep packet inspection without adding latency to the network (Tolly, Jan ’03). Alteon Application Switches offer:

- Integrated secure sockets layer (SSL) acceleration with end-to-end encryption and dedicated application processing support
- SSL virtual private networking (VPN) and client machine security auditing for clientless remote access to applications—the first integrated SSL VPN Layer 4-7 switch on the market
- Multi-layer security to networks through a host of features that are complementary to application-layer security such as comprehensive intrusion detection system (IDS) load balancing, port mirroring, bandwidth management, application abuse protection, high-speed filtering, NAT, access lists, Peer-to-Peer application management, etc.
- Network investment protection by extending the life of existing server and network infrastructures with features such as local and global application server and network device load balancing, application redirection, bandwidth management, etc., while also providing continued performance headroom for innovative software application and feature development
- High port density in a simplified small form factor, with up to 28 ports in a single rack unit

The Alteon Application Switch Advanced Denial of Service Protection capability includes such powerful application-layer security features as a database of common DoS attacks and UDP/TCP Pattern Matching Guards that enable administrator-defined attack signature blocking, IP range Access Lists, protection against UDP Blasts, and Protocol Rate Limiting are also included. Combining all these features in a single platform enables Alteon Application Switches to provide an industry-leading DoS protection package that protects servers and the network from performance and service-disrupting attacks.

When a client sends a request with a virus string/attack, the Alteon Switch processes the request with application-layer security deep packet inspection, matches to a list of offending patterns, and denies entry to the network. The offending packet is dropped and a reset is sent to the offending client. SYSLOG messages and SNMP traps are subsequently generated to warn the system administrator of a possible attack. The Alteon Application Switch hardware assist mechanism enables blazing identification and classification of virus/attack signatures. Once an initial packet is denied, the denial of subsequent session packets can be accelerated within the architecture. Examples of attacks that the

---

**Network optimization and sophisticated security**

- Application-layer VPN-SSL VPN
- Comprehensive DoS Protection (TCP, IP, ICMP, UDP)
- Intelligent P2P application management
- SSL acceleration (server offload) with end-to-end encryption
- IDS load balancing
- DMZ server and application load balancing and health checking
- Link gateway load balancing
- Global server load balancing/failover
- Bandwidth management/application prioritization
- NAT
- Sophisticated filtering
- SYN attack alarms
- Layer 7 deny filters
- ACL list
- Application abuse protection
Advanced Denial of Service protection package will thwart are LAND, Nullscan, Xmascan, Scan SYNFIN attack, Smurf attack, Fraggle attack, Nullport attack, SYN with SPORT < 1024, JOLT attack, Blat attack, PEPSI attack, Mstream attack, etc.

Alteon SSL VPN is a key component of the application-layer security features of the Alteon Application Switch. With application processors dedicated to the SSL VPN feature and supporting SSL acceleration, the Alteon Application Switch is the perfect high-performance Application-Layer Security Gateway. An Alteon Application Switch can be deployed at the edge of an enterprise network and acts as a secure remote access gateway or secure high value internal communications if placed in the data center. Even if placed at the edge of the network, encrypted application tunneling ensures end-to-end security. Data is secure from the client to the VPN gateway and on to the internal application, not just to the gateway. Authentication, access control, and auditing features provide granular user control and tracking down to the individual application or file level. Global SSL VPN Load Balancing enables the Alteon Application Switch SSL VPN solution to be deployed in a distributed environment to provide multiple redundant access points to the private network. The Alteon SSL VPN uses Application Address Translation to dynamically “externalize” internal applications and rewrite non-secure URLs so that clients are only engaged in secure HTTPS sessions. Utilizing the Alteon “Single System Image” capability enables the Alteon Application Switch SSL VPN solution to massively scale in a plug-n-play fashion by clustering up to 255 Alteon Appliances with the Alteon Application Switch.

The Alteon Application Switch SSL VPN feature integrates seamlessly into any network and uses existing client technology to minimize installation, operational, and support headaches. Scalability is a simple plug-and-play procedure with additional appliances. Accessing secure applications is as simple as reaching a Web site using the familiar Web browser interface. By utilizing existing client software and the Internet for a simple remote access solution, dial-up costs are mitigated, and without the need to install and manage client software, total cost of ownership is reduced. Offloading SSL public key operations to optimized hardware also lowers the cost of supporting the SSL sessions themselves by up to 70 percent.