Whitepaper

Juniper Networks Layered Security Solution

Re-establishing the Trusted Network

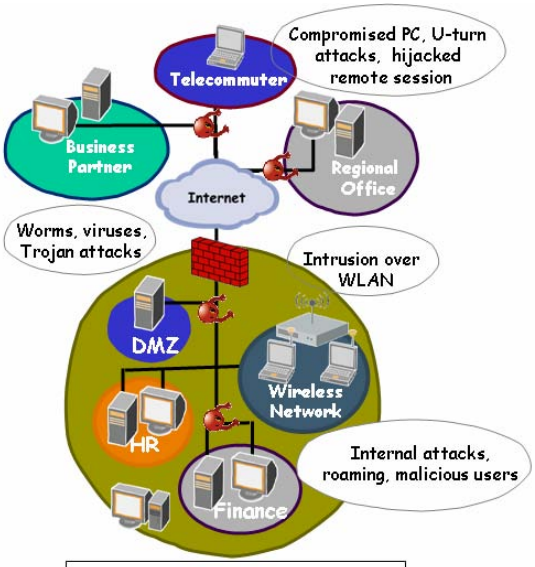
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 200055-003
November 2006

Introduction—The Network Security Challenge

Although basic network security issues have changed very little over the past decade, the network security landscape has changed dramatically. Today's IT professionals still have the primary responsibility of protecting the confidentiality of corporate information, preventing unauthorized access, and defending the network against attacks, they also face new and increasingly tough challenges as they operate in today's complex and dynamic network security environment.

- **Ubiquitous Internet access:** Internet access from a myriad of devices has made every home, office, and business partner a potential entry point for an attack. This ubiquitous access leaves the corporate network open to sophisticated attacks that can be launched by deliberate attackers or unknowingly by remote users logging onto the corporate network and allowing an attack to "piggy-back" on their communications session. The trend of working at home and using a work PC for personal use increases the possibility of dangerous and annoying attacks such as Spyware, Phishing, and SPAM, and needs to be addressed at the corporate network level. A 2005 CSI FBI survey found that 65% of corporations surveyed had been attacked by an external source.



A summary of today's security threats

- **Internal attacks:** While stopping external attacks remain a constant challenge, equally troubling and difficult to defend against are the attacks that are perpetrated from inside the network by employees who have access and ultimately complete control over the network's resources. Internal attacks can range from unauthorized server or resource access to a disgruntled employee destroying or stealing proprietary information.
- **Regulatory compliance:** Sarbanes-Oxley, GLBA, BASEL II, and HIPAA are merely a few of the many different regulations with which corporations are now being asked to comply. In each one, security is either referred to as a key item such as protecting corporate data, or is called out specifically as in the case of encrypting all patient files. Either way, compliance requirements are making life for a security administrator a bit more complicated.
- **Changing levels of trust**: An ever widening range of network access is being granted to employees and non-employees, making the network increasingly vulnerable. Remote employees, business partners, customers, and suppliers may have different levels of access to corporate resources, and appropriate measures must be taken to protect the corporate network at all of these levels. While the applications that remote users have access to through the DMZ increases, companies are simultaneously trying to reduce costs by minimizing the application instances between internal and external users, and this makes it necessary for security policies to accommodate application use by both groups.

The Layered Security Solution

Industry analysts and security experts agree that the key to striking a balance between tight network security and the network access required by employees, business partners, and customers is a layered security solution.

A layered security solution provides an IT department with a complete set of tools that they can deploy to achieve end-to-end security from the remote site to the data center. A layered security solution is designed to protect critical network resources that reside on the network. If one layer fails, the next layer will stop the attack and/or limit the damages that may occur. The table below describes the different security layers and their intended use:

Security Layer	Description
Virtual Private Network (VPN)	Protects communications between sites and/or users with an encrypted, authenticated communications session.
Network Firewall	Protects the network by controlling who and what can access to the network. Stop denial of service (DoS) type attacks.
Intrusion Prevention	Combination of network and application level protection that detects and stops application level attacks.
Antivirus	Protects against virus attacks at the desktop, gateway, and server levels.
Web Filtering	Stop users from visiting inappropriate Web sites or inadvertently downloading Spyware and other malicious applications from known sites.
Anti-Spam	Reduces the amount of junk e-mail being thrown at the corporate networks.

Table 1: Layered security component summary

Different Network Locations Require Different Security Layers

One of the positive attributes that layered security brings is that it allows an IT department to apply the appropriate level of resource protection to the various network entry locations based upon their different security, performance, and management requirements.

For example, remote users will have lower bandwidth requirements and access to fewer technical resources but they still need to protect their PC and the corporate network from attacks, viruses, and from prying eyes. At the other end of the spectrum, protecting the data center/core will require higher levels of performance and access to technical resources in order to support the required levels of security.

This section will discuss the types of attacks that may occur at each of the network locations and the security layers that can be deployed at each location to protect network resources. The discussion will begin with the outlying remote users and remote sites, then work inwards to the network perimeter, ending up at the data center/network core.

Securing Remote Access Communications

Remote access is defined as a user connecting to the corporate network via a public or private connection. The key security goal to strive for with remote access is the protection of content and user identity as it traverses the network. The primary security layer that should be deployed for remote access protection is a VPN for private two-way communications along with strong forms of user authentication and access control. A VPN will help protect the communications from being viewed or hijacked by malicious users. In addition to protecting communications, firewalls with strong forms of access control should be used at the destination point to verify user identity prior to granting VPN access.

Finally, Web filtering and antivirus software can be used to control employee Web site access to protect the company from litigation and the network from inadvertent downloads of viruses, malware, or Trojans.

Security Layer	Deployed for Remote User Access?
Virtual Private Network (VPN)	Yes – Origination point
Network Firewall	No
Intrusion Prevention	No
Antivirus	Yes
Web Filtering	Yes
Anti-Spam	No

Table 2: Remote access layered security component summary

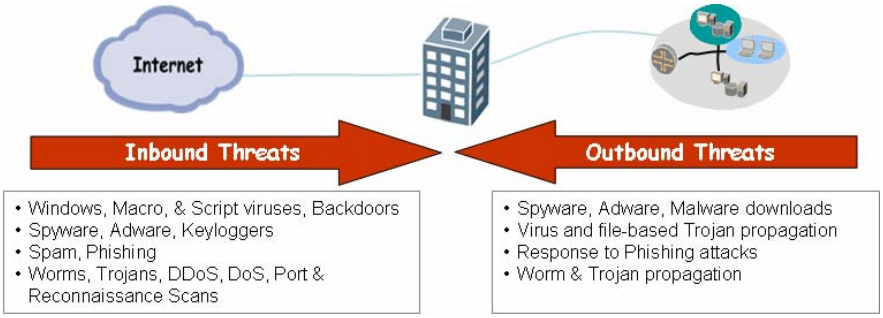
Protecting Site-to-Site Communications

With exploding growth in the number of branch offices being deployed and the increase in partner access to corporate resources, site-to-site communications are becoming key business infrastructure components. Site-to-site communications, both employee and non-employee, can be defined as the interaction between two offices of any type or any size. The site-to-site security layers must account for the fact that they are protecting resources at both sites from external threats such as session hijacking, u-turn attacks, and Trojan or worm attacks that can be launched from a trusted PC that has been compromised. Internal attacks are increasingly common and can include unauthorized server access, improper use of bandwidth, and planting Spyware.

The first security layer to deploy is a firewall with user access control and authentication. This is followed closely by a VPN for secure two-way communications to protect site-to-site communications from attacks and hackers. Firewall access control may be as simple as using a traditional IP address-based process for granting or denying network permissions based on user ID and password. As the user characteristics and attack landscape continues to change, more granular forms of access control that use criteria such as end point state, user identity, and network information are becoming available. Regardless of the access control methodology deployed, one fact is clear. Access control is a critical component of a layered security offering.

With more and more companies providing direct access to the Web at remote sites, end users are casually surfing to sites that may be known malware download sources, or unknowingly revealing personal or corporate private data such as credit cards, passwords or corporate trade secrets via e-mail scams or hidden background programs that collect and forward data. This means that an IT manager must not only stop attacks at the network, application, and content layers, but must also stop both inbound and outbound threats as well.

- Inbound threats are those that originate from outside the corporate network, for example from an attacker on the Internet who intends to penetrate the corporation's perimeter defenses. These threats include virtually all manner of attacks, from worms to viruses to Spyware to Phishing e-mails.
- Outbound threats are those that originate from someone sitting inside the corporate network, such as an employee sitting in their cube who has a machine that has been unknowingly compromised and is propagating a worm or virus throughout the corporate network. Other examples of outbound attacks are users who respond to Phishing attacks by entering their personal data on a malicious Web site, and Spyware sitting on an employee's machine quietly sending sensitive corporate information to some malicious party on the Internet.



Protecting site-to-site communications requires a layered security solution that will stop all manner of inbound and outbound attacks using Firewall and IPSec VPN bolstered by a mix of content security components such as:

- **Integrated Intrusion Prevention (IPS):** Inspect application traffic of all types, fully understand the details of each protocol, and use a combination of methods such as application level stateful inspection, anomaly detection, and other heuristics to stop threats.
- **Web filtering:** Uses a categorized list of URLs that is constantly updated to block access to known malicious Web sites, thereby reducing the number of malicious downloads that are brought into the network.
- **Anti-Spam:** Implement a first line email filter to block known Spam and Phishing sources thereby reducing the flood of unwanted email and the number of incoming attacks.
- **Antivirus:** Use a file-based antivirus (AV) solution that deconstructs the payload, decodes the file or script, evaluates it for potential viruses, and then reconstructs it, sending it on its way.

Security Layer	Deployed for Site-to-Site?
Virtual Private Network (VPN)	Yes – Origination and termination point
Network Firewall	Yes
Intrusion Prevention	Yes
Antivirus	Yes
Web Filtering	Yes
Anti-Spam	Yes

Table 3: Site-to-site layered security component summary

Fortifying the Network Perimeter

The perimeter represents the point at which external traffic gains initial access to the network via VPN termination, as well as the point through which internal traffic will traverse the Internet. With the diversity of traffic that the perimeter represents, the security solution must protect against the widest range of attacks using an assortment of security layers that may include VPN, DoS, Firewall, AV, IPS, and possibly Anti-Spam.

The perimeter security layers must protect against hackers trying to penetrate the network, DoS, and sophisticated viruses and application level attacks that target vulnerabilities that have not been patched. To control the Web sites that employees may visit and thereby protect the company from litigation and the network from inadvertent downloads of viruses, malware, or Trojans, a Web filtering component can be added to the perimeter protection solution. And as the scourge of junk e-mail continues to grow, gateway Anti-Spam should be considered as a first line filter to complement full featured Anti-Spam protection offerings. With several

different security technologies being deployed at the perimeter, it is be important to consider how they will be controlled. A centralized, policy-based management solution will usually provide the ability to unify the perimeter security decisions.

Security Layer	Deployed for Perimeter Security?
Virtual Private Network (VPN)	Yes – Origination and termination point
Network Firewall	Yes
Intrusion Prevention	Yes
Antivirus	Yes – Server or gateway based
Web Filtering	Yes
Anti-Spam	Yes

Table 4: Perimeter layered security component summary

The Last Line of Defense: Protection at the Network Data Center/Core

At the heart of an enterprise is the network data center (or network core) where the applications and data that drive day-to-day business reside. Financial, HR, and manufacturing applications with supporting data represent the company crown jewels and if compromised, can sink even the most stable enterprise. The core network security layers must protect these business critical resources by preventing unauthorized user access, containing internal attacks launched by disgruntled employees, and protecting against application level attacks.

The layers of security that should be deployed at the network data center include firewall(s) to tightly control who and what gets in and out of the network, a VPN to protect internal communications, and a dedicated Intrusion Prevention solution to prevent application level attacks and worms from inflicting damage.

Security Layer	Deployed for Data center/Core Security?
Virtual Private Network (VPN)	Yes
Denial of Service	Yes
Network Firewall	Yes
Intrusion Prevention	Yes
Antivirus	No
Web Filtering	No
Anti-Spam	No

Table 5: Data center/core layered security component summary

Securing the LAN

In conjunction with applying layered security to the network core, it is becoming increasingly common for IT departments to deploy security internally to prevent unauthorized user access to network resources, encrypt/decrypt communications, and contain damage that may occur if an attack succeeds. Users have become far more sophisticated, and controlling their malicious actions, either inadvertent or intentional, has become an increasingly regulated process as companies use layered security as a means to protect themselves from litigation.

Regulations such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), HIPAA, and Basel II are also influencing the deployment of internal security. While these regulations may not necessarily call out specific security technology requirements, they do require that companies make every effort to protect their critical applications, their customer and patient data, and be able to prove how they have done so to auditors. One method to secure the LAN and help address regulatory requirements is to implement a firewall on every LAN segment. There are two ways to achieve this: either implement separate physical firewalls or implement a single physical solution that provides multiple virtual firewalls and high interface density to protect many physical network segments with a single solution. When considering LAN security options, access control offerings that expand beyond the traditional IP address, source, and

destination to incorporate more granular criteria such as end-point state, user identity, and network information (traditional IP address, source, and destination) should be taken into consideration.

Security Layer	Deployed for LAN Security?
Virtual Private Network (VPN)	Yes
Network Firewall	Yes
Intrusion Prevention	Yes
Antivirus	No
Web Filtering	No
Anti-Spam	Yes

Table 6: LAN layered security component summary

Additional Layered Security Considerations

A layered security solution can be an effective means of protecting the network from the sophisticated hackers and the attacks that they can perpetrate. However, a layered security solution can be rendered ineffective if it is unable to handle the traffic thrown at it, or does not provide the reliability features necessary to maintain day-to-day business operations. Additional key considerations that can influence the layered security solution's effectiveness include its ability to:

- Deliver predictable and sustainable performance that scales to Gbps network speeds for firewall and IPSec VPN traffic
- Provide performance headroom to manage traffic spikes that are both business and attack related
- Secure complex applications such as VoIP and streaming media
- Facilitate deployment into complex networking environments without network topology changes
- Operate 24x7x365 through built-in high availability and reliability features
- Simplify deployment and management of layered security components

Components of the Juniper Networks Layered Security Solution

It is a generally accepted fact that intrusions and attacks are inevitable and that a layered security strategy comprised of multiple complementary security technologies, all working together, helps minimize risk by presenting multiple barriers to attackers. This strategy also provides network administrators with more time to react to prevent further damage when an attack has occurred.

Security Layer	Remote Access Security	Site-to-Site Security	Perimeter Security	Core Security	LAN Security
Virtual Private Network (VPN)	Yes	Yes	Yes	Yes	Yes
Network Firewall	No	Yes	Yes	Yes	Yes
Intrusion Prevention	No	Yes—remote site	Yes	Yes	Yes
Antivirus	Yes	Yes	Yes—server based	Yes	No
Web Filtering	Yes	Yes	Yes	No	No
Anti-Spam	No	Yes	Yes	No	Yes

Table 7: Layered security summary

The Juniper Networks line of FW/IPSec VPN products provide IT departments with a complete range of high performance security appliances designed to address the varied deployment locations that customers require. Stateful firewall, integrated IPS, DoS mitigation, and IPSec VPN are standard features on every platform. In addition, the SSG Family of branch office platforms can be deployed with a complete set of integrated Unified Threat Management (UTM) security features. With Juniper Networks security solutions, enterprises can deploy layered security solutions to protect their remote users and sites, their regional offices, and the network perimeter, as well as the network data center/core. The remainder of this document will describe the various components from Juniper Networks that can be deployed in a layered security solution.

Firewall: Access Control and Authentication

Acting as the first layer of security by controlling who and what has access to the network is a firewall. The Juniper Networks firewall uses stateful inspection to protect the network from malicious content. With stateful inspection, data such as source and destination IP addresses, source and destination port numbers, and packet sequence numbers are collected from TCP and UDP pseudo-sessions and then maintained in state tables for future use in analyzing traffic. Juniper Networks stateful inspection firewall protects the network from malicious content by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to and from that network. When necessary, the firewall can perform TCP reassembly to ensure proper interpretation of the communication session.

User Access Control and Authentication

Determining who has access to the network to protect it from outside hackers, attackers, and malicious users is another aspect of access control. In a layered security solution, each network entry point should have a firewall installed to provide user access control and authentication. The integrated firewall/VPN product line can perform user authentication against a variety of different user repositories and technologies that includes:

- Internal database on the firewall
- External repositories including RADIUS, SecurID, LDAP, and Active Directory, with support for redundant servers
- XAUTH support to allow authentication of dial-up users in addition to IPSec authentication
- 802.1X authentication

The Juniper Networks integrated firewall/VPN authentication also includes a Web-based authentication mechanism that allows a user to be authenticated to access any network service via an Internet browser. When deployed at each critical network entry point, firewalls can act as an initial layer of defense, controlling who and what has access to the network.

For more granular access control, Juniper firewall offerings, when deployed as part of the Unified Access Control (UAC) solution, can enforce advanced policies to grant/deny access to resources and applications based upon user identity, endpoint security state, and network information. This overlay deployment can be standalone, with firewalls placed in critical network choke points, or it can be deployed in addition to 802.1X-based Layer 2 admission control which is also enabled by the UAC solution.

Network Segmentation and User Containment

Once thought of as only a perimeter defense security layer, firewall-based access control is being deployed throughout the infrastructure to protect different segments of the network such as finance, HR, and engineering. Used internally, firewalls provide additional layers of access control to protect against the organization's sprawling definition of “authorized user”, as well as to provide containment against worm attacks. By segmenting the internal network with firewalls, enterprises are able to address some of the regulatory requirements brought on by SOX, GLB, HIPPA, and Basel II. With granular logging and reporting capabilities, the IT department can track and report on who has access to network resources, an especially important requirement for regulatory audits. Adding firewalls to the infrastructure enables an organization to protect specific resources, helps to prevent users from unauthorized roaming, and contains damages in the event that an attack occurs.

Rather than implementing a separate, physical firewall for every network segment, the Juniper Networks integrated firewall provides a more cost effective solution— the ability to utilize a single appliance to deploy multiple firewalls in one of two ways. The first uses the physical interfaces, which range in number from 5 to 78 depending on the product, to divide the network into secure segments. For additional segmentation, the entire line of integrated firewall/VPN products have the ability to divide the network into secure virtual segments that, when combined with physical interfaces, can provide additional layers of security at a cost far lower than deploying individual point solutions.

DoS Attack Protection

Juniper Networks integrated security solutions can be configured to protect against more than 30 different internal and external attacks, including SYN flood attacks, UDP flood, and Port Scan. DoS protection should be implemented at each network entry point to protect critical resources. The DoS attack protection that is built in to the Juniper Networks FW/VPN leverages stateful inspection to look for and then allow or deny all connection attempts that require crossing an interface on their way to and from the intended destination. Stateful inspection is only one component in a DoS protection solution. The other components are performance related, including a high session ramp rate and throughput of up to 30Gbps on the highest performing platform.

Intrusion Prevention

With application level attacks becoming more common and more easily propagated, appropriate levels of protection must be implemented at remote sites, at the perimeter and at the network core. Key criteria to take into consideration when deploying application level protection include:

- Will the deployment be a local site with IT support resources or will it be a remote site with few support resources?
- What are the network performance requirements?
- Are the primary protocols that need to be protected internal, external facing, or both?
- Is an integrated or standalone IPS solution the best alternative?

To address these key issues and provide advanced application level attack detection and prevention, the Juniper Networks line of security solutions provides two IPS options: Intrusion Detection and Prevention, and Deep Inspection Firewall.

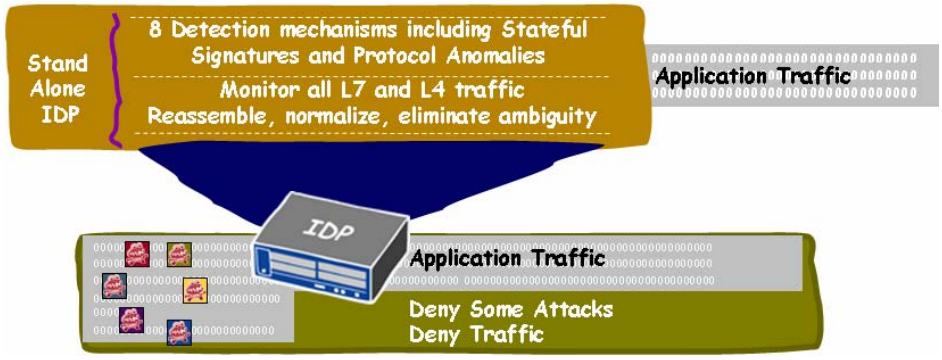
Juniper Networks IDP

In high speed deployment locations, application level attack protection is delivered by Juniper Networks Intrusion Detection and Prevention (IDP), deployed in either a standalone mode or as an integrated FW/VPN/IDP appliance in the form of the ISG Series (ISG 2000 and ISG 1000). Regardless of the deployment form factor, IDP will detect and block attacks across 60+ network protocols using one or more of eight detection mechanisms and powerful signature customization capabilities.

Juniper Networks IDP is the only solution of its kind that integrates true intrusion prevention with application and network profiling to provide administrators with an up to the minute assessment of network activity. Network information collected by Juniper Networks IDP includes items such as IP/MAC addresses (host connected to and from) and port number, while application level information collected includes items such as application used over network, version number, user name, and URL. With Juniper Networks IDP, an administrator has the power to quickly answer questions such as:

- What Windows users have logged in from a specific IP address?
- What IP addresses have specific users logged in from (based on factors like their Windows User id, AIM Nick Name, MSN Nick Name, or IRC Nick Name)?
- What versions of SSH (clients & servers) have operated in the environment?

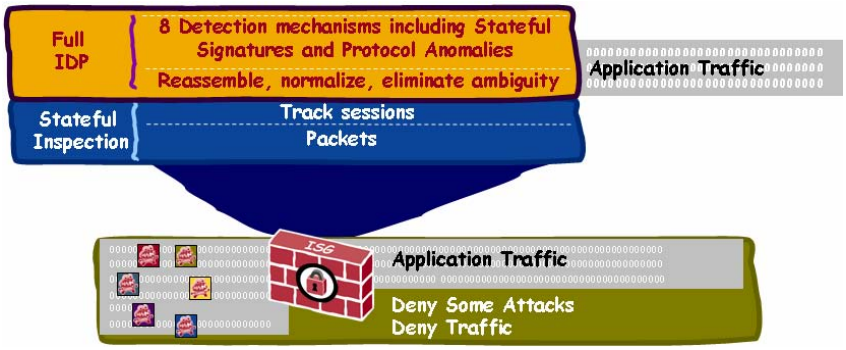
This type of granular detail on current network activity allows security teams to quickly and confidently deploy inline attack prevention and avoid the uncertainty found in the trial and error of today's IDS/IPS solution deployment process.



The combination of application and network profiling and inline attack prevention delivered by Juniper Networks IDP also improves network security's proactive response capability. Any vulnerabilities or issues uncovered by Juniper Networks IDP can be quickly translated into incremental changes to security policies resulting in tighter network security. Or if an attack has somehow gotten through, Juniper Networks IDP can be used as a forensics tool to perform rapid attack investigative analysis using the intuitive GUI to drill down on an attack. Juniper Networks IDP not only helps protect the network against attacks, it provides IT with information on rogue servers and applications that may have been added to the network without their knowledge. Armed with this critical information, IT can proactively protect the network by modifying the security policy. Like all Juniper Networks security solutions, Juniper Networks IDP is controlled using a rules-based management approach to deploying advanced attack protection that will detect attacks and prevent them from impacting the network.

IDP Deployment Options: Integrated or Stand Alone

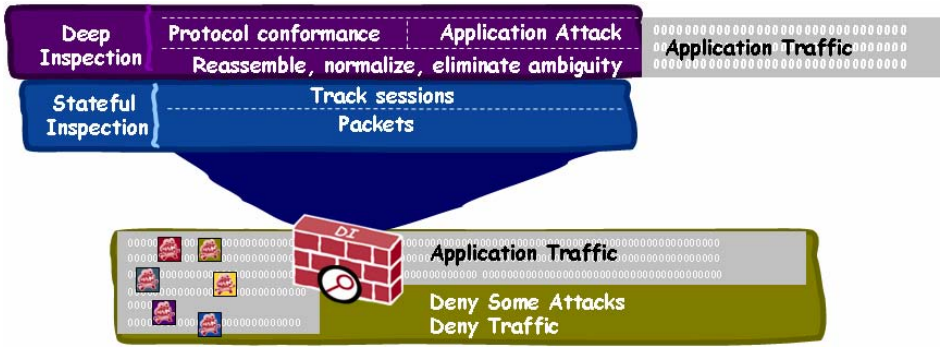
For high speed perimeter and internal network environments where an integrated solution is the ideal approach, the Juniper Networks ISG 2000 and ISG 1000 (ISG Series) can be upgraded to run the same IDP software used in the standalone appliances. Using hardware acceleration provided by up to 3 security modules, each with its own processing and memory, the ISG Series can deliver up to 2Gbps of IDP throughput to protect high speed environments.



For deployment scenarios where standalone IDP is a requirement, the Juniper Networks IDP Family is an ideal solution, available in a range of platforms to fit specific deployment locations including telecommuter, branch office, perimeter and datacenter. Irrespective of the integrated or standalone approach, both the ISG Series and the IDP family can stop worms, Trojans, Spyware, malware, and other emerging attacks from penetrating and proliferating across the network

Deep Inspection Firewall

In branch and perimeter locations, IPS functionality is delivered by Juniper Networks Deep Inspection firewall, which builds on the strengths of stateful inspection and integrates the most deterministic intrusion prevention technologies to determine whether to accept or deny application level traffic and attacks.



Deployed at the perimeter, IPS delivered by Deep Inspection focuses on preventing protocol anomaly attacks by looking for protocol conformance and extracting data from identified application “service fields” where attacks are perpetrated. Stateful signatures are also used to look for specific pattern matches of the vulnerability. A key differentiator is that all Juniper Networks IPS offerings look at the vulnerability as opposed to the specific attack. This increases the scope of attack protection by detecting attack variations and producing fewer false positives. Stateful signatures are also used to expand the scope of attack detection.

When an attack is detected and evaluated against the security policy, an administrator can choose one of eight attack responses, including accept or deny, to stop the attack at the gateway so that it never reaches its destination.

Virtual Private Networks

The next layer of protection utilizes a Virtual Private Network (VPN) to encrypt communications that are traversing an untrusted medium that may include the Internet or an internal network segment. There are two types of VPN solutions to consider: IPSec VPN or SSL VPN. An IPSec VPN assumes that the two endpoints, either a network to network (site-to-site) or machine to network (client-to-site) are connected via a virtual network connection. With an IPSec VPN, users theoretically will have access to all resources on the network. An SSL VPN establishes an encrypted connection from a browser to the desired application or set of applications based on a user's credentials. This method of access allows the user to log into the system but provides control over which applications are available based on the endpoint's trust level (network accessing from, types of security application, level running on the system, and other similar criteria. The key considerations when selecting IPSec or SSL VPN are shown in the table below.

Usage Profile	User Type	Remote Network Security	Connection Type	VPN Type
Remote office, Branch office	Employee	Managed/Trusted	Fixed	IPSec VPN
Mobile employee	Employee/Non-employee	Unmanaged/Untrusted	Mobile	SSL VPN
Partner/Extranet	Employee/Non-employee	Unmanaged/Untrusted	Remote	SSL VPN

Table 8: IPSec vs. SSL VPN considerations

There are two VPN solution categories that Juniper Networks can provide customers.

- **Site-to-Site VPN:** This VPN solution entails a device-to-device communications link with all information between the two devices being protected by an encrypted and authenticated tunnel. With a site-to-site VPN, all users behind each device are provided a secure communications link to the associated destination which is best secured using an IPSec VPN.
- **Remote Access VPN:** This VPN solution is typically deployed to remote users such as the teleworker, business partner, supplier, and other remote user who requires access to network resources. Depending upon the requirement, a remote access VPN can be serviced by IPSec or SSL VPN. Because SSL VPNs do not require the deployment, installation, or configuration of software on a user's machine, they represent an attractive solution for widespread deployment to employees and non-employees alike. SSL VPNS are also particularly effective when the enterprise needs to connect internal resources to business partners or customers where the installation of software on individual machines is impractical.

Juniper Networks can satisfy customers' site-to-site and remote access VPN requirements as a one-stop VPN solution provider.

Site-to-Site VPNs

The entire Juniper Networks integrated firewall/VPN product family is capable of establishing a site-to-site VPN that protects all authorized users with an encrypted and authenticated tunnel. Using policy-based security management that is built into VPN allows an administrator to mix and match different algorithms (3DES, DES, or AES) within a policy to provide the level

of encryption and protection desired.

Juniper Networks integrated firewall/VPN offers customers the first site-to-site IPSec VPN solution capable of providing system level resiliency for a truly fault tolerant solution that meets enterprise level connectivity needs. In many cases, customer network connectivity has improved with the implementation of a Juniper Networks integrated firewall/IPSec VPN solution. Some of the reliability and resiliency features that are built in to the integrated firewall/VPN solution include:

- Physical path redundancy to reduce the reliance on a single transport mechanism or service provider
- Stateful firewall and VPN failover to help lower the possibility of a single point of failure with redundant devices and redundant components in those devices
- Dynamic routing that helps minimize the reliance on manual intervention to establish a new route in the event that the current route fails
- Redundant VPN tunnels and VPN monitoring that reduces the failover time of a VPN connection

With a Juniper Networks integrated firewall/VPN, customers can be confident that their VPN is going to provide the secure, “always on” connectivity required in today’s highly competitive and demanding business world.

Secure Access SSL VPN

Because SSL VPNs do not require the installation of client software, they are an excellent solution for providing access to authorized resources to remote/mobile employees, business partners, and customers. Juniper Networks Secure Access appliances offer a unique and simplified approach to the provisioning and support of secure remote access for these stakeholders. From any Internet-connected Web browser, users can access a wealth of applications that include client server applications, rich Web-based enterprise applications, Java applications, file shares, and terminal hosts.

Using flexible management along with a rich set of remote access and security features, an administrator can establish security policies and levels of remote access that are appropriate for each business purpose. Juniper Networks Secure Access solutions combine three SSL-based access methods within a single appliance to allow an IT department to cost effectively balance two often diametrically opposed goals: maximizing security and at the same time maximizing breadth of access.

- **Clientless Core Access:** Core Access uses the SSL support present in Web browsers, standards-based e-mail clients, PDAs, and other handheld devices to provision access to remote and mobile employees, business partners, and temporary employees. Core Access focuses on extending Web-based resources like partner extranets to individuals whose devices and networks are not managed internally.
- **Secure Access Manager (SAM)**: Secure Application Manager for Java (J-SAM) or Windows (W-SAM) acts as an application proxy for accessing more complex types of client/server applications such as proprietary mail servers like Exchange and Domino, ERP and CRM applications, and some legacy or custom applications as well. J-SAM or W-SAM is an agent-based technology that transparently extends browser-based access to client/server applications in order to provide broad client/server application support for remote and mobile employees, partners, and intranet users.
- **Network Connect (NC)**: For employees and IT personnel who require unfettered resource access as though they were on the LAN, Juniper’s Network Connect (NC) offers a lightweight agent-based network connection that can be provisioned to authenticated

and authorized users “on the fly.” Network Connect extends the broadest form of remote connectivity without requiring desktop software installations because it uses protocols (PPP, SSL) and applications (Internet Explorer, browsers) already resident on most PCs.

Provisioning access with Juniper Networks Secure Access solutions is easy once the business need has been identified. Administrators only need to create user groups that correspond to a business need (partners, contractors, temporary employees, telecommuters, wireless LAN users) and then associate the access method and security controls that apply to each. Most importantly, the Juniper Networks Secure Access appliance supports dynamic provisioning of the connectivity type based on the need. This means that any of the three access methods can be applied to a given user or user group based on where the user is located, the type of network and device being used, and the resources to which access is required.

Antivirus

By integrating a best-in-class gateway antivirus (AV) offering from Kaspersky Lab, Juniper Networks integrated security appliances can protect Web traffic, e-mail and Web mail from file-based viruses, worms, backdoors, Trojans, and malware. Using policy-based management, inbound and outbound traffic can be scanned, protecting the network from attacks that originate from both outside and inside the network. Unlike other integrated antivirus solutions that are packet or network signature-based, the Juniper-Kaspersky solution deconstructs the payload and files of all types, evaluates them for potential viruses, then reconstructs them and sends them on their way.

The Juniper-Kaspersky solution detects and protects against over 500,000 viruses, worms, malicious backdoors, dialers, keyboard loggers, password stealers, Trojans, and other malicious code. Included in this joint solution is a best-in-class detection of Spyware, Adware, and other malware related programs. Unlike some solutions that use multiple network based scanners to detect different types of malware, the Juniper-Kaspersky solution is based on one unified comprehensive best-in-class scanner, database, and update routine to protect against all malicious and malware related programs.

Web Filtering

All Internet content that is read, sent, or received carries inherent risks. Employee access to the Internet continues to introduce new dangers and content that can negatively impact any company in four fundamental ways:

- **Security Threats:** Viruses, spyware, and other malware can all enter a company’s network through Web-based e-mail, file downloads, instant messaging, P2P applications, and other non-work related sites.
- **Legal Threats:** Inappropriate content can lead to gender, minority, or religious harassment and discrimination issues. Illegal downloading and distribution of copyrighted or illegal material over a company’s network present legal liability issues as well.
- **Productivity Threats:** The temptations of non-work related Web destinations are endless. Just 20 minutes of recreational surfing a day can cost a company with 500 employees over $8,000 per week (at $50/hour/employee).
- **Network Threats:** An employee can crash a network just by logging into the wrong Website. Other activities like recreational surfing and downloading MP3 files can degrade network performance and divert valuable bandwidth from critical business needs.

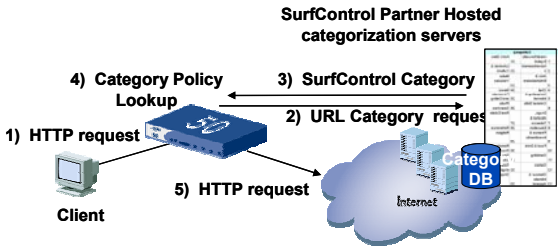
To help prevent against these and other Web borne threats, Juniper Networks provides two

methods of protection via integrated and redirect web filtering.

Integrated Web Filtering

Integrated Web filtering leverages SurfControl's market leading solution, allowing enterprises to build Web access policies on the firewall using the ScreenOS WebGUI or NetScreen-Security Manager to access a SurfControl URL database that includes over 13 million URLs in over 54 categories.

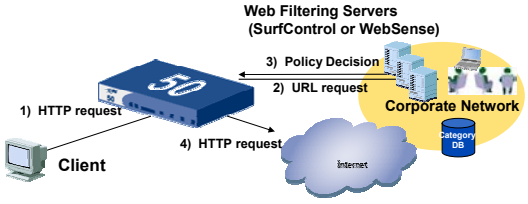
1. Client initiates an HTTP URL request.
2. Firewall intercepts URL request and checks device cache for URL. If URL is not in the cache, it is sent to SurfControl server (hosted by SurfControl partner).
3. SurfControl partner hosted server responds with category for URL, such as "Weapons" or "Sports".
4. Firewall matches category to policy and either allows, denies, or redirects to internal Web page allowing defer/continue option.
5. If allowed, HTTP request granted.



Redirect Web Filtering

Redirect Web filtering funnels Web access requests from the firewall to an external Web filtering server for enforcement of the organization's Web filtering policies. With a redirect solution, the customer installs and manages the Web filtering software from either SurfControl or Websense.

1. Client initiates an HTTP URL request.
2. Firewall intercepts URL request and sends to SurfControl/Websense URL filtering server (hosted at customer premise).
3. Web filtering server responds with policy decision for URL, such as "Weapons" or "Sports" and allows, denies, or redirects to internal Web page.
4. If allowed, HTTP request granted.



Anti-Spam

To help slow the flood of unwanted e-mail and the potential attacks they carry, Juniper Networks has teamed with Symantec Corporation to leverage its market leading Anti-Spam solution for small to medium office platforms. Installed on the Juniper Networks FW/VPN gateway, the Anti-Spam engine acts as a first line of defense, filtering incoming e-mail for known spam and Phishing users. When a known malicious e-mail arrives, it is blocked and/or flagged so that the e-mail server can take the appropriate action.

Additional Layered Security Considerations

A layered security solution cannot be truly effective if it is unable to handle the network throughput it was designed to protect, is difficult to deploy and/or manage, or is unable to sustain 24x7x365 reliability. Juniper Networks layered security solution helps ensure that network resources are protected by providing the ability to:

- Manage throughput at Gbps speed for both firewall and VPN connections
- Handle traffic spikes that are both business and attack related through a combination of overall throughput, processing horsepower, and rapid session ramp rate
- Secure complex applications such as VoIP and streaming media
- Integrate with the current network without requiring significant changes to the network topology
- Facilitate branch office WAN connectivity
- Operate 24x7x365 through built-in high availability and reliability features

Performance

Performance is a critical factor in any security solution. If a security solution is unable to maintain high performance levels at all times, it becomes a hindrance to daily business activity and is more susceptible to attacks. At the heart of every Juniper Networks integrated FW/VPN solution is a high performance platform designed from the ground up to accelerate security processing. With a security specific processing architecture and an optimized datapath to achieve and maintain high throughput levels for both large and small packet sizes, Juniper Networks is able to accelerate firewall, encryption, authentication, and PKI processing and this results in performance that far surpasses competitive security solutions in terms of throughput, rapid ramp rate, and low latency.

Controlling the high performance firewall/VPN platform is ScreenOS, a real time, security specific operating system that controls all aspects of the security device including network integration and security applications. The combination of ScreenOS and the high performance platform means that the Juniper Networks solution does not suffer from connection table and processing limits found in security solutions running on general purpose operating systems. Tightly integrated with ScreenOS is a set of robust security applications that can be deployed as the basis of any layered security solution. The integrated applications include:

- Common Criteria and ICSA certified stateful inspection firewall to control access
- ICSA certified IPSec VPN that facilitates interoperability and secure communications
- Virtual interfaces that allow the network to be divided into secure segments
- High availability to ensure maximum network reliability
- Rich set of management interfaces, both internal and external, to facilitate deployment

Juniper Networks unique blend of purpose-built performance and integrated security applications provides the basis for a robust, layered security solution.

Complex Applications: VoIP

To protect complex applications such as VoIP, a traditional firewall needs to leave a large range of TCP or UDP ports open and this introduces potential vulnerabilities or sources for an attack. The Juniper Networks FW/VPN solutions include H.323 and SIP Application Layer

Gateways (ALGs) that provide much greater protection and flexibility for enterprise-wide deployments.

The VoIP ALGs negotiate layer 3 and 4 information, listening to the control connection and automatically and dynamically opening and closing pinholes through the firewall only for the duration of the call. This provides a higher level of security within the network because the ports only remain open while the call is active. When the call has ended, or unexpectedly disconnected, the ports (pinholes) are shut down. This keeps the rest of the ports in deny state, providing significantly tighter access control protection than a traditional firewall. For even greater access control protection, administrators can set a policy that blocks calls from certain parties or networks, or allows calls only from specific partners at specific times.

When deploying a firewall for VoIP security, an important consideration is where it will be deployed. An ALG listens to the VoIP control message and opens the corresponding VoIP payload RTP ports so it is important to route all VoIP control and payload traffic through the same firewall. In addition to providing VoIP ALGs to protect communications, Juniper Networks FW/VPN solutions help protect the network and VoIP communications in several other important ways:

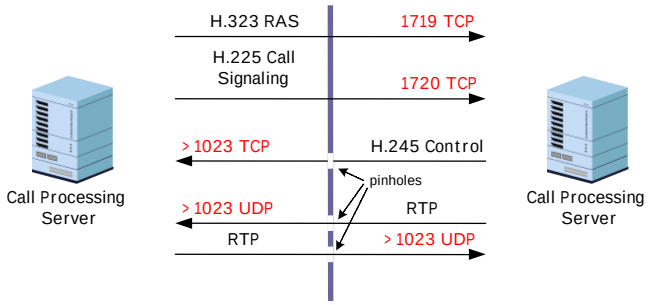


Figure 1: H.323 Application Layer Gateway (ALG)

- **NAT Support for SIP, H.323, MGCP, and SCCP:** Many VoIP applications require the ability to recognize and translate private addresses into public addresses and this enables customers to conceal their network topologies (NAT). NAT represents the ultimate challenge for VoIP protection, that of maintaining the phone call while protecting the IP address, no easy feat for a security solution. The VoIP ALGs in ScreenOS are fully supported when NAT is enabled.
- **SIP Source Flooding Attack Prevention:** This enables customers to set a threshold value for the number of connections initiated by a specific IP within a specified time period.
- **SIP UDP Source Flooding Attack Prevention:** This enables customers to limit the number of SIP requests over UDP.

