

White Paper

# Branch Office Reference Architecture

---

Employing the Juniper Enterprise Framework for  
Branch Office Solutions



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408.745.2000  
1.888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

## Table of Contents

Executive Summary . . . . .	4
Introduction . . . . .	4
Target Audience . . . . .	4
An Open Systems Approach. . . . .	5
Applying Juniper’s Enterprise Framework at the Branch Office. . . . .	5
The Juniper Networks Branch Office Reference Architecture. . . . .	6
Branch Office Profiles. . . . .	6
Connectivity . . . . .	7
Security . . . . .	7
Performance . . . . .	7
Branch Office Devices. . . . .	9
General Design Considerations. . . . .	10
Infrastructure . . . . .	10
LAN . . . . .	10
Wireless LAN (WLAN) . . . . .	11
WAN Connectivity . . . . .	11
VPN . . . . .	11
QoS . . . . .	12
High Availability (HA). . . . .	12
Services . . . . .	13
Firewall . . . . .	13
DoS Attacks . . . . .	14
Unified Threat Management (UTM) . . . . .	14
WAN Optimization and Application Acceleration . . . . .	14
Applications . . . . .	15
Business Applications . . . . .	15
Real-Time Applications: VoIP, Video and Unified Communications . . . . .	15
Policy and Management . . . . .	15
Unified Access Control . . . . .	16
Backup and Restore. . . . .	16
Centralized Management . . . . .	16
Branch Office Type A - Basic Profile . . . . .	18
Connectivity . . . . .	19
LAN . . . . .	19
WLAN . . . . .	19
WAN . . . . .	19
Security . . . . .	19
Firewall . . . . .	19
UTM . . . . .	19
Branch Office Type B – Optimized Profile . . . . .	20
Connectivity . . . . .	21
LAN . . . . .	21
WLAN . . . . .	21
WAN . . . . .	21
Security . . . . .	22

Firewall . . . . .	22
UTM . . . . .	22
Unified Access Control . . . . .	22
High Availability . . . . .	23
Branch Office Type C - Critical Profile . . . . .	23
Connectivity . . . . .	24
LAN . . . . .	24
Wireless LAN . . . . .	24
WAN . . . . .	24
MPLS . . . . .	25
Security . . . . .	25
Firewall . . . . .	25
UTM . . . . .	25
Unified Access Control . . . . .	25
High Availability . . . . .	25
VoIP and Unified Communications . . . . .	26
Optimizing Application Performance . . . . .	26
Conclusion . . . . .	27
About Juniper Networks . . . . .	27
Appendix 1 . . . . .	28
Product Tables . . . . .	28
Partner Products . . . . .	28
Symantec . . . . .	28
Kaspersky . . . . .	28
SurfControl and Websense . . . . .	29
Avaya IG550 . . . . .	29
Glossary . . . . .	31

## List of Figures

Figure 1: The Juniper Networks Enterprise Framework . . . . .	5
Figure 2: Branch Office Architecture . . . . .	6
Figure 3: High Availability at the Branch Office . . . . .	12
Figure 4: Branch Office Type A - Basic Profile . . . . .	18
Figure 5: Branch Office Type B - Optimized Profile . . . . .	20
Figure 6: Unified Access Control for Branch Offices . . . . .	22
Figure 7: Branch Office Type C – Critical Profile . . . . .	23
Figure 8: WAN Acceleration Configuration with WX/WXC Integrated Service Modules in Edge Devices . . . . .	26

## List of Tables

Table 1: Branch Office Features and Capabilities . . . . .	8
Table 2: Product Recommendations Based on Branch Office Profiles . . . . .	10
Table 3: JUNOS Operating Efficiencies (Lake Partners 2007) . . . . .	17

## Executive Summary

According to a 2006 report from Nemertes Research, approximately 89 percent of employees work outside company headquarters and require immediate access to—and consistent response times from—centralized business applications and resources to do their jobs. However, existing branch office infrastructure solutions do not currently meet the new requirements for performance, security and connectivity. Also, they do not provide the centralized management capabilities needed to reduce costs, streamline operations, and ensure the fast and consistent response times for distributed users accessing centralized applications and resources that are critical to business productivity.

The increased adoption of IP telephony and video applications, as well as the deployment of new applications and the webification of existing applications, is driving bandwidth demand ever higher. According to Forrester Research (2006), 46 percent of all firms in North America have installed IP telephony systems and 39 percent use voice over IP (VoIP) to communicate with their remote offices.

Security is also a pressing concern. FBI/CSI statistics show that 72 percent of all companies surveyed reported at least one security incident in 2006. Not surprisingly, a 2006 Forrester Research survey found that 57 percent of all firms consider “upgrading security environment” a top priority. Forrester Research (2006) also reports that 51 percent of the firms surveyed consider server centralization and data center consolidation a key priority. According to Business Technographics, stringent regulatory requirements made data management and archiving another top priority for 2006. And companies in every industry are demanding consolidated, centralized management solutions that help reduce the time and resources devoted to keeping branch offices online and operational.

## Introduction

Any interruption of network operations impairs productivity in the branch, which in turn negatively impacts the business. To avoid such disruptions, enterprises need a branch office solution that ensures fast and consistent response times for centralized business applications and resources, while streamlining operations and the rollout of new applications and technologies through centralized management and consolidation. Juniper Networks delivers a proven IP infrastructure for the branch office that enables the performance, flexibility, security and intelligence needed to increase branch office user productivity.

This Branch Office Reference Architecture provides the key architectural considerations and details required to incorporate branch office designs into your enterprise.

## Target Audience

- IT managers
- Systems engineers
- Network analysts and engineers
- Network administrators
- Security managers
- Others with like responsibilities

## An Open Systems Approach

Using an open systems approach that leverages the Open Systems Interconnection (OSI) stack model and standards-based interfaces ensures the architecture is flexible, scalable, and extensible. It is critical, that a branch office design ensure support for open-standards and protocols such as RIP, BGP, and MPLS that enables network designers to leverage the innovations that are happening in the industry. Implementing proprietary protocols over the network must be considered carefully, as this can lead to vendor lock-in which ends up dictating what applications and services enterprises can deploy over the long run.

Juniper Networks simplifies the OSI model into three functional layers controlled by a Policy and Management domain (figure 1). These layers are the Infrastructure Layer, the Services Layer, and the Applications Layer.

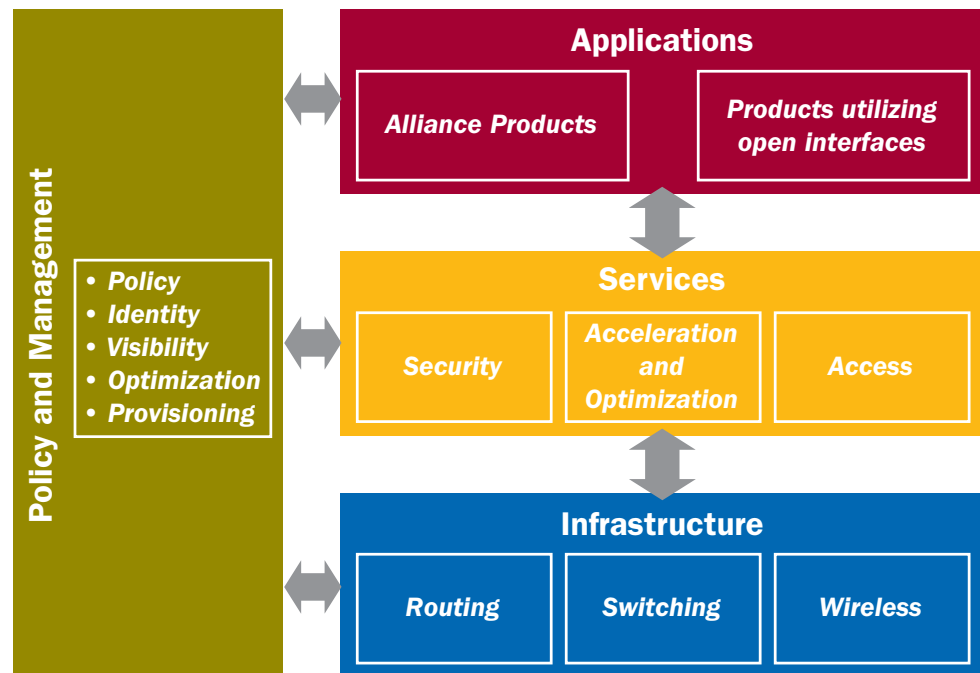


Figure 1: The Juniper Networks Enterprise Framework

The Applications layer provides support to the various software applications that are required to run the business. It provides the environment which allows applications to run and interoperate. The Infrastructure layer combines the network, data link, and physical layers and consists of routing and switching features that manage the network including LAN and WLAN switching, connection management, data flow, application quality of service (QoS), and transmission. The Services layer combines the traditional presentation, session, and transport layers and provides support to users and applications. It includes security services, applications interfaces, and acceleration and optimization services. The Policy and Management domain integrates with the customer's centralized policy and management functions that help reduce operations costs while simultaneously enabling compliance.

### Applying Juniper's Enterprise Framework at the Branch Office

The Juniper Networks Enterprise Framework supports the branch office by providing a best-in-class heterogeneous network environment that uses open, standards-based and industry-accepted interfaces and is based on the industry-standard Open Systems Interconnection (OSI) stack model. Enterprises use this framework to logically view their network infrastructure and applications in order to make decisions that best serve the requirements of deploying enterprise applications.

Juniper Networks takes a holistic approach to enterprise networking and takes into account the user perspective, the network perspective and the applications perspective. The company’s understanding of applications and how they are accessed from a variety of locations enable Juniper to provide a branch office architecture that meets the demands of high-performance organizations with enterprise solutions that are also tightly aligned to the business needs.

Customers like to deploy fewer, more highly integrated branch devices and manage them from a central location. Juniper provides branch office products that integrate routing, switching and security functionality, and support open standards that allows customers to leverage their existing investment and migrate seamlessly to the new infrastructure, and at the same time ensure that all their existing as well as new applications work in a seamless manner.

### The Juniper Networks Branch Office Reference Architecture

The sections that follow detail Juniper Networks branch office reference architecture (Figure 2) and present the design details that are specific to each of the branch office profiles. Juniper’s high-performance network infrastructure enables enterprises to create a responsive and trusted environment for the deployment of branch office infrastructure, services, and applications.

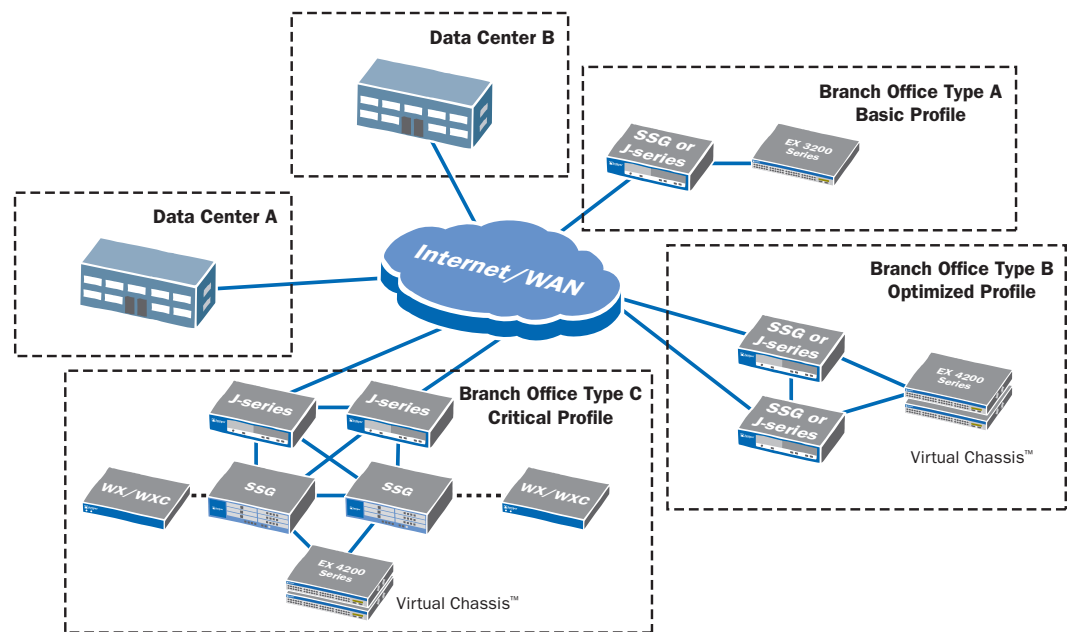


Figure 2: Branch Office Architecture

### Branch Office Profiles

Branch offices are business satellite facilities that are geographically dispersed and this makes network connectivity critical to branch business operations. At the same time, branch offices contain a relatively small amount of computing resources when compared to central facilities or data centers. Branch facilities typically are located where customer interactions occur, which means there is increased demand for supporting applications and assuring application performance, and an increased demand for security. Since branch offices usually lack the presence of a local IT staff, and the equipment hosted at these facilities must be not only cost effective, feature-rich and highly reliable, but also offer centralized management capabilities.

Since most enterprises employ far more users in branch offices than at headquarters, they need a branch office infrastructure that performs as well as the infrastructure in the headquarters. Most branch offices connect directly to headquarters via either a private WAN link or a VPN over the Internet, or they choose to deploy VPN over the private WAN link.

As more branch offices connect directly to the Internet rather than back-haul Internet traffic to headquarters, this introduces a new set of security, performance, connectivity and reliability challenges. Further deployment of real-time applications like voice and video causes another set of performance challenges—particularly from a latency, jitter and packet loss perspective.

For the purposes of this paper, it is assumed that all branch offices require the features and functionality discussed below.

### **Connectivity**

- Flexible connectivity to the WAN and Internet that supports a variety of interfaces (DSL, cable, T1/E1, DS3 etc.) that scale from kbps speeds to Gbps speeds
- Allow for split tunneling such that Internet traffic goes straight to the Internet, and data center traffic simultaneously is tunneled
- Assure sufficient bandwidth is allocated for critical applications especially with server centralization where most/all applications are accessed from remote data centers
- Support for granular QoS so that traffic can be prioritized based on real-time, business-critical or best effort (or as business demands) so that new applications like VoIP and video can be rolled out without requiring any/little change to the branch office infrastructure
- Support in-line power in order to deploy devices like IP phones, cameras, etc.
- Seamless LAN and WLAN connectivity
- Ensure service availability of both the LAN as well as WAN connectivity

### **Security**

- Provide a security policy that ensures quality of service (QoS), mitigates Denial of Service (DoS) attacks and threats, and ensures that the organization meets compliance criteria
- Rarely allow business applications (inbound) communication to the branch network, even then only from trusted sources
- Perform Network Address Translation (NAT) on all traffic going out to the Internet
- Require visibility into all traffic to the Internet, and the ability to control Web access
- Usually require Unified Threat Management (UTM) features (unless all traffic is backhauled to the headquarters/data center)
- Ensure that security features provide protection so that no virus penetrates the branch network
- Verify that no malicious payloads come into the branch office or are sent over to the headquarters/data center
- Enforce policies to ensure that employees, partners and guests get access only to authorized resources

### **Performance**

- Support server centralization without compromising end user expectations on application performance
- Deployment of integrated devices should not impact network performance
- Operations
- All fault and performance monitoring is done from a centralized location.
- All configurations for the branch office devices are determined centrally and deployed to each device remotely.
- All security policies are decided centrally and deployed using scripts, automation, and the remote deployment capabilities of the devices discussed.

Juniper's reference architecture builds a model that addresses the needs of the end users as well as the number of users at that particular branch office location. Juniper Networks classifies branch office architectures into three branch office profiles—Branch Office Type A - Basic, Type B - Optimized and Type C - Critical and each of these 3 profiles can vary in size – from supporting as few as 5 users to as many as 100s of users.

- *Branch Office Type A - Basic* – This branch office profile typically consists of a single integrated security and routing device, and one or more Ethernet switches to address the number of devices that are connected. WAN connectivity to the data center(s) is implemented with single or dual Internet connections. This profile is designed for small branch office locations where cost effectiveness is paramount (for example, retail facilities and small offices) and supports a basic feature set with standard availability. Typically, they consist of a simple LAN infrastructure to provide employee access. Very small branch office locations may just utilize the switching capabilities of the integrated security and routing device.
- *Branch Office Type B - Optimized* – This branch profile consists of two integrated security and routing devices and two or more Ethernet switches, all deployed in a fully-meshed configuration. WAN connectivity to the data centers utilize both private WAN and Internet connections. This profile supports small to medium-size branch office locations and offers high availability. Typically these are larger offices, and may require support for network segmentation or separate networks like employee network and guest network which drives the need to enforce identity based access control,
- *Branch Office Type C - Critical* – This branch profile consists of two edge routers, two security gateways, and two or more Ethernet switches, all interconnected via full mesh. WAN connections to the data centers use both Internet and private WAN connectivity. This profile provides the highest level of performance and availability and is designed to support diverse requirements for services such as VoIP, video, etc. Also, some of these types of branch office may directly be on the MPLS network as well. Also, and in addition to network segmentation and/or separate networks, these branch offices may host some local servers and services which drive the need to create a separate server LAN network.

Table 1 presents a summary of the features and capabilities correlated to each of the branch office profiles. The specific design and deployment considerations of each profile are presented in separate sections later in this document.

**Table 1: Branch Office Features and Capabilities**

	Feature	Capability	Type A – Basic	Type B – Optimized	Type C – Critical
<b>Connectivity</b>	Wide Area Network (WAN)	T1/E1	—	•	•
		MPLS *	—	—	•
		Broadband	•	•	•
	LAN	Wired	•	•	•
		PoE	•	•	•
		Wireless	Optional	Optional	•
<b>Security</b>	Unified Threat Management (UTM)	Deep Inspection	•	•	•
		Antivirus	•	•	•
		Web Filtering	•	•	•
	IPSec VPN	Integrated Firewall	•	•	•
<b>High Availability</b>	Link and Device Redundancy	Device Redundancy	—	•	•
		Link Redundancy	Optional	•	•
<b>Performance Optimization</b>	WAN and Applications Acceleration	WX/WXC	—	—	•

\* Denotes a functionality of J-series devices.

## Branch Office Devices

The branch office profiles support a variety of branch office environments, and differ in scale, complexity and performance requirements. The architecture allows organizations the flexibility to choose the edge devices used in the Type A and B branch profiles, so that they deploy a solution that best suits their branch office application.

The Type A - Basic and Type B – Optimized branch offices may be configured with either Juniper Networks Secure Services Gateway Series (SSG Series) or Juniper Networks J-series Service Routers (J-series). Both device families support secure communications using an IPSec VPN network. The Type C-Critical branch office requires both the J-series and the SSG firewall devices.

The SSG Series run the best-in-class security operating system ScreenOS and offers a full complement of security features that includes integrated UTM, stateful firewall, Antivirus, Web filtering and Deep Inspection. These devices also offer a variety of WAN and switching interfaces as well. The SSG is the recommended device for use in applications requiring high levels of security for secure branch office communications over the Internet.

The J-series routers run the industry leading JUNOS network operating system and are designed with firewall features coupled in addition to routing and switching functionality. They are ideal for branch office applications where backhauling all the traffic to a central site is mandated. They offer one-box convenience that simplifies deployment and device management.

Both the J-series and the SSG products support Ethernet interfaces that allows enterprises to connect a few Ethernet devices like PC's, printers etc. For additional connectivity requirements, all of the branch office profiles utilize the Juniper Networks EX-series Ethernet switches that support both fixed-configuration and virtual chassis configurations.

The EX 3200 series offer high-performance standalone switches for access-layer deployments in branch and remote offices. The EX 4200 series Ethernet switches with Virtual Chassis™ technology combine compact, pay-as-you-grow economics of stackable switches with the performance, flexibility, availability and manageability of chassis-based platforms. All EX-series switches offer an integrated Layer 2/3 packet forwarding engine that runs the same modular JUNOS™ software as all Juniper routers, ensuring a consistent implementation and operation of each control plane feature across an entire Juniper infrastructure. In addition, they support features like PoE, 802.1X based authentication, High Availability options, etc. that are critical for branch office deployments.

