Quick Reference Guide

Juniper your customer's Net™

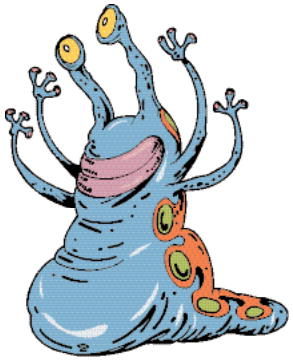
Juniper Networks Overview

Juniper Networks transforms the business of networking. A leading global provider of networking and security solutions, Juniper Networks maintains an intense focus on customers who derive strategic value from their networks. Its customers include major network operators, enterprises, government agencies, and research and educational institutions globally. Juniper Networks delivers a portfolio of networking solutions that support the complex scale, security and performance requirements of the world's most demanding mission-critical networks, including the world's top 25 service providers and 8 of the top 15 Fortune 500 companies.

Juniper Networks was founded with a single mission - to anticipate and solve the industry's most difficult networking and security problems. Today, Juniper Networks is enabling customers worldwide to create a competitive advantage by transforming the business of networking through:

- Securing networks against increasingly frequent and sophisticated attacks
- Leveraging networked applications and services that provide a competitive market advantage
- Providing secure and tailored access to remote resources for customers and business partners

Juniper Networks brings a new pace of innovation to the industry through purpose-built platforms and sophisticated software. It is recognized as a center of excellence in the development of silicon and software that support high- performance, intelligent networks, and remains at the forefront of industry initiatives that drive the continuing transformation of these networks and the businesses they support.



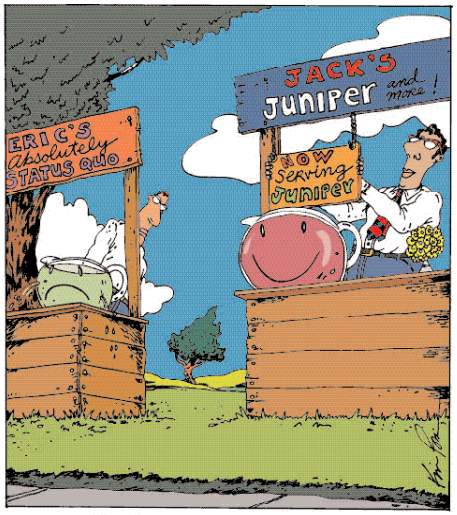
Juniper Networks Overview
Transforming our Business Partners 2
J-Partner Reseller Program Overview 3
Specialization Helps Capture New Opportunity 3
Maximizing the Total Financial Opportunity – The Juniper TFO 3
Juniper Networks Product Portfolio 4
Routers 6
Juniper Enterprise Routers at a Glance 6
JUNOS Router Software 6
J-Series Routers 8
M-Series Routers 11
Firewall / IPSec VPN Products 17
NetScreen ScreenOS Software 18
Small Office / Remote Office Security Solutions 19
Juniper Networks NetScreen-Hardware Security Client 21
Juniper Networks NetScreen-5GT 22
Juniper Networks NetScreen-5GT ADSL 23
Juniper Networks NetScreen-5GT Wireless 24
Juniper Networks NetScreen-5XT 26
Regional Office / Medium Enterprise Security Solutions 27
Juniper Networks NetScreen-25 / NetScreen-50 29
Juniper Networks NetScreen-204 / NetScreen-208 30
Central Office / Large Enterprise Security Solutions 31
Juniper Networks NetScreen-500 34
Juniper Networks ISG Series with IDP 36
Juniper Networks NetScreen-5200 / NetScreen-5400 38
Juniper Networks NetScreen-Remote VPN & NetScreen-Remote Security Client 40
SSL VPN
Juniper Networks SSL VPN Appliance Line 41
Juniper Networks Secure Access 700 42
Juniper Networks Secure Access 2000 44
Juniper Networks Secure Access 4000 46
Juniper Networks Secure Access 6000 48
Intrusion Detection and Prevention (IDP) 50
Application Acceleration Platforms 52
DX Application Acceleration Platforms 53
WX/WXC Application Acceleration Platforms 56
Management
Juniper Networks NetScreen-Security Manager 60
Juniper Networks NetScreen-SA Central Manager 63
WX Central Management System Software 64
Juniper Networks Frequently asked Questions 66
Product Warranty Information 68
General Disclaimer 69

Transforming our Business Partners

This compact reference guide gives you all the information needed to help you sell Juniper Networking Solutions. It includes product overviews, key features and benefits, plus essential selling suggestions that will enable you to effectively and efficiently position Juniper Networking solutions.

You can use this quick reference guide to:

- Identify key sales opportunities and recommend Juniper Network solutions
- Identify customer scenarios and cross sell Juniper Networking products
- Familiarize yourself with the Juniper Networks Product portfolio
- Get all the extra information that you need when closing a deal.



Now that there was a choice, Eric knew his days as a Reseller were numbered if he didn't start offering Juniper too.

J-Partner Reseller Program Overview

Juniper Networks revolutionizes the way resellers and vendors work together with the J-Partner Reseller program. Regardless of purchase volume, J-Partner rewards you for the value you add to selling and supporting Juniper Networks solutions. Through specialization and certification options, you gain access to one of the broadest portfolios of networking and security solutions available today.

Specialization Helps Capture New Opportunity

Define your value-add through specialization in one or more Juniper Networks solutions:

