Secure Services Gateway 500 Series System Architecture Overview
Contents

Contents ........................................................................................................................................ 2
Executive Summary ................................................................................................................ 3
Introduction ........................................................................................................................ 3
The Juniper Networks Secure Services Gateway 500 Series .............................................. 4
   A Purpose-Built Platform ................................................................................................. 4
   Software Architecture ................................................................................................. 5
      The Flow-Based Forwarding Advantage .................................................................... 6
      LAN/WAN Extensibility ........................................................................................... 7
      ScreenOS Routing Engine ....................................................................................... 8
Summary ............................................................................................................................ 8
Executive Summary

The need for strong network security is impacting the manner in which network services are deployed to outlying enterprise locations (regional, branch, small remote offices) and medium businesses. This trend is, in turn, driving a new class of security solution that addresses the key security, performance and connectivity requirements of these locations. This paper will describe how the Secure Services Gateway 500 Series architecture can help address the regional branch office security and connectivity requirements.

Introduction

Driven by low cost bandwidth and a desire to improve productivity, enterprises are deploying direct Internet connections at regional and branch offices to replace or augment branch-to-corporate backhaul connections. Direct internet access greatly improves performance and connectivity at the remote office while decreasing overall bandwidth and equipment costs at the head-end. With increased access comes increased risk of attack - end users who are now able to freely check their web mail accounts and venture to points on the web that were previously inaccessible, increase the risk of a virus, worm or Spyware infecting the corporate network via the branch office.

At the same time, frequent internal attacks and unauthorized access are forcing companies to reconsider the traditional LAN deployment methodology that allowed anyone or any traffic to have access to any location on the network. According to the CSI/FBI Survey, at least 56% of companies had at least one internal attack. Today, network security is as much about stopping internal attacks originating from malicious employees and hackers gaining unauthorized access to the inside of the network via Spyware, and innumerable other methodologies as it is about protecting from external attacks.

A third trend indicates that as companies further embrace the use of the Internet as a key WAN infrastructure component, they are looking at faster technologies such as Metro Ethernet to deliver the added bandwidth needed for new applications. Growth statistics support the migration towards Metro Ethernet with 10/100 Mbps and 1 Gbps interface growth rates of 52% and 74% respectively (Infonetics, Metro Ethernet Market Share, Oct, 2005).

The business trends at regional/branch offices and medium businesses indicate that the ideal solution system architecture be one that delivers optimal security, performance and connectivity capabilities. The ideal solution architecture will be one that delivers the right mix of the following criteria:

- Security-first architecture with advanced features such as network, application and content security as well as policy-based security domains/network segmentation
- Ability to protect against internal and external attacks at both WAN and LAN speeds with a combination of network level security along with processing intensive application and payload-based (content) security
- Capable of making security and traffic routing decisions in fractions of a second and do so when 100s of Mbps or more of network traffic is being thrown at it.
- Modular I/O architecture to deliver a migration path for future security and connectivity options.
The Juniper Networks Secure Services Gateway 500 Series

The Juniper Networks Secure Services Gateway 500 Series (SSG) represents a new class of purpose-built appliance that is architected from the ground up to deliver a high performance security and LAN/WAN routing platform. The SSG 500 Series can be deployed in several ways.

- As a standalone network and application level security solution to stop worms, Spyware, Trojans, malware and other emerging attacks.
- As a consolidated security and routing solution, taking full advantage of WAN hardware and software connectivity options.

The purpose-built nature of the SSG 500 Series delivers the security, performance and WAN connectivity to make it an ideal solution for regional/branch offices, medium businesses and service providers that want to protect their WAN and high speed internal networks while extending the platform return on investment through high levels of system and interface modularity.

A Purpose-Built Platform

One of the key tenets of the Juniper Networks FW/VPN platforms has been the ability to deliver high performance security through a purpose-built security platform. A purpose-built platform delivers its performance by leveraging the combination of the appropriate processing tightly integrated into a security specific platform controlled by a security specific operating system. Like all the previous Juniper Networks FW/VPN appliances, the SSG delivers its impressive performance through the combination of custom-built hardware, powerful processing and a security specific operating system. The SSG 550/SSG 550M delivers a minimum of 1 Gbps of IMIX traffic while the SSG 520/SSG 520M can process a minimum of 600 Mbps. IMIX traffic was chosen for firewall performance measurement for the SSG 500 Series as it is more representative of real-world customer network traffic and as such is as much as five times more demanding than a single packet size performance test. The IMIX traffic used is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic.

The SSG 500 Series hardware architecture leverages the successful traits established by the market leading NetScreen-5GT architecture that uses a combination of a powerful general purpose processor and a security co-processor. The heart of the SSG 500 Series is a customized, security specific board designed to maximize network security performance through a combination of a powerful processor, a security co-processor and up to 1 GB of RAM. 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.
Juniper Networks is one of the only vendors to utilize custom built boards, conceived and designed in-house, to maximize security processing and throughput. Whereas off-the-shelf, PC-like boards with performance limiting buses are used in some other offerings, the SSG accelerates security and traffic routing decisions by using multiple high speed buses, each dedicated to a set of interfaces or an interface card to quickly and efficiently funnel traffic to the CPU where security and traffic routing decisions are made. The SSG board design delivers processing power that is optimized for high performance networks such as LAN to a next-generation WAN and LAN to LAN.

Software Architecture

Juniper Networks ScreenOS 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. 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 perform access control and stop network level attacks
- IPS (Deep Inspection firewall) to stop application level attacks
- Best-in-class antivirus based on the Kaspersky Lab scanning engine that includes Anti-Phishing, Anti-Spyware, Anti-Adware protection to stop viruses, Trojans and other malware before they damage the network
- Anti-Spam via a partnership with Symantec to block known spammers and phishers
- Web filtering using SurfControl to block access to known 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, SCCP and MGCP to inspect and protect VoIP traffic

The tight integration of ScreenOS with the hardware platform helps eliminate performance bottlenecks and known security flaws found in some traditional solutions.

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 product development and engineering documentation by classifying them as an “Engineering Zone”, 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 the internal and external attack protection requirements required in today’s enterprise environments.

The Flow-Based Forwarding Advantage

Working in conjunction with the hardware platform, 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 lookups 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.

**LAN/WAN Extensibility**

Taking a modular approach to connectivity, the SSG 500 Series brings unmatched LAN/WAN extensibility with four fixed 10/100/1000 Ethernet interfaces plus six interface expansion slots that can support traditional LAN or WAN interface cards.
The combination of fixed LAN interfaces, I/O expansion slots and routing protocols that have been integrated into the SSG 500 Series make it one of the most extensible firewalls on the market. The benefit to the end-user is greater flexibility as the SSG 500 Series can be deployed either as a standalone security device or as a combination security device and router.

**ScreenOS Routing Engine**

Since its release approximately five years ago, 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.

With the release of the SSG 500 Series, several new WAN encapsulations were added to 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 in addition to the long supported OSPF, BGP, and RIP v1/2. The SSG 500 Series can claim the unique distinction of supporting the widest range of routing protocols of any firewall on the market.

**Summary**

The SSG 500 Series continues Juniper Networks long, distinguished track record of delivering purpose-built high performance security solutions that meet current and future customer needs. The SSG 500 Series is built from the ground up to perform regional/branch office security and routing using the optimal combination of a large, high performance processor, assisted via a security co-processor controlled by a flow-based, security specific operating system. The combination of performance elements helps optimize security traffic processing, making the SSG 500 series an ideal offering for regional/branch office and medium business deployments.