Table 2 provides a tabular guide that presents Juniper Networks branch office solutions based on branch office scale mapped to each of the profile definitions. A mapping of product functionalities to each of the profiles may be found in Appendix 1.

**Table 2: Product Recommendations Based on Branch Office Profiles**

Size of Branch	Small	Small-Medium	Medium	Medium Large	Large
Number of users	10 Users	50 Users	100 Users	250 Users	500 Users
Interface Type	Broadband	T1-E1	MLPPP-MLFR	MLPPP-MLFR	DS3
<b>Branch Office Type A - Basic</b>	SSG 5 or J-2320 and EX-3200	SSG 20 or J-2350 and EX-3200	SSG 140 or J-2350 and EX-4200	SSG 3X0 or J-4350 and EX-4200	SSG 550M or J-6350 and EX-4200
<b>Branch Office Type B-Optimized</b>	SSG 5 (x2) or J-2320 (x2) and EX-4200 (x2)	SSG 20 (x2) or J-2350 (x2) and EX-4200 (x2)	SSG 140 (x2) or J-2350 (x2) and EX-4200 (x2)	SSG 3x0 (x2) or J-4350 (x2) and EX-4200 (x6)	SSG550M (x2) or J6350 (x2) and EX-4200(x11)
<b>Branch Office Type C-Critical</b>			SSG 140 (x2) and J2350 (x2) and EX-4200 (x2)	SSG 3x0 (x2) and J4350 (x2) and EX-4200(x6)	SSG550M (x2) and J6350 (x2) and EX-4200(x11)

## General Design Considerations

There are some general design considerations that can be applied universally, regardless of the branch office profile. The following paragraphs discuss these considerations as they apply to network infrastructure, services and applications, as well as network policy and management.

### Infrastructure

#### LAN

When planning a LAN deployment, an architect should consider the following requirements. First, the capacity requirements of the LAN dictate the speed and number of ports required for connecting all machines at a branch to the LAN. Second, logical segmentation and how many logically separate networks should share the same LAN need consideration. Additional considerations include more application-specific requirements such as redundancy of LAN switching, Power over Ethernet (POE) capabilities of the LAN devices, and QoS marking at the source. Support for 802.1X, along with available security features such as Access Control Lists (ACLs), are also key considerations. Branch offices use one or more of the following LAN connection types:

- Employee LAN networks are used by employee workstations and are used to connect out to computing resources such as business applications, file servers, collaboration applications/ tools and the Internet.
- Guest LAN networks are used by non-employees for connecting to external resources, typically over the Internet. Guest LAN networks may be allowed to connect to a limited set of local business applications.
- Server LAN networks are mainly used to connect business application servers, file servers and collaboration servers to the branch- office network.

An enterprise branch office LAN infrastructure typically comprises one or two layers depending on the size of the branch. Small branch offices, of up to a few hundred ports, typically use an Access layer, comprised of one of two access switches deployed in a wiring closet, for interconnect of devices such as laptops, desktops, phones, printers, access points and cameras. Larger branch office site, supporting from 100's to 1000's of devices, typically have an Aggregation Layer to consolidate multiple access switches in multiple wiring closets. Each layer within the branch LAN hierarchical

topology has a specific function. The access layer serves as the periphery of the LAN network and provides interfaces to desktop computers, printers, network-connected phones and wireless access points deployed within the campus or branch. Switches serving the access layer are typically deployed in centralized wiring closets with copper, twisted pair cable “star-wired” to each of the supported devices. The Aggregation Layer serves as an aggregation point for multiple wiring closets. The Aggregation Layer is important in that it provides a layer between the WAN and the wiring closet. The Aggregation Layer is found in larger branch office deployments and is not necessary for small branch sites.

The LAN infrastructure is implemented with Juniper’s EX-series Ethernet switches. The HA options as well as the aggregation layers are typically implemented by using the Juniper EX-series switches with Virtual Chassis™ Technology.

### **Wireless LAN (WLAN)**

Wireless access found in each type of branch office. When designing a wireless network, a primary concern is often security. Today’s WLAN standards offer a good level of security functionality but in the final analysis, the security of the network is only as good as its security functionality implementation. Juniper SSG products offer enhanced security functionality for WLAN and can support multiple Service Set Identifiers (SSIDs) per device. By using multiple SSIDs, different security functionality can be used at different wireless networks, providing the best in both security and ease-of-use capabilities. Network architects tend to select the tighter security functionality with WiFi Protected Access (WPA) encryption and 802.1X authentication to provide a truly secure WLAN for the branch office. Additionally where needed, architects may grant open access to wireless with limited risk by employing a controlled Layer 3 security policy.

### **WAN Connectivity**

The branch office utilizes one, two or three of the following branch uplink connection types:

- Private Management of Point-to-Point (PTP) circuits - Typically these circuits will provide Layer 2 (L2) connectivity between two locations. A branch office is more likely to use this connection type, typically referred to as L2VPN or Private Circuits, where locations are permanent and importance of data communications is high.
- Provider Provisioned VPN (PPVPN) - The enterprise receives a full mesh of connectivity between multiple nodes. Referred to as L3VPN, this connectivity is typically Layer 3-based and the provider manages routing between the full meshed.
- The Internet – It usually connects between sites over the Internet with IPSec tunneling being used.

### **VPN**

The ability to establish IPSec VPN tunnels is clearly a fundamental necessity of a branch office solution. From a practical perspective, there should be sufficient capacity in terms of simultaneous tunnels (> 100) and encrypted throughput (> 100 Mbps) to meet any business objectives that may arise.

A full range of common encryption protocols such as 3DES and Advanced Encryption Standard (AES), key exchange (IKE, X.509), and user authentication options like passwords, RADIUS, Layer 2 Tunneling Protocol (LDAP) and tokens, along with associated features such as NAT traversal and L2TP within IPSec for Microsoft VPN clients, should be available to ensure a high degree of security as well as interoperability.

## QoS

In order to truly assure application connectivity over large networks, QoS is a key requirement. Defining a QoS strategy requires mainly two elements:

- Classifying the network and application traffic according to levels of sensitivity and criticality
  - As an example, a business application such as SAP or Oracle that manages purchase orders needs to deliver better performance to end users than simple Internet access. Another example would be VoIP traffic, which needs higher priority than business applications because it has less tolerance for delay, jitter or packet loss.
- Enforcing the strategy at the network choke points - The reason that choke points like routers and firewalls are specifically called out is that typically LANs do not suffer from congestion. It is mainly when the LAN is connected to the WAN that prioritization is necessary. To enforce a successful QoS strategy, enterprises should try to limit policing to only critical elements and choose suitable systems for classification and for policing. For example, in the Branch Office Type C profile, the SSG firewall does the classification and the J-series router does the enforcement.

## High Availability (HA)

Because there are various levels of HA, enterprises need to identify what level they want to achieve), and then deploy the appropriate level of device and link redundancy that supports the HA requirements.

Link-level HA essentially requires two links to operate in an active backup setting so that if one link fails, the other can take over (or likely reinstate) the forwarding of traffic that had been previously forwarded over the failed link. Failure on any given access link should not result in a loss of connectivity. This only applies to branch offices with at least two upstream links connected either to a private network or to the Internet

Another level of HA is device-level HA, effectively doubling up on devices to assure that there is a backup device to pick up in the event of a failed device. Typically the link redundancy and device redundancy are coupled, and this coupling effectively ties failures together. No single device failure should result in a loss of connectivity from the branch office to the data centers (except for branch offices Type A-Basic, which don't provide redundant devices).

A truly HA design that provides assured connectivity to business critical enterprises, branch offices should employ a combination of link and device redundancy that should connect the branch to dual data centers as shown in Figure 3. Traffic from the branch office should be dual-homed to each data center so that in the event of a complete failure in one of the data centers, traffic should be able to be re-routed to a backup data center. Whenever failures occur (link, device or data center), traffic should be rerouted in less than 30 seconds. Within this period of time, packet loss might occur but sessions will be maintained if the user applications can withstand these failover times.

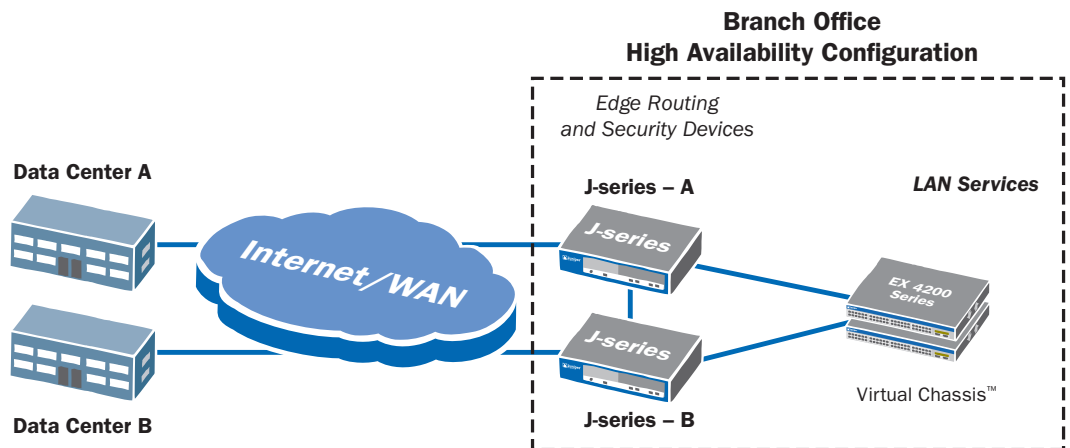


Figure 3: High Availability at the Branch Office

The branch office design that requires HA should also use two integrated routing and firewall devices as well as two Ethernet switches for full device redundancy within the branch. Using dual devices allows for a device to fail without taking down the network. It is important to note that a device may fail thereby causing a link failure, but the architecture provides a means to reroute the network traffic without service disruption.

The branch office integrated router and firewall devices are deployed in an active/active configuration and use separate WAN links. Cross connections between the integrated router and firewall devices ensure that a failure in one will not affect traffic flow between the data center(s) and the using endpoint. Load balancing should be performed so that traffic is balanced across the dual connections to the data centers. If a link fails, all traffic is directed via the remaining link through the use of redundancy protocols.

