

Whitepaper

SSG 5 and SSG 20 Feature Overview

Matt Keil
Product Marketing Manager, Security
Products



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

Part Number: 200196-001

EXECUTIVE SUMMARY	3
INTRODUCTION.....	3
THE SSG 5 AND SSG 20.....	3
A PURPOSE-BUILT PLATFORM	4
INTERFACE FLEXIBILITY	4
<i>Wireless Connectivity</i>	<i>5</i>
SOFTWARE ARCHITECTURE: THE FLOW-BASED FORWARDING ADVANTAGE.....	5
INTEGRATED SECURITY FEATURES	6
<i>Security Zones</i>	<i>7</i>
BRIDGE GROUPS.....	7
INTERFACE / TUNNEL REDUNDANCY.....	8
SCREENOS ROUTING ENGINE	8
WIRELESS SECURITY	9
<i>Wireless Authentication</i>	<i>9</i>
<i>Wireless Data Privacy</i>	<i>9</i>
<i>Wireless Security Zones.....</i>	<i>10</i>
SUMMARY	10

Executive Summary

The Secure Services Gateway 5 (SSG 5) and Secure Services Gateway 20 (SSG 20) are two new branch office security and routing platform additions to the SSG family. Complementing the SSG 500 Series, these two solutions bring an unmatched combination of LAN/WAN networking flexibility and Unified Threat Management (UTM) security features to small office, retail site, and fixed telecommuter environments. This paper will describe how key features of the SSG 5 and SSG 20 can help address the security, performance and connectivity requirements found in small branch offices and small, stand alone businesses.

Introduction

While not as large as their regional brethren in terms of number of employees and stature, small branch offices, fixed telecommuter sites and retail outlets have the same security and networking requirements as their larger counterparts:

- Access to corporate network applications to accomplish daily tasks along with direct internet access supported by sufficient bandwidth to maintain user satisfaction
- Appropriate network security to control internal and external user access while blocking all manner of malicious attacks

To address these business requirements while controlling CAPEX and OPEX, IT managers should evaluate solutions that possess a solution system architecture that delivers the right mix of the following criteria:

- Security-first architecture to protect against internal and external attacks across both WAN and LAN connections with advanced best-in-class Unified Threat Management Security (UTM) features.
- Advanced security features such as policy-based security domains and network segmentation
- Performance to protect WAN and LAN traffic even when processing intensive UTM features are enabled

The SSG 5 and SSG 20

The Juniper Networks Secure Services Gateway 5 (SSG 5) and Secure Services Gateway 20 (SSG 20) are purpose-built security appliances that deliver a perfect blend of performance, security and LAN\WAN connectivity for small branch office and small business deployments. Traffic flowing in and out of the branch office can be protected from worms, Spyware, Trojans, and malware by a complete set of Unified Threat Management (UTM) security features including Stateful firewall, IPSec VPN, Intrusion Prevention, Antivirus (includes Anti-Spyware, Anti-Adware, Anti-Phishing), Anti-Spam, and Web Filtering. The SSG 5 and SSG 20 can be deployed in several ways.

- As a stand alone network protection device, leveraging the rich set of UTM security features to stop worms, Spyware, Trojans, malware and other emerging attacks
- As a combination security and routing device to help reduce IT capital and operational expenditures
- As a traditional branch office router, taking full advantage of the proven routing engine

Used by enterprises, service providers and stand alone businesses alike, the SSG 5 and SSG 20 are ideally suited for locations that are smaller, with fewer employees yet still require advanced security and routing features to protect business critical traffic traversing the WAN and high speed internal networks. Typical deployment examples include small businesses, distributed branch offices, retail outlets, and fixed telecommuter environments.

A Purpose-Built Platform

To address the network security processing requirements, the SSG 5 and SSG 20 leverage the successful traits established by the market leading NetScreen-5GT architecture which uses a purpose-built platform assembled from custom-built hardware, powerful processing and a security specific operating system. Juniper Networks is one of the only vendors to utilize custom built boards, conceived and designed in-house, to maximize security processing and throughput that is optimized for high performance networks such as LAN to a next-generation WAN and LAN to LAN. At the heart of the SSG 5 and SSG 20 is a customized, security specific board designed to maximize network security performance through a combination of a powerful processor and 128MB of DRAM, expandable to 256MB. With the increasing emphasis on application level and content security, extra memory becomes a key performance enabling factor by allowing the platform to more effectively manage the dynamic nature of today's attacks.

Interface Flexibility

With support for five 10/100 interfaces plus two I/O expansion slots, the SSG 20 is the first integrated security and routing platform in the small branch office market to support field installable WAN I/O connectivity options.

Customers can, at their convenience, order and install ADSL2/2+, T1, E1, ISDN BRI S/T and V.92 modem cards to complement the existing 10/100 interfaces. This brings a level of I/O flexibility to the small office market that is unmatched by any competitor. Supporting the WAN cards are the appropriate WAN encapsulations including PPP, MLPPP, Frame Relay (FR), MLFR and HDLC. Not to be overshadowed, the SSG 5 is available with three factory configured I/O options to complement the seven fixed 10/100 interfaces. Options include RS-232 Serial/Aux or and ISDN BRI S/T or a V.92 modem.

Integrated Devices: How Much Can You Save?

A recent Branch Office Best Practices study conducted by Nemertes Research interviewed over 200 IT professionals at 78 companies to determine how to cost-effectively manage the network and branch office infrastructure. In terms of devices and device management, the study presented the following statistics.

- The average number of devices in a branch office that need managing = 7
- The average amount of time spent managing branch offices = 34% per IT staff member
- The average burdened salary of an IT staff member = \$98,621
- Branch office device management per IT employee = \$33,531 (35% * \$98,621)

If the number of devices can be reduced by one, simply by implementing an integrated device (FW + DSL Modem, FW + routing, FW + AV gateway, etc), then IT departments can conceivably reduce the management expenditure by approximately 4.9% (assuming 34% / 7 = 4.9%). Translated to cost savings, this means that an IT department can conceivably save \$4034.46 annually PER IT employee (\$98,621 * 4.9%).

When viewed in terms of specific installation costs for integrated vs non-integrated devices, the study presented the following statistics.

- The average amount of time to install a single function device on-site is 4 hours at \$40 per hour
- The average amount of time to install a multi function device on-site is 6 hours at \$40 per hour

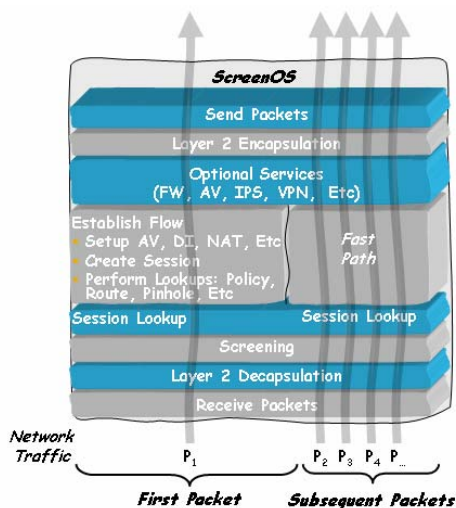
If only one branch office needs to be managed, then saving \$80 by moving to an integrated device may not be worthwhile. However, the interviewees in the study indicated that the average number of branch offices was 514, which translates to a savings of \$41,120, thereby supporting the concept that an integrated device can present very significant cost reductions.

Wireless Connectivity

In addition to the hard wired I/O options available, both the SSG 5 and SSG 20 can be factory configured with dual radios supporting 802.11 a + 802.11 b/g. The first radio transceiver uses the 2.4 GHz radio band, which supports the 802.11b standard at 11 Mbps, the 802.11g standard at 54 Mbps, and 802.11 SuperG standard at 108 Mbps. The second radio transceiver uses the 5 GHz radio band, which supports the 802.11a standard at 54 Mbps. The two radio transceivers can work simultaneously.

Software Architecture: The Flow-Based Forwarding Advantage

ScreenOS, the controlling element for all Juniper FW/VPN platforms, is a real-time, security specific operating system that has been built from the ground up to work in conjunction with the hardware platform to maximize performance. ScreenOS helps accelerate security and traffic making decisions through a process known as Flow-based processing. Flow-based



processing leverages session state to minimize individual packet-by-packet decision making processes and thereby accelerate the overall performance of branch office solutions.