Network Integration

Network interoperability becomes especially important as the network topology changes or as new offices, business partners, or customers are added to the network. To simplify network integration and help minimize administrative effort when changes to network topology are required, Juniper Networks integrated firewall/VPN solutions support a variety of network deployment modes:

- **Transparent Mode:** This allows a Juniper Networks firewall/VPN appliance to be deployed without any changes to the network, providing firewall, VPN, and DoS mitigation functionality without an IP address and making the device "invisible" to the user. Transparent mode is the simplest way to add security to the network.

- **Route Mode:** Route mode does not require IP address translation when traversing the Juniper Networks firewall/VPN solution, meaning that the IP address assigned is the address of record when a packet reaches its destination. Route mode is commonly used when the security device needs to actively participate in the network using either static routing and/or dynamic routing. Through support for industry standard dynamic routing protocols such as BGP, OSPF, and RIPv2, an administrator can quickly deploy a layered security solution with a minimum amount of manual configuration.
- **NAT Mode:** In NAT mode, an IP address or a group of IP addresses can automatically be translated into a single IP address based upon a predefined security policy. NAT mode provides additional security by hiding IP addresses from public view behind a single IP address.

Juniper Networks firewall/VPN security devices support both static address assignment and dynamic address assignment through DHCP or PPPoE. This allows Juniper Networks firewall/VPN solutions to operate in any network environment.

WAN Connectivity

With the release of the Secure Services Gateway (SSG) Family, Juniper Networks has brought to market the broadest range of firewall platforms that support WAN connectivity options as well as traditional LAN (Ethernet) connectivity. Supporting the wide range of WAN interfaces (T1, E1, DS3, ISDN, Serial, V.92) is a complete set of WAN encapsulations that has been integrated into the ScreenOS routing engine to better support the WAN hardware interface options. The ScreenOS routing engine now supports Frame Relay, Multilink Frame Relay, PPP, Multilink PPP, and HDLC.

The combination of fixed LAN interfaces, I/O expansion slots, and routing protocols that have been integrated into the SSG Family make it the most extensible branch office firewall line on the market. The benefit to the end user is greater flexibility, as the SSG Family can be deployed either as a standalone security device or as a combination security device and router.

Reliability

Many of today's attacks are aimed at bringing down the server or network. As such, high availability is almost entirely dependent on the effectiveness of the security layer. If the security solution goes down, the network becomes vulnerable to attack or, in the worst case scenario, can become completely disabled. In order to help maintain 24x7x365 operation, Juniper Networks has built redundancy features into almost all of its security products. Nearly all of the Juniper Networks solutions have built-in high availability to help minimize the chances of the network becoming vulnerable due to a failure. When deployed in redundant pairs, Juniper Networks security solutions will automatically mirror the configuration, leveraging stateful inspection to create and maintain session tables.

In the event of a failure, a failover algorithm reroutes network traffic to the backup unit that already contains the necessary network configurations, session state, and security associations so that processing can continue—all in less than a second. Each Juniper Networks security product line (FW/VPN, IDP and SSL VPN) has built-in reliability support including several modes of failover, load sharing, clustering, and integration with third party failover solutions.

Management

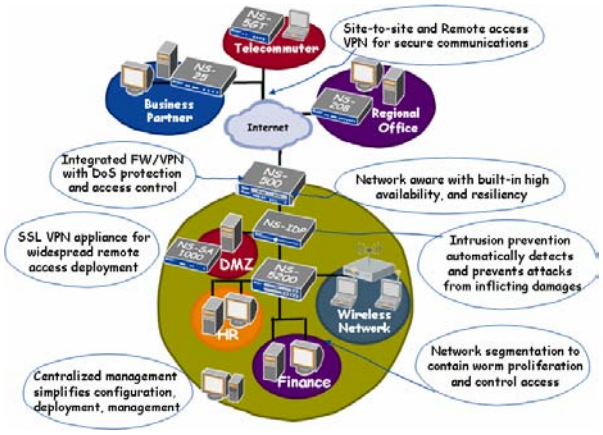
By definition, a layered security solution uses multiple applications that can be deployed across the enterprise, working in parallel to protect the network. The distributed nature of layered security and the desire to control administrative costs mandates that robust

management be an integral component of any layered solution. A key component of Juniper Networks security appliance offering is a policy-based management approach that provides administrators with a centralized security management platform. This platform has been specifically designed to minimize the administrative effort associated with configuring, managing, monitoring, and reporting on security devices and policies.

To protect against the possibility of a layered security management nightmare, Juniper Networks is one of the few vendors that provides a centralized, policy-based management offering that is capable of controlling standalone firewall/VPN appliances, standalone IDP appliances, and integrated firewall and IDP appliances. Using a single user interface that simplifies the management of complex tasks, Juniper's centralized management solution provides a unifying platform that aligns security management with the IT organization's structure, so that all groups can work in concert as they control and administer configuration, network settings, and security policies. It gives users ready access to required information while controlling the administrative tasks they are allowed to execute. And it provides a complete set of investigative tools for in-depth network visibility and closed loop reporting. From a single, centralized console, an administrator can configure, deploy, manage, and maintain a single unified layered security policy across several different appliance families, thereby reducing the chance of configuration errors and lowering overall TCO.

Conclusion

In the network security world, one thing is certain: networks will remain the target of increasingly sophisticated types of attacks originating both internally and externally. Compounding the difficulty associated with protecting the network from new types of attacks is the dramatic expansion of who may or may not have access to the corporate network. These two factors are forcing IT departments to evaluate and implement layered security solutions that are designed to:



- Control who and what has access to the corporate network through robust firewall functionality
- Protect against DoS attacks through built-in intelligence and high performance
- Facilitate secure communications with a VPN so that remote users, business partners, and customers can conduct business across the Internet
- Detect sophisticated application level attacks and quickly react, in a proactive manner, to minimize or eliminate any damages that may result from the attack

With the goal of re-establishing the trusted network, Juniper Networks offers its customers an industry leading layered security solution, one that is highly effective at protecting the network from a never ending wave of intrusions and attacks. With the Juniper Networks layered security solution, enterprises can cost effectively safeguard their applications and data, secure their communications, and protect their "company jewels" from unauthorized access. They can create a network environment that can truly be trusted, and they can do it without sacrificing network performance, flexibility, reliability, or management control.