Using full mesh connectivity, the integrated router and firewall devices are connected to two Ethernet LAN switches. Full mesh connectivity and cross connections between the switches ensure that a device failure does not take down the network. Doing this ensures that the network does not affect user experience due to a fault or failure condition.

Lastly, branch offices with redundant devices should provide session persistence so that in the event of a failure, established sessions should not be dropped, even if traffic was being forwarded by the failed device.

## Services

### Firewall

Juniper's network design follows best practice principles of "least privileged" and "need to know" by dividing the network into purpose-defined segments with the use of security zones. The following definitions describe the main security zones to which each LAN segment is connected:

- **Trust Zone** – The Trust security zone connects the employee network to the security gateway located at the branch. This is based upon the assumption that all machines connecting to the Trust zone are part of the control and administration domain of the branch and, in turn, of the overall enterprise. Typically there will be no traffic that is destined to the Trust zone except for management/control traffic for the enterprise.
- **Untrust Zone** – The Untrust security zone connects the networks that are not fully controlled by the overall enterprise to the security gateway of the branch. "Not fully controlled" is defined as a physical segment that the wire goes through, which is not supervised by the enterprise.
- **Server Zone** – The Server zone is used for branch-specific services. These services are used only by branch users and not for remote users. Typically only inbound traffic will be allowed into the Server zone and probably some outbound server traffic such as Domain Name System (DNS), updates and Simple Mail Transfer Protocol (SMTP).
- **Guest Zone** – The Guest zone is used whenever unmanaged, non-controlled machines are connected to the network (for example, customers or partners coming into the branch office). The security policy for this zone should only allow access out to the Internet, and security services are not required for this zone except for limiting potential liability.
- **VPN Zone** – The VPN zone is used solely for the purpose of terminating IPSec VPN tunnels. The VPN zone is useful in defining a detailed security policy that defines permissions for traffic carried over a secure link from the headquarters networks to the branch Trust or Server zones.

### **DoS Attacks**

As part of the security design, it is important to consider how to protect the branch office infrastructure and any applications from DoS attacks that occur primarily with inbound traffic from the Untrust zone. Juniper recommends zone-level screening that includes the following:

- Limit number of connections from any source IP address
- Limit number of connections to specific destination IP address
- Limit number of connections for different network services such as Internet Control Message Protocol (ICMP) and DNS
- The network operating system of devices in the branch office network should themselves be auto policed so that a DoS attack to the device cannot bring down the network. Juniper's JUNOS operating system polices traffic to the control plane so that a DoS attack is incapable of bringing down the network device.

### **Unified Threat Management (UTM)**

As the network attack landscape continues to evolve, network architects can no longer afford to focus solely on protection against a single type of attack and expect their network to remain unaffected. The security considerations should include the following:

- The security solution at the branch office must not only stop attacks at each layer network, application and content, but they also need to stop both inbound and outbound threats.
- Need to implement a true, file-based Antivirus (AV) offering that deconstructs the payload, decodes the file or script, evaluates it for potential viruses and then reconstructs it, sending it on its way.
- To protect the network against application level attacks targeting software vulnerabilities via the network such as most network worms, or the sending of sensitive credit card data from a Spyware infected system, an Intrusion Prevention System (IPS) is the recommended solution.
- An IPS should look deep into the application layer traffic to detect attacks. It is important to choose a solution that does more than merely inspects the packets at the network layer or decodes only a few protocols at Layer 7– the solution should understand and 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.
- Implement a gateway Anti-Spam solution that can act as a preliminary filter by blocking known Spam and Phishing sources

Juniper Networks offers UTM security features as an integrated function in the SSG Series, and enables a business to protect itself from worms, spyware, trojans and malware. This is done by implementing a comprehensive set of security features that include antivirus (anti-spyware, anti- adware, anti-phishing), anti-spam, Deep Inspection and Web filtering.

### **WAN Optimization and Application Acceleration**

It is important to consider the competing demands of cost containment and increased network traffic. Since WAN costs typically account for IT's highest expenditure after headcount, most enterprises do not have the luxury of simply adding more WAN capacity to their networks. Branch offices WAN Optimization and application acceleration solution should support the following key requirements:

- Enable server centralization by providing LAN like application performance as users in branch offices access file and other servers in centralized locations.
- Support a variety of applications like email, file services, as well as implement technologies that accelerate protocols like TCP/IP etc.
- Support QoS and bandwidth optimization features that are critical to deployment of real-time applications like voice and video

Juniper Networks WX WAN Optimization and Application Acceleration Framework™ defines specific attributes that a WAN optimization and application acceleration platform must have in order to overcome the bandwidth, latency, congestion and manageability issues that impede application performance over the WAN. Each element of the WX Framework™ addresses a specific challenge that prevents applications from running efficiently over a WAN. Those elements are organized into four distinct categories: compression and caching, acceleration, application control and visibility. Working together, these interdependent technologies enable the Juniper Networks WAN application acceleration platforms (WX application acceleration platforms) and Juniper Networks WXC™ application acceleration platforms to make the most efficient use of available WAN resources and accelerate the performance of business-critical applications.

## **Applications**

### **Business Applications**

Typically, business applications are very sensitive to network downtime and poor network performance. Key considerations in deployment of business applications are availability, the connectivity of applications and the links to applications. Today's business applications are becoming more and more Web-based and moving away from client/server models. That being the case, there are fewer requirements from the infrastructure to support the Web applications. There are, however, some requirements to assure that these communications are always available.

For example, security should be fail-open from the branch perspective, but all communications to business-critical applications should be logged. The preferred data path should go through a leased line with assured QoS rather than over public unsecured Internet. These types of considerations should be taken into account when setting the boundaries for enabling business-critical communications.

### **Real-Time Applications: VoIP, Video and Unified Communications**

As enterprises deploy new productivity enhancement communication tools such as IP telephony, video conferencing and unified communications (integrated voice, video, chat), the key to successful deployment is to have a network infrastructure that provides fast and consistent application performance, high availability, reliability and security. As enterprises plan to provide this functionality to branch office users, it is critical that they have a clear understanding of what protocols are used (SIP, H.323) and what network requirements exist (latency, jitter, packet loss), combined with an understanding of the new security vulnerabilities that are continually being introduced. It is important to assign appropriate QoS to the network traffic so that the downstream network devices can expedite real-time traffic to ensure a satisfactory end user experience. Using the protocol specific application-level gateway (ALG) features on the firewall device is a recommended practice to protect the branch office IP Telephony gateway devices from potential attacks.

Many IP hard phones support Link Layer Discovery Protocol (LLDP), an open standard protocol that enables secure plug and play device discovery for third-party IP phones. Further, they support authentication methods in 802.1X, an Institute of Electrical and Electronics Engineers (IEEE) standard for port-based access control. Once an IP phone is placed on the network and connected to a switch, it is located using the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) protocol. Using 802.1X-based authentication, the RADIUS server places the phone on an appropriate VLAN.

### **Policy and Management**

According to Juniper Networks, it is not enough to have just a security policy. Policy-based networking must be implemented from the network, user and application perspectives. An applications policy includes acceleration and optimization, QoS, user access to each individual application, time of day and role-based access. The use of access control lists, user and identity management, and single sign-on (SSO) features are all part of the enterprise's policy and management heuristics.

### **Unified Access Control**

More often than not in today's ubiquitous world of Internet and network access, there are uncontrolled computers connecting to controlled networks, and this effectively renders these networks uncontrolled.

The main consideration points for deployment of Network Access Control (NAC) technologies are:

- Accessibility of user store and policy server
- Possibility to introduce 802.1X from a machine and infrastructure perspective
- Availability of infrastructure to assess computer risk levels - Effectively, do enterprises have a common antivirus or other host security client strategy that works and is reliable enough to make sound access control decisions?
- Impact to business from failures of NAC mechanisms
- Understanding of the real objectives of the NAC strategy - Is it to restrict access to resources? Is it to protect the infrastructure?

Juniper Networks provides the ability for unified access control to enforce dynamic access control policies based on user identity and endpoint integrity on an 802.1X switch/wireless access point infrastructure. Unified access control validates user identity, endpoint integrity and network information at L2, enabling administrators to enforce access control policy on a heterogeneous switch infrastructure and across the enterprise, and to deny user access to the network until user credentials and endpoint integrity status are validated.

The policy enforcement features for user access enable segregation of access into:

- Employees (Trusted users)
- Guests (Guest-level access viewed as Untrust)
- Servers and Devices (IP phones, PDAs, PCs)

### **Backup and Restore**

Bulk backup and restore capabilities are needed at branch offices to back up local data to centralized servers, and to restore branch office operations after system or network outages. When enterprises have a large amount of data transferring between certain branch/regional offices, it becomes important to optimize the WAN traffic so that other applications are able to get the expected service and performance.

Juniper's WX/WXC WAN application acceleration platforms provide a seamless way to compress WAN traffic and deliver performance improvements to the tune of 2X to 20X depending on the protocol (CIFS, MAPI, and so on). The Branch Office Type C profile can deploy outboard high-performance acceleration devices to supplement the architecture and further boost the performance of the enterprise network.

### **Centralized Management**

As enterprises look at rolling out new functionality to a large number of branch offices, it becomes increasingly important to take a new approach to network and security management. IT departments need to be provided with an easy-to-use centralized management solution that controls all aspects—including device configuration, network settings and security policy. Using standards-based and Juniper element management is both necessary and desirable based on the design principle of leveraging product strengths and reducing design risks. The slight increase in complexity of using both needs to be weighed against increased function and reduced function risk.

According to a 2006 McKinsey & Company report, the IT department of a typical enterprise spends 40 - 60 % of its budget to maintain and enhance basic IT services such as business applications, regulatory compliance, e-mail and web services. Juniper Networks lowers this cost greatly by providing JUNOS standard on all Juniper Networks switches and routing devices.

*NSM*- NetScreen-Security Manager (NSM) is a powerful, centralized management solution that controls the entire device life cycle of firewall/IPSec VPN and IDP devices, including basic setup and network configuration with local and global security policy deployment. Unmatched role-based administration allows IT departments to delegate appropriate levels of administrative access to specific users, thereby minimizing the possibility of a configuration error that may result in a security hole. NSM can scale from small to large enterprises by offering NSMExpress and NSM Central Manager as an easy-to-use plug-and-play appliance preloaded with the latest version of NSM software.