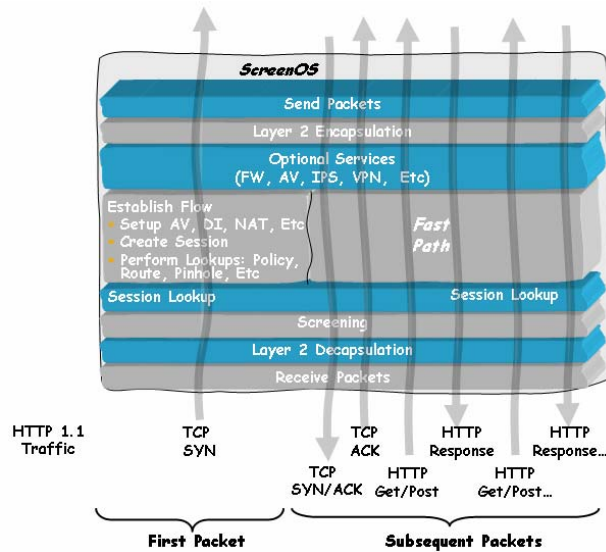
Flow-based processing inspects traffic at a TCP/UDP level using a five tuple match of source and destination zone, source and destination address, and service type to determine and understand if the traffic is a new or existing flow. If the traffic is new, then it goes through a slow path to do route and policy lookups, once this is done, all subsequent packets in the flow are sent through the fast path based upon the action determined by the first packet. As long as future traffic matches the initial flow, the processing continues unabated. If the traffic is new, then the first packet decision making process is followed, as described above. In the figure below, flow-based forwarding establishes traffic flow with first packet while subsequent packets follow the fast path.

Traditional branch devices use 'atomic forwarding' which performs route and policy lookups on every packet. Flow-based processing delivers the following characteristics:

1. Firewall: little or no performance impact for performing firewalling once first packet is processed. Performance is not penalized for having a large rule set – performance for a 50 rule policy is as fast as a single rule policy.
2. Routing: traffic routing is accelerated by minimizing route table looks ups to a single look up per session unless the route changes. If so, then the session table gets updated.
3. QoS Classification: classification is done as part of the five tuple lookup, thereby

- having no impact on throughput performance.
- 4. NAT/PAT: because NAT is session aware, it has zero impact on performance.
- 5. Services assignment: session awareness means AV other types of protection can be applied to specific flows on a granular basis.
- 6. HA: by being flow based, all session info is in a single repository which will facilitate the synchronization of state info quickly when a failover occurs.

A flow-based processing solution is faster at applying security and services – particularly at the branch / regional and remote office locations where traffic patterns are less varied than those at the central site or datacenter.



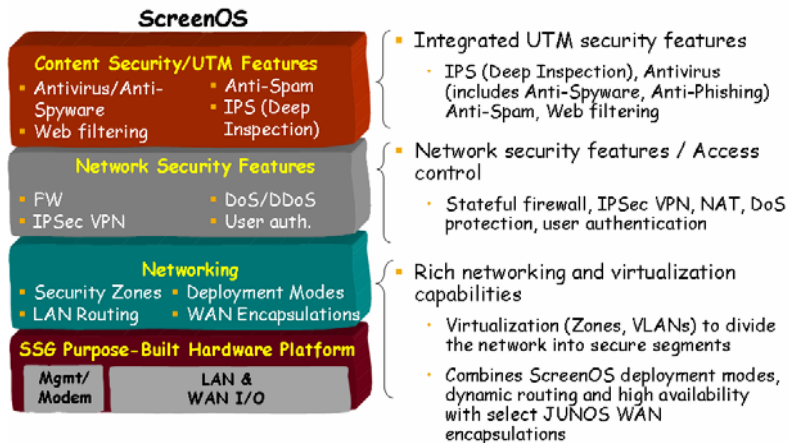
Using HTTP traffic to further illustrate the flow-based advantage, the figure above shows that the first TCP packet establishes the flow while all subsequent packets traverse the fast path, thereby accelerating performance.

Integrated Security Features

Tightly integrated into ScreenOS is a comprehensive set of Unified Threat Management (UTM) security features to protect against network and application level attacks while simultaneously stopping content-based attacks. UTM security features include:

- Stateful inspection firewall to control who and what has access to the network
- IPS (Deep Inspection firewall) to stop application level attacks
- Antivirus (includes Anti-Phishing, Anti-Spyware, Anti-Adware) to stop viruses, Trojans and other malware
- Anti-Spam to block known spammers and phishers
- Web filtering to control access to know malicious download sites or other inappropriate web content
- Site-to-site IPSec VPN to establish secure communications between offices
- Denial of service (DoS) mitigation capabilities
- Application Layer Gateways for H.323, SIP and MGCP to inspect and protect VoIP traffic

The tight integration of operating system and applications with the custom hardware platform helps eliminate performance bottlenecks and known security flaws found in some competitive security and routing solutions.