*JUNOS*- In addition to offering advanced carrier-class network services, JUNOS provides a consistent feature set and centralized management capability across the branch office routing and switching platforms which simplifies planning, speeds implementation, and enables intuitive day-to-day operations and management of any network.

By running a common operating system, these Juniper solutions dramatically reduce maintenance and management overhead while ensuring a consistent feature set across all products, as well as a consistent implementation and management of those features. This equates to time savings in all categories of operations. In addition to a reduction in training time, the inherent interoperability across all platforms greatly simplifies new feature deployment, software upgrades and other network modifications. A single consistent code set enables customers to qualify and deploy just one release. For many customers, the testing time of a new release is cut from what was months down to just a few weeks.

JUNOS also offers error-resilient configuration that prevents operators from inadvertently bringing down the network. IT must explicitly commit changes after entering and reviewing all modifications. In addition to automatically checking for errors or incorrectly constructed configurations that could cause potential problems, JUNOS provides a rollback command to quickly restore any of the 50 prior configurations.

*J-Web*- In addition to a full-featured command-line interface (CLI), J-Web, a web-based tool, is available to configure and manage any JUNOS device.

Built on JUNOS, J-Web offers highly available branch offices of all sizes a graphical user interface for device management complementing the exiting suite of element and service management products from Juniper. J-Web provides IT administrators and network operators with simple to use tools to quickly and seamlessly monitor, configure, troubleshoot and manage any switch, router, or firewall.

J-Web allows non-technical users in branch office/small office environments to commission and bring a router online quickly and easily. It offers seamless GUI access to all of the features and functions of JUNOS, reducing timelines for new service deployments. J-Web can be quickly integrated into existing network management or OSS (Operational Support System) applications such as Micromuse Netcool Omnibus, Dorado RedCell Manager, IBM Tivoli and HP OpenView, thereby minimizing complexity for the service provider or enterprise customer. Fast error-free service changes and upgrades can be made with J-Web's quick configuration wizards, and new services can be rapidly created and deployed with the use of configuration and QoS wizards that allow for real-time changes to service parameters.

In an independent study in 2007, Lake Partners quantified the time savings Juniper Networks customers experienced using JUNOS across a number of common network operational tasks. The results are presented in Table 3:

**Table 3: JUNOS Operating Efficiencies (Lake Partners 2007)**

Network Operations Task	Average JUNOS Efficiency
Adding Infrastructure	29%
Upgrading and Planned Events	23%
Troubleshooting and Unplanned Events	54%
Monitoring and Optimizing	24%
<b>Average Time Saved With JUNOS Software</b>	<b>25%</b>

This time savings translates to a substantial, tangible cost savings. According to Lake Partners, an infrastructure of any size running JUNOS software can save up to 29 % on operational costs.

More details around centralized management and implementation are discussed in the data center-related documents.

## Branch Office Type A - Basic Profile

The Branch Office Type A - Basic profile as shown in Figure 4 is the simplest branch design. It typically consists of a small office or retail environment with a local LAN that interconnects employee and guest workstations, laptops, servers, printers, and in some instances IP telephonic equipment. The Type A-Basic profile is a cost-effective branch office solution that leverages commercial broadband performance yet implements secure Internet connectivity through the use of Deep Inspection firewalls, antivirus, Deep Inspection, and Web filtering.

The Branch Office Type A - Basic computing environment typically has controlled applications needs and minimal or no resident servers. It has an external connection leading to the Internet with two IPSec VPN tunnels assigned to two different headquarter locations and is partitioned into three separate security zones—Trust, Untrust and VPN.

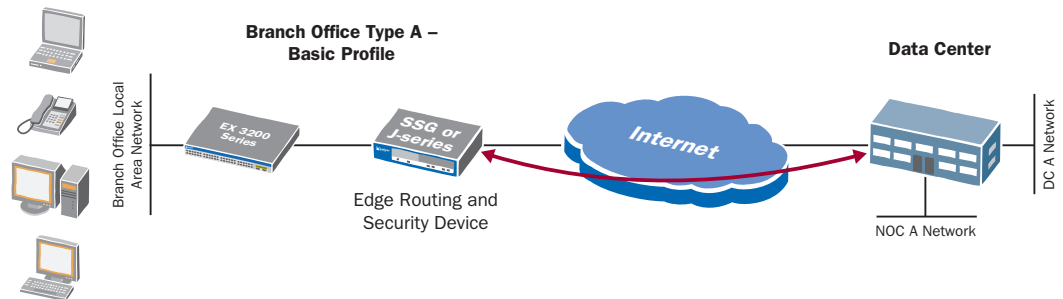


Figure 4: Branch Office Type A - Basic Profile

From a design perspective, the Type A - Basic configuration uses the SSG Series or the J-series router as the branch security device. The SSG device offers higher levels of protection since it provides additional security functions—for example, integrated capabilities for UTM such as firewall, antivirus, Web filtering and Deep Inspection.

The alternative configuration for the Type A - Basic profile replaces the SSG device with a J-series Services Router. The device functions as the branch office firewall and is deployed near the branch perimeter. The J-series devices are best suited for use when branch office requirements dictate the need for high-performance firewalls, with higher routing performance, but do not require UTM functionality—which is typically the case where all traffic to/from the branch office is backhauled to the Data Center.

LAN connectivity in the Type A - Basic branch office is implemented with a single fixed configuration EX 3200 series Ethernet switch. These devices offer cost efficient complete Layer 2 and Layer 3 switching capabilities, 10/100/1000BASE-T copper port connectivity with either full or partial power over Ethernet (PoE), and the full JUNOS feature set.

Typically, device or link redundancy is not required for the Type A - Basic branch office, although a backup dial connection or backup broadband connectivity can be easily implemented if desired. In addition, the Type A - Basic design can accommodate both wireless and wired LAN infrastructures. If hardware redundancy is desired within a single device, then select the EX-series switch and the J-Series router with dual internal power supplies.

Because the key requirements of a Branch Office Type A - Basic profile are secure connectivity over broadband using single device architecture, Juniper recommends using the SSG device to provide additional security functionality for Internet-connected branch locations.

## Connectivity

### LAN

This Branch Office Type A - Basic design is typically implemented using one or more EX-series switches. For enhanced scalability and availability requirements, an EX-series Virtual Chassis switch can be implemented. This branch office profile will usually consist of a single LAN network used by employees to connect out to computing resources such as business applications, file servers, collaboration applications/tools and the Internet. If wireless LAN is a requirement, then typically it is limited to employee only access.

### WLAN

For a Branch Office Type A - Basic profile, a simplistic WLAN infrastructure is typically implemented by using the wireless capabilities of the SSG 5 or SSG 20 devices. These devices also offer enhanced security functionality for the WLAN and can support multiple SSIDs per device. In this case, enterprises can extend the wired line communication capabilities by having a single SSID and using WPA encryption to provide a truly secure WLAN access.

### WAN

The Branch Office Type A - Basic profile is implemented using either one SSG or one J-series device (selected based on performance requirements) that connects to the Internet either over DSL or cable modem, and a backup connection to the Internet through an ISDN, secondary broadband connection or dial backup. Each connection from branch to data center or headquarters needs to have typically one IPsec tunnel that will permanently connect to the two different data center or headquarter locations, thus ensuring reliable connectivity while being cost effective. All inter-enterprise traffic is sent over the IPsec tunnel, while the rest of the Internet traffic is directly sent to the Internet over the broadband connection.

## Security

### Firewall

For Branch Office Type A- Basic configurations, Juniper recommends setting up the Trust, Untrust and VPN zones on the firewall.

- **Trust Zone** – All devices and connections in this zone are trustworthy, and all laptops, PCs and other LAN-based devices are connected to the Trust zone of the network.
- **Untrust Zone** – This zone is usually assigned to the primary and backup Internet connections and is used solely for the purpose of terminating IPsec VPN tunnels.
- **VPN Zone** – This zone is used solely for the purpose of terminating IPsec VPN tunnels. Any traffic that is directed at the corporate data center or headquarters location is always sent over the IPsec VPN tunnels.

### UTM

The SSG Family of products provides comprehensive UTM features to protect against network and application-level attacks and simultaneously stops content-based attacks. The following UTM features are recommended to be implemented for all types of branch offices.

*Deep Inspection*

Juniper recommends using Deep Inspection for any service where one of the endpoints may contain malicious code that could potentially exploit vulnerability at either of the endpoints. This includes any inward-bound network traffic from the Untrust part of the network or outward-bound traffic to the Untrust part of the network.

It is also important note to only use the signatures that are relevant to inbound or outbound traffic. For example, for outbound HTTP traffic originating from an employee’s computer to the Internet (Trust to Untrust), it is very important to secure the server-to-client vulnerability.

Additionally, Juniper recommends that enterprises secure the client-to-server interactions to limit the enterprises’ liability in case of attacks originating from their IP address space. It is also very important to ensure that all attack blocking and identifications are logged and monitored regularly.

*Antivirus, Anti-Adware, Anti-Phishing, Anti-Spyware*

Juniper recommends that enterprises scan all peer-to-peer and email traffic for worms, viruses, trojans and other malware to ensure that branch office devices do not receive any contaminated content.

Some customers may choose to block out peer-to-peer traffic completely. It is recommended to apply scanning to all external file transfers/sharing, more specifically to three different traffic vectors: Webmail, user POP3 mail retrieval and mail server SMTP inbound email. Further, it is important to centrally collect all the logs originating from the antivirus engine.

*Web Filtering*

Web filtering is most critical as a service for tracking productivity and corporate user behavior. Juniper recommends the use of Web filtering for all inter-enterprise Web traffic (branch to data center or headquarters) as well as all external Web traffic. It is important to note that the security profile should comply with the enterprise’s top-level security policy and acceptable use policy.