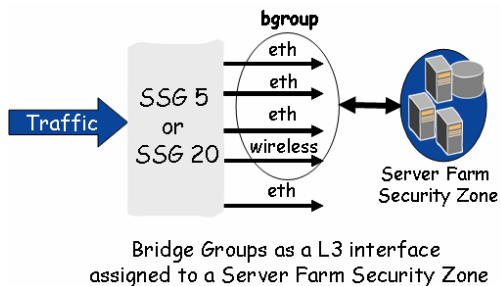
Security Zones

In addition to built-in security applications, ScreenOS provides the ability for administrators to create multiple security zones each with its own firewall and associated policies. A security zone is a logical grouping of interfaces, sub-interfaces and IP hosts and subnets that will share security access controls and settings, thereby delivering additional security control within the network. Organizations can use security zones to more easily address internal LAN security requirements such as protecting network servers from local users and wireless access by classifying them as “Server Farm” such that all of the interfaces and IP hosts and networks assigned to that zone will have a common security stance and access rules. Security Zones, a technology pioneered by Juniper Networks, combined with LAN speed performance will allow customers to easily address their internal and external attack protection requirements.

Bridge Groups

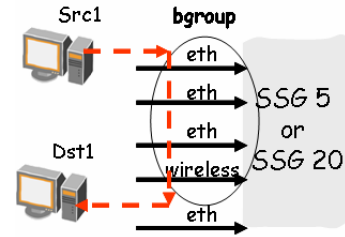
Bridge Groups bring tremendous configuration flexibility to the SSG 5 and SSG 20 by allowing an administrator to select multiple Ethernet and/or wireless interfaces and group them together, effectively creating an abstract or virtual L3 interface and/or L2 switch. A Bridge Group carries the same characteristics as a physical interface in that they can be assigned to a Security Zone where they are subject to the associated security policy. Bridge groups can be used in two ways.

1. Bridge Groups allow an administrator to group multiple physical interfaces as a single “virtual” L3 interface, then assign a security policy to or from that bridge group. The security policy is based upon a zone architecture where traffic to or from a bridge group is enforced.. As traffic traverses the device, the policy is applied and appropriate action taken, regardless of which physical interface is delivering the traffic within a particular bridge group. Traffic within a bridge group will have traffic switch between the ports without having a security policy applied.



Bridge Groups as a L3 interface assigned to a Server Farm Security Zone

- Bridge Groups can also be used as a L2 switch in combination with a wireless interface to simplify network configuration by allowing wireless interfaces and Ethernet interfaces to belong to the same subnet. In this scenario, a branch office would only require allocation of a single subnet minimizing network configuration and management of the device.



Bridge Groups as a virtual L2 Switch

Bridge Groups bring added interface configuration flexibility to the SSG 5 and SSG 20 platforms, allowing the administrator to define how each interface is most effectively used.

Interface / Tunnel Redundancy

In addition to the interface configuration flexibility provided by bridge groups and security zones, the SSG 5 and SSG 20 deliver interface and VPN tunnel redundancy to ensure business communications continue unabated. Combined with the optional HA modes (HA Lite and Active/Passive), the interface and tunnel resiliency brings reliability at every level – device, interface and tunnel - to the SSG 5 and SSG 20.

An administrator can configure any one of the Ethernet or WAN interfaces as a primary or secondary. If an interface problem occurs, the failover can be done manually, by the administrator or it can be configured to happen automatically, as determined by IP monitoring (layer 3 path monitoring) features within ScreenOS. This basically means that when an IP address is unreachable through the primary interface, a failover to the secondary interface occurs.

Commonly used in conjunction with interface redundancy are multiple modes of VPN tunnel redundancy including Active / back up tunnels and dual active tunnels. An active/back up tunnel configuration is exactly what it sounds like – a VPN tunnel acts as a primary while a secondary tunnel acts as a back up. While a dual active tunnel configuration means traffic flows through both tunnels, with ScreenOS performing some very rudimentary load balancing of traffic. When a tunnel failure occurs, all traffic is forced through the active tunnel.

When VPN tunnel redundancy is configured, administrators can use VPN tunnel monitoring to assign weights to each tunnel which in turn will determine when the rapidity with which interface failover occurs. Assigning a weight of 10 (out of 100) to a tunnel means it is considered low priority while a weight of 100 is of higher priority. In addition to acting as a tunnel failover mechanism, VPN monitoring can periodically test the primary interface and then revert back if it is up.

ScreenOS Routing Engine

Since its release in 2001, the Juniper Networks ScreenOS routing engine has quietly established itself as a very powerful and proven branch, remote office routing engine that allows customers to deploy a single platform as a combination firewall and router. The ScreenOS routing features are used extensively by our FW customers around the world. In some cases, it is as simple as a single, outbound BGP route with OSPF enabled to support the internal routing requirements. At the other end of the spectrum is a large financial organization with approximately 10,000 sites that use the public internet to transmit data.