**Branch Office Type B – Optimized Profile**

The Type B – Optimized branch office design shown in Figure 5 is a configuration that adds a few more resources to the Type A - Basic profile. These include high availability and an additional security zone that is used for guest access. It includes 2 security devices, one device connects to a private link (L2VPN) and the other connects to the Internet. Device redundancy is achieved through the use of bridge groups with floating default routes. LAN redundancy is implemented with a EX 4200 series Virtual Chassis Ethernet switch connected to the edge devices in full mesh to provided an HA configuration.

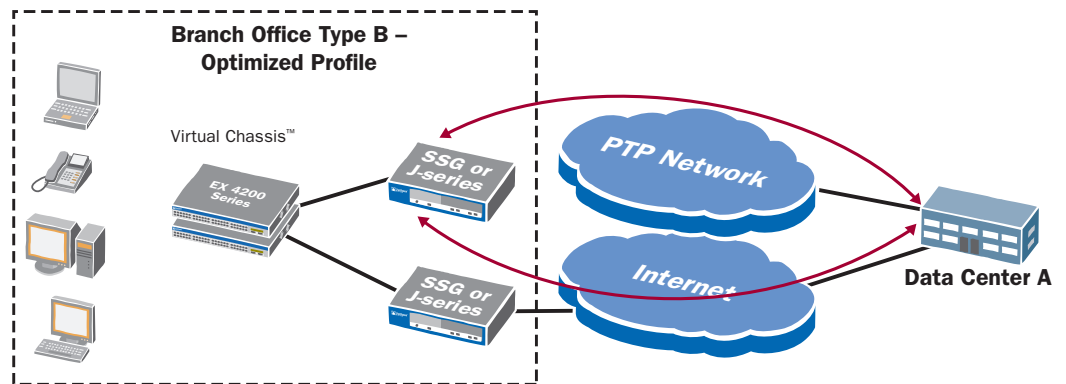


Figure 5: Branch Office Type B - Optimized Profile

The Type B - Optimized profile configured with SSG devices provides the same UTM features, firewall, antivirus, Web filtering and Deep Inspection as the Type A-Basic profile. In the Type B - Optimized profile, wide area communications are accomplished with either T1/E1 or broadband connectivity for high-speed performance, with the added security of device redundancy (using additional SSG or router devices) to ensure edge reliability using an HA configuration.

The Type B - Optimized configuration accommodates both wireless and wired LAN infrastructures and offers a guest access zone, load sharing and identity-based access control. LAN connectivity in the Type B - Optimized branch office is implemented with EX-series Virtual Chassis Ethernet switches. These switches offer cost efficient complete Layer 2 and Layer 3 switching capabilities, 10/100/1000BASE-T copper/fiber port connectivity (24- or 48-port) with either full or partial power over Ethernet (PoE) along with redundant fans and power supplies.

Because the key requirements of this type of branch office are reliable connectivity, device HA, guest access security, load sharing and identity-based access control, Juniper Networks recommends using a pair of SSG devices coupled with a single EX-series Virtual Chassis Ethernet switch with the devices configured in an HA configuration.

The alternate configuration for this profile replaces the SSGs with the J-series routers and configured for HA. The same segmentation and zones are also used in this configuration as those for the SSG device.

## **Connectivity**

### **LAN**

The Type B - Optimized branch office builds on the details discussed in the Type A - Basic configurations and is typically implemented using one or more EX-4200 Virtual Chassis switches. In addition to the employee LAN network (discussed in Type A - Basic section), the Type B - Optimized profile adds another network for "Guest Access" - typically used by non-employees for connecting to external resources over the Internet. Guest LAN networks may be allowed to connect to a limited set of local business applications as well. Additionally, Wireless LAN networks may be used for Guest as well as Employee access. In addition, the design considers VLAN capabilities for segmentation of traffic and uses the Ethernet switch High Availability (device and meshed redundancy) to ensure consistent level of services within the branch office as they are important considerations.

### **WLAN**

A simplistic WLAN infrastructure is typically implemented in this branch office configuration by using the wireless capabilities of the SSG 5 or SSG 20 devices. These devices also offer enhanced security functionality for WLANs and can support multiple SSIDs per device. By using multiple SSIDs, different security functionality can be used at different wireless networks, providing the best in both security and ease-of-use capabilities. Juniper Networks recommends the use of tighter security functionality with WPA encryption and 802.1X authentication combined with unified access control (discussed later) to provide a truly secure WLAN for the Type B - Optimized branch office. Additionally, it is possible to grant open access to guest users while limiting the risk by implementing a controlled L3 security policy.

### **WAN**

The Type B - Optimized branch typically has a pair of SSG devices or can use a pair of J-series with the appropriate model chosen based on performance and scalability requirements. One device is connected to the Internet either over DSL or cable modem and the second device is connected via a private link, thus offering redundant connectivity and redundant devices. Connections from the branch to the data center (or headquarters) are primarily via a private line/L2VPN/leased line. Over this connection, there is typically a need for two IPSec tunnels that permanently connect to the two different data center or headquarter locations. The primary connection to the Internet is via

the broadband connection. This connection is also used as a backup connection for traffic from the branch to data center/headquarters. To ensure secure connectivity in case the primary connection fails, two IPSec tunnels established over the Internet are recommended, with each tunnel connected to a different data center/headquarters location. When a primary leased line circuit is available, the only traffic running on these tunnels is the VPN monitoring traffic. All Internet traffic is sent directly to the Internet over the broadband connection using split tunneling.

## Security

### Firewall

In addition to the 3 zones (Trust, Untrust, Guest and VPN) setup in Type A - Basic branch profile, Juniper recommends setting an additional zone called Guest Zone for Branch Office Type B - Optimized profile. This zone is used solely for connecting machines that are not owned or managed by the enterprise IT department. It is normally used to provide Internet connectivity for users such as visitors, customers and partners.

### UTM

The recommended UTM policies are the same as those for the Branch Office Type A - Basic profile.

### Unified Access Control

Juniper Networks provides the ability for unified access control to enforce dynamic access control policies based on user identity and endpoint integrity on an EX-series (802.1X compliant) switch port or 802.1X wireless access point (Figure 6). Unified access control validates user identity, endpoint integrity and network information at L2, enabling administrators to enforce access control policies on a heterogeneous switch infrastructure. The enterprise denies users access to the network until their user credentials and endpoint integrity status have been validated.

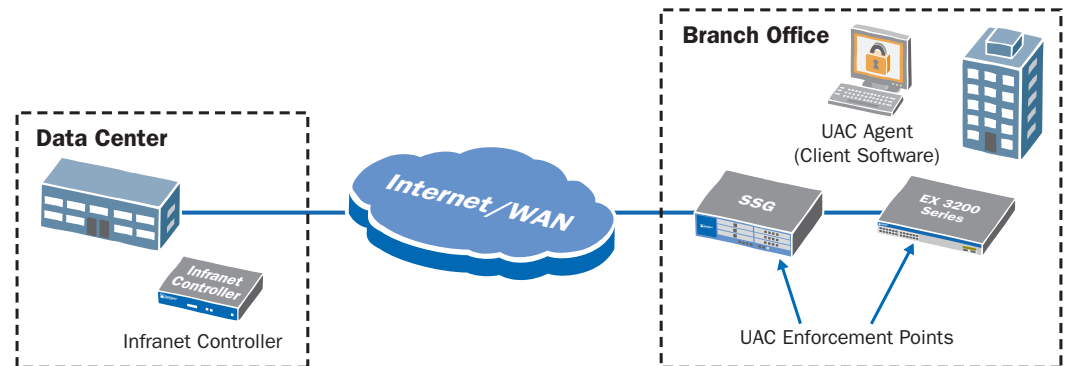


Figure 6: Unified Access Control for Branch Offices

It is recommended that unified access control at the branch be implemented using 802.1X authentication in order to associate users with the right VLANs and the right security zones, respectively, before connecting to the network. This means that enterprises need to enforce relevant access control security policies at the network level.

Users who do not pass the security posture assessment or do not map to a role that is allowed access to the corporate network will get associated to a Guest zone, and users who pass posture assessment and authentication will get associated with a Trust zone. It is also recommended that there be an easy-to-use remediation policy so that non-compliant users can find an easy way to become compliant. Also, it is critical to ensure that the connectivity from the branch office to the location where the Infranet Controller (IC) or the policy server is located is always available.

## High Availability

The Branch Office Type B - Optimized branch configuration provides device redundancy by having two SSG or J-series devices that ensure secure connectivity to the data center or headquarters: One device uses a point-to-point connection over a leased circuit, and the other is connected to the Internet and provides secure IPSec connectivity to the data center/headquarters using a broadband Internet connection. It is important to note that in this configuration, a lack of connection to the external world (point-to-point or via broadband) results in that particular device also being unavailable.

Further, the EX-series switches that sit behind the SSG and J-series devices are implemented based on the Virtual Chassis and are configured in active/active HA configurations so that reliable local area connectivity is achieved.

## Branch Office Type C - Critical Profile

The Branch Office Type C design supports “business critical” branch locations as shown in Figure 7, and adds a few services and resources to the Type B - Optimized profile. These include an additional zone for hosting local servers and an additional router device set for added flexibility (separation of routing and security domains) and services such as voice. Device redundancy is achieved through use of dynamic routing protocols and direct links between the firewall layer and the router layer. The Type C profile meets high-speed and high-performance demands. It is a services-ready solution that includes local server security, optimized VoIP, WAN optimization and identity-based access control. It is a High Availability profile for the larger branch office’s networking demand.

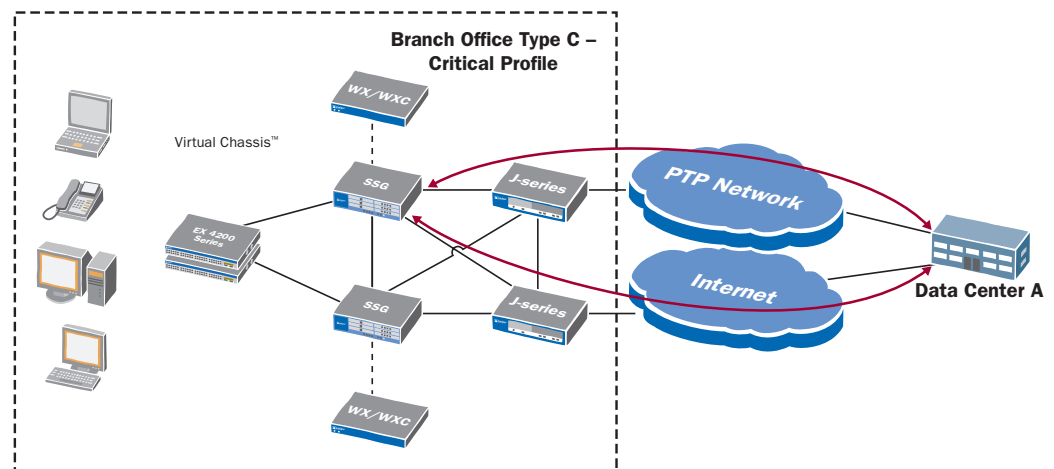


Figure 7: Branch Office Type C – Critical Profile

The Branch Office Type C - Critical branch office also offers a full complement of UTM capabilities. Wide area communication is accomplished with either DS3 or leased private connectivity for high-speed performance, with privatization and the added security of device and link redundancy. The branch office Type C profile accommodates both wireless and wired LAN infrastructures, and is implemented by using one or more EX-series Virtual-chassis Ethernet Switches and offers a server zone, guest access zone, load sharing, identity-based access control and optimized VoIP. Because the key requirements of this type of branch office are high availability, high speed/high performance, services-ready, VoIP and WAN optimization, Juniper recommends using a pair of standard J-series routers, a pair of SSG devices deployed in a High Availability configuration, and a single EX-series Virtual-chassis Ethernet Switch connected to the gateways in a full mesh configuration.

The standard J-series routers provide the routing functionality as well as embedded Avaya VoIP gateway functionality (if the enterprise is running an Avaya IP telephony solution). The SSG devices provide the firewall, VPN and UTM functionality. The WX devices (integrated service modules) can be integrated into the J-series router chassis configurations to provide WAN optimization and application acceleration functionality. The EX-series Ethernet switches (Virtual-chassis) provides assured LAN connectivity and are deployed in a redundant configuration for HA purposes. Dual 24-port or 48-port stackable switches can be deployed initially; as requirements grow, additional EX -series switches (up to a maximum of 10) can be interconnected and managed as a single device, delivering a scalable, pay-as-you grow solution for expanding network environments.

## **Connectivity**

### **LAN**

The LAN considerations for the Type C - Critical branch office builds on the considerations discussed in Type B - Optimized section. Since, this profile supports some local servers and services; an additional Server LAN network is supported. Any additional logical segmentation needed (.e.g. based on employees function –sales, marketing etc.) is typically implemented by deploying one or more VLANs. The Virtual Chassis EX switches are recommended to build out the LAN infrastructure for this type of branch office. Depending on number of users, an additional aggregation layer may be implemented as well. Other considerations include more application-specific requirements such as redundancy of LAN switching, POE capabilities of the LAN devices, and QoS at the LAN level. Other considerations would be support for security features such as 802.1X and ACLs.

### **Wireless LAN**

In Type C - Critical branch offices, a more complicated WLAN infrastructure is typically implemented by using the wireless capabilities of Juniper's wireless partners. Juniper recommends the use of tighter security functionality with WPA encryption and 802.1X authentication combined with unified access control (discussed later) to provide a truly secure WLAN for the Type C profile.

Other key considerations are radio coverage to ensure strong signals across the site and rogue detection through wireless IPS. Additionally, enterprises may grant open access to guest users while limiting the risk by implementing a controlled L3 security policy.

### **WAN**

The Type C - Critical branch office typically has a pair of J-series routers and a pair of SSG devices and EX-4200 Virtual Chassis switches (the appropriate models chosen based on performance and scalability requirements). One device is connected to the Internet either over DSL or cable modem and the second device is connected via a private link, thus offering redundant connectivity and redundant devices. Connections from branch to data center or headquarters are primarily via private line/L2VPN/leased line. Over this connection enterprises typically need to have two IPSec tunnels that will permanently connect to the two different data center or headquarter locations. The primary connection to the Internet is over the broadband Internet link. Without backhauling the traffic to headquarters, this connection uses a split tunneling mode to separate the traffic that goes out to corporate resources from the traffic going out to the Internet.

The Internet connection is used as a secondary connection from branch to data center/headquarters. To ensure secure connectivity, two IPSec tunnels are recommended, each to a different data center/headquarters location. VPN monitoring traffic is the only traffic over the IPSec VPN connection when the primary point-to-point connection to the data center/headquarters is available. All traffic to the Internet is sent directly over the broadband link.

## MPLS

Larger branch offices that implement the Type C - Critical configuration, may be connected directly to the MPLS network. When deploying MPLS, most enterprises will typically deploy it transparently as provided by a service provider, offering a reliable IP VPN service to the enterprise with strict service-level agreements (SLAs). In cases where the enterprise decides to build its own MPLS network, it may see advantages of increased reliability in conjunction with flexible network deployment. However, for smaller and medium-size enterprises, the cost effectiveness of MPLS still remains in question due to the fact that MPLS is an overlay on top of an expensive leased line infrastructure.

The Juniper Networks J-Series routers can support any DiffServ-Code Point or other IP precedence marking to enable the service provider to follow the priority schemes defined by the enterprise. This is in addition to controlling a queue of traffic at the edge of the branch office network after specific applications have been marked for appropriate QoS.

For enterprises that assemble and maintain their own MPLS network, the J-Series routers offer full-featured functionality for L3VPN or L2VPN-based MPLS networks and can serve as the ideal branch customer premises equipment (CPE) device for the self-managed enterprise MPLS network. Using MPLS, the enterprise can take advantage of the leased line's HA network infrastructure and can offer easy and predictable QoS.

## Security

### Firewall

In addition to the 4 zones (Trust, Untrust, VPN, and Guest) discussed in Type B - Optimized section, the Type C - Critical branch office provides an additional Server Zone. The Server Zone is used solely for local servers that provide critical services to branch office users such as DNS and SMTP.

### UTM

The recommended UTM policies are the same as those for the Type A - Basic branch office profile.

### Unified Access Control

The recommendations for deploying unified access control are the same as those for the Type B - Optimized branch office profile.

## High Availability

The Type C profile provides the highest level of availability by using device redundancy, as well as link redundancy, without these being dependant on each other. The routers connect between themselves and firewalls in full mesh with unique IP address connectivity. Each SSG firewall connects to both routers without a shared IP Address—no Virtual Router Redundancy Protocol (VRRP) and no NetScreen Redundancy Protocol (NSRP)—providing redundancy through dynamic routing protocol (DRP). The SSG devices connect to a shared LAN (broadcast domain) using a floating IP address (similar to VRRP). The SSG device connected to the J-series that has the point-to-point link to the data center/headquarters is the Active SSG device that holds the IP Address. The second SSG device acts as the backup device and assumes the IP address in case the primary (Active) SSG device fails on the LAN side.

In addition, the SSG devices synchronize session state between themselves, such that an SSG device failure does not force a session failure. The LAN switches are implemented with at least two redundant full switches in active/active configuration to provide HA. Further, enabling DoS protection on routers through stateless packet filtering helps to prevent the SSG device from receiving more user control plane traffic than it can handle, thus providing a higher level of availability.

LAN HA is implemented with EX-series Virtual Chassis Ethernet switches connected in a fully meshed configuration to the SSG gateways. This ensures that critical levels of service are maintained.

## VoIP and Unified Communications

This architecture permits the use of any IP telephony vendor solution to be deployed at the branch office. This Branch Office Type C - Critical profile provides a highly robust and secure environment for deploying VoIP both in a centralized mode, where all VoIP traffic is sent over the WAN to headquarters, as well as in a distributed mode, where there is more intelligence at the branch office itself (providing for higher local survivability). It is recommended that the ALGs for H.323, SIP and MGCP be turned on, to secure VoIP traffic to and from the data center/headquarters location.

For security purposes, it is recommended that IP phones be grouped together on VLANs or certain phones (for example, for contractors or guest workers) may be placed on separate VLANs. Sometimes each office or cube in an enterprise supports only one network connection, so most IP phones today include an integrated Ethernet bridge with a port connection for a computer.

It is important to note that a computer deployed with Juniper Networks UAC Agent also supports 802.1X, allowing automatic, secure discovery and authentication for both computers and phones (as long as the switch supports multi-drop 802.1X). Laptops of traveling workers can be authenticated via the centralized Infranet Controller (IC) and placed on an appropriate VLAN.

Enterprises deploying Avaya IP Telephony can consolidate the number of devices that they deploy and manage in their branch offices by embedding Avaya IG550 Media Gateway functionality in Juniper J-series J4350 and J6350 devices.

## Optimizing Application Performance

In the Branch Office Type C - Critical profile, if performance requirements are significantly higher, at least two WX or WXC devices are required to perform data compression (one on each side of the WAN as in Figure 8). Two or more devices that can compress and decompress data for each other are said to be in the same community. Businesses can selectively enable or disable data compression between any two devices in the same community. When they install a WX or WXC device, they must specify the IP address of a registration server. The registration server is a WX or WXC device that stores the network information for all the other WX and WXC devices that report to it, and is typically located at the data center or headquarters.

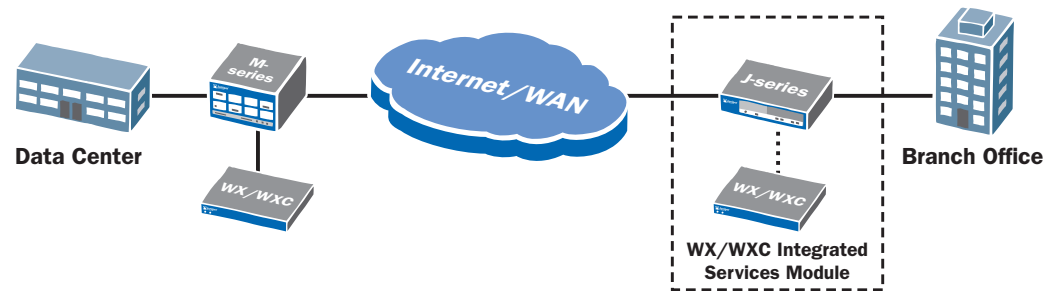


Figure 8: WAN Acceleration Configuration with WX/WXC Integrated Service Modules in Edge Devices

Since data compression occurs only between devices in the same community, businesses can optimize performance in large deployments by limiting the number of devices in each community. To send compressed traffic between communities, businesses can create a hierarchical structure where selected devices reside in multiple communities (discussed in greater detail in the WX Operators manual).

## Conclusion

Juniper Networks offers a set of very compelling solutions to meet the needs of branch office deployments. The reference architecture addresses the concerns of enterprises in each of the areas of connectivity, security, end-user performance and ease of operations. The different branch office profiles (Type A - Basic, Type B - Optimized, and Type C - Critical) address the requirements of today's branch office workers while ensuring that businesses continue to gain efficiencies in capital and operating expenses. The solutions outlined are built to scale to address current as well as future demands of high performance businesses. Finally, implementing these solutions with a single network operating system such as JUNOS allows enterprises to simplify management and realize significant savings in operational expenditure.

Additional information is available at [www.juniper.net](http://www.juniper.net).

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

## Appendix 1

### Product Tables

Product/Technology	Branch Type A – Basic	Branch Type B – Optimized	Branch Type C – Critical
Firewall/VPN	Uses integrated security functionality in SSG or J-series	Uses integrated security functionality in SSG or J-series	Uses integrated security functionality in SSG
Routing	Uses integrated routing functionality in J-series	Uses integrated routing functionality in J-series	Uses integrated routing functionality in J-series
Switching	Integrated into J-series and SSG Family EX-3200	EX-4200 Virtual Chassis	EX-4200 Virtual Chassis
Unified Threat Management (Antivirus, Anti-phishing, Anti-spyware, Anti-Adware, Anti-Keylogger, Anti-spam, Web Filtering)	Uses integrated security functionality in SSG	Uses integrated security functionality in SSG	Uses integrated security functionality in SSG
Unified Access Control	Policy enforcement is integrated into the SSG firewall. UAC appliance (Infranet Controller) is typically deployed at data center or headquarters location.		
WAN Application Acceleration	—	—	WX WXC
Centralized Management	NetScreen-Security Manager for security WX Central Management System (CMS) for WAN Application Acceleration JUNOScope for enterprise routers and switches		

### Partner Products

#### Symantec

Juniper Networks has teamed with Symantec Corporation to leverage its market-leading anti-spam solution for Juniper's small to medium office platforms to help slow the flood of unwanted email and the potential attacks they carry. Part of a complete set of UTM features available on Juniper Networks firewall/VPN gateway, the anti-spam engine filters incoming email for known spam and phishing users to act as a first line of defense. When a known malicious email arrives, it is blocked and/or flagged so that the email server can take an appropriate action. Anti-spam is available on Juniper Networks NetScreen-Hardware Security Client (NetScreen-HSC), NetScreen-5GT Series, NetScreen-25/50 and the SSG Family as an annually licensed feature.

#### Kaspersky

By integrating a best-in-class gateway antivirus (AV) offering from Kaspersky Lab, Juniper Networks integrated security appliances can protect Web traffic, email and Web mail from file-based viruses, worms, backdoors, trojans and malware. Using policy-based management, inbound and outbound traffic can be scanned, thereby protecting the network from attacks originating from outside the network, as well as those that originate from 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, evaluating them for potential viruses and then reconstructs them, sending them on their way.

The Juniper-Kaspersky solution detects and protects against over 100,000 viruses, worms, malicious backdoors, dialers, keyboard loggers, password stealers, trojans and other malicious code. Included in the joint solution is a best-in-class detection of spyware, adware and other malware-related programs. Unlike some solutions that use multiple non-file based scanners to detect different types of malware, the Juniper-Kaspersky solution is based upon one unified comprehensive best-of-breed scanner, database and update routine to protect against all malicious and malware-related programs. Antivirus is available on the NetScreen-HSC, NetScreen-5GT Series and the SSG Family as an annually licensed feature.

### SurfControl and Websense

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 an enterprise in four fundamental ways:

- **Security Threats:** Viruses, spyware and other malware can all enter an enterprise's network through Web-based email, file downloads, instant messaging, P2P applications and other non-work related sites.
- **Legal Threats:** Content that is inappropriate can lead to gender, minority or religious harassment and discrimination. Illegal downloading and distribution of copyrighted or illegal material over an enterprise's network has legal liability issues as well.
- **Productivity Threats:** 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:** Employees can crash an enterprise's network just by logging in to the wrong Web site. Other activity like recreational surfing and downloading MP3 files can divert valuable bandwidth from critical business needs.

To regulate inappropriate Web usage, Juniper Networks has teamed with both SurfControl and Websense to provide either an integrated (on-box) or redirect (two boxes) Web filtering solution.

**1. Integrated Web Filtering:** Integrated Web Filtering leverages an "in the cloud" architecture hosted by SurfControl's certified hosting partner that allows enterprises to build Web access policies from the largest URL database (over 6 million pages) spread across more than 40 categories. From the WebUI or NetScreen Security-Manager, an administrator can assemble firewall policies that incorporate and enforce Web access rights. Integrated Web filtering is available on the NetScreen-HSC, NetScreen-5GT Series, NetScreen-25/50 and the SSG Family as an annually licensed feature.

**2. Redirect solution with SurfControl or Websense:** Traffic is redirected from any of the firewall/VPN appliances to a customer-hosted server running the Web filtering software where Web access grant/deny decisions are made and executed. The customer is responsible for the server, the software and the associated management of the solution. Redirect Web filtering is supported across the entire product line.

### Avaya IG550

The Avaya IG550 Integrated Gateway provides an additional choice in the Avaya line of Media Gateways. Enterprises can now consolidate the number of devices that they deploy and manage in their branch offices. By embedding Avaya Media Gateway functionality in Juniper J-series J4350 and J6350 branch office routers, Avaya and Juniper can offer enterprises a one-box telephony, routing and security solution. This solution provides high-sustained network performance when under load, integrated voice and data security, and multilevel business continuity options. This best-in-class solution is available through Avaya direct channel and certified Avaya and Juniper resellers.

The Avaya IG550 Integrated Gateway consists of two primary components: a Telephony Gateway Module (TGM) and Telephony Interface Modules (TIMs).

The TGM550 module inserts into any slot in the J4350 or J6350 router and delivers a rich telephony feature set to the branch office. This feature set includes:

- Access to central Avaya Communication Manager and other communications applications
- Support for call center agents
- 6-party meet-me conferencing
- Local survivability in the event of a WAN failure
- Local music-on-hold and voice announcements
- Full encryption of voice traffic

The TGM operates as any other Avaya H.248-based gateway and includes a two-analog trunk/two-analog station module, modular Digital Signal Processors (DSPs) and a memory expansion slot.

There is a choice of several TIMs with analog, T1/E1/PRI and BRI options. The TIM514 analog module contains four trunks (FXO) and four stations (FXS); the TIM510 DS1 module supports T1/E1 and ISDN-PRI; and the TIM521 module supports four ISDN-BRI interfaces.

## Glossary

3DES	Triple Data Encryption Standard	NLS	Network Layer services
AES	Advanced Encryption Standard	NSM	NetScreen Security Manager
ATM	Asynchronous Transfer Mode	NTP	Network Time Protocol
AV	Antivirus	PE	Provider Edge
CRM	Customer Relationship Management	POE	Power over Ethernet
CPE	Customer Premises Equipment	POP3	Post Office Protocol Version 3
DHCP	Dynamic Host Configuration Protocol	PPVPN	Provider Provisioned VPN
DI	Deep Inspection	PTP	Point-to-point
DMZ	Demilitarized Zone	QoS	Quality of Service
DNS	Domain Name Server	RADIUS	Remote Authentication Dial-In User Service
DoS	Denial of Service	RDP	Remote Desktop Protocol
ERP	Enterprise Resource Planning	SAML	Security Assertion Markup Language
FR	Frame Relay	SFA	Sales Force Automation
FTP	File Transfer Protocol	SIP	Session Initiation Protocol
GRE	Generic Routing Encapsulation	SMB	Server Message Block
HA	High Availability	SMTP	Simple Mail Transfer Protocol
HTTP	Hypertext Transfer Protocol	SOAP	Simple Object Access Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	SSG	Secure Services Gateway
ICA	International Communications Association	SSH	Secure Shell
IDP	Intrusion Detection Processor	SSL	Secure Socket Layer
IKE	Internet Key Exchange	Split Tunneling	Allows a VPN user to access the Internet and private LAN or WAN via the same physical network connection
IM	Instant Messaging	TELNET	Teletype Network
IMAP	Internet Message Access Protocol	TNC	Trusted Network Computing
IPSec	Internet Protocol Security	UAC	Unified Access Control
ISDN Network	Integrated Services Digital Network	URL	Uniform Resource Locator
ISP	Internet Service Provider	URPF	Unicast Reverse Path Filtering
LAN	Local Area Network	UTM	Unified Threat Management
LDAP	Lightweight Directory Access Protocol	VLAN	Virtual LAN
L2	Layer 2	VNC	Virtual Network Computing
L2TP	Layer 2 Tunneling Protocol	VoIP	Voice over Internet Protocol
L2VPN	Layer 2 VPN	VPN	Virtual Private Network
MAPI	Messaging Application Programming Interface	WF	Web Filtering
MPLS	Multiprotocol Label Switching	WINS	Windows Internet Name Service
NAC	Network Access Control	WLAN	Wireless Local Area Network
NAT	Network Address Translation	XML	Extensible Markup Language
NBT	Net BIOS over TCP/IP		
NFS	Network File System		

CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS FOR  
NORTH AND SOUTH AMERICA  
Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
www.juniper.net

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS  
Juniper Networks (UK) Limited  
Building 1  
Aviator Park  
Station Road  
Aldershot  
Surrey, KT15 2PG, U.K.  
Phone: 44.(0).1372.385500  
Fax: 44.(0).1372.385501

EAST COAST OFFICE  
Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978.589.5800  
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS  
Juniper Networks (Hong Kong) Ltd.  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

**To purchase Juniper Networks solutions, please  
contact your Juniper Networks sales representative  
at 1-866-298-6428 or authorized reseller.**