For LAN routing, the SSG 5 and SSG 20 support OSPF, BGP and RIPv1/2 while WAN encapsulation support for the SSG 20 includes Frame Relay, Multilink Frame Relay, PPP,

Multilink PPP and HDLC. The SSG 5 WAN encapsulation support includes PPP only – a limitation based upon the type of connectivity options currently available.

Wireless Security

Protecting the wireless communications is one of the broadest sets of wireless authentication and privacy mechanisms on the market, delivering what can best be described as a true, integrated wireless security solution.

Wireless Authentication

Authentication is critical to wireless LAN deployment since an unsecured wireless access point will expose not only enterprise wireless users, but also the wired infrastructure. An enterprise can be confident that users on the wireless network have been properly authorized to access specified resources by using newer, secured authentication techniques. In addition to the authorization mechanism already supported by ScreenOS such as Radius, RSA, SecureID, LDAP and local database, the SSG 5 and SSG 20 Wireless includes support for the following wireless-specific authentication mechanisms:

- Pre-Shared Key (PSK)
- MAC Address Access Control List
- EAP-PEAP
- EAP-TLS
- EAP-TTLS over 802.1X

Many corporations have already deployed limited WLAN capabilities at their headquarters or large sites. These limited deployments are currently using methods of authentication and privacy that, while older or less secure than the newer algorithms, still need to be supported. By offering a wide range of authentication and privacy options, Juniper Networks ensures enterprise-wide consistency in the WLAN security policies without making obsolete the existing investment in wireless infrastructure.

Wireless Data Privacy

For data privacy, encryption is used to protect messages from unauthorized viewing in case they are intercepted in the air. The SSG 5 Wireless and SSG 20 Wireless both support the following wireless confidentiality mechanisms:

- WEP
- WPA
- WPA2 (AES or TKIP)
- IPSEC VPN

As with the older authentication protocols, some of the older encryption, or more precisely key exchange methods, are vulnerable to attack. Juniper Networks has included these older encryption methods for compatibility with previously installed wireless solutions.

Wireless Security Zones

Like all of the Juniper FW/VPN appliances, the SSG 5 and SSG 20 utilize a zone based architecture that allows the physical interfaces, including the wireless access point, to be used in various configurations to build a security policy that fits the needs of any small office. In short, security zones allow the network administrator to separate users by physical or logical port. When traffic is required to cross a zone boundary, a security policy is enforced. Traffic within a zone may also have a security policy applied. Each zone-to-zone boundary may have a unique policy, meaning that a single firewall can support numerous policies.

Security Zones on the SSG 5 and SSG 20 Wireless enable four Service Set Identifiers (SSIDs) to be simultaneously broadcast from a single device.¹ This powerful feature coupled with the security functions and management capabilities already developed for the existing firewall product line sets the SSG 5 and SSG 20 Wireless apart from every other remote site security appliance vendor's offering.

Each of the SSIDs available in the device is associated with a zone which correlates to a level of trust. SSIDs can be assigned different security levels by selecting mapping them to the various fixed port modes available in the device. For example, one wireless zone may require no authentication and would be associated with the "Wireless1" zone. While a second wireless zone could require the strong authentication of EAP-TTLS over 802.1X, and would be associated with the "Wireless2 or the trust zone". This same concept can be applied to the data privacy method used on a per wireless zone basis too. In fact over 50 different security features can be individually enabled on a per wireless zone basis. These features include Antivirus, Anti-Spam, IPS (Deep Inspection), Denial of Service attack prevention, web filtering and more.

By segmenting wireless users in these zones, a security policy may be built for wirelessly attached users attempting to access resources within the office, while another policy can be used for users attempting to access resources on the Internet. By providing multiple SSIDs, each with varying levels of trust associated with them, complex security policies can be created which enable untrusted wireless users a restricted level of access to resources, while authenticated (thus more trusted) users may access more resources. No other remote site secure access point product provides this level of flexibility and security.

Summary

The SSG 5 and SSG 20 are purpose-built, high performance platforms that deliver a perfectly balanced set of UTM security features, connectivity options supported by powerful routing, to the small branch office and small business market. These two new platforms extend the Secure Services Gateway family and in so doing, continue Juniper Networks tradition of delivering innovative security products that address current and future customer requirements.

¹ In total, the device supports configuration data for up to 16 SSIDs in the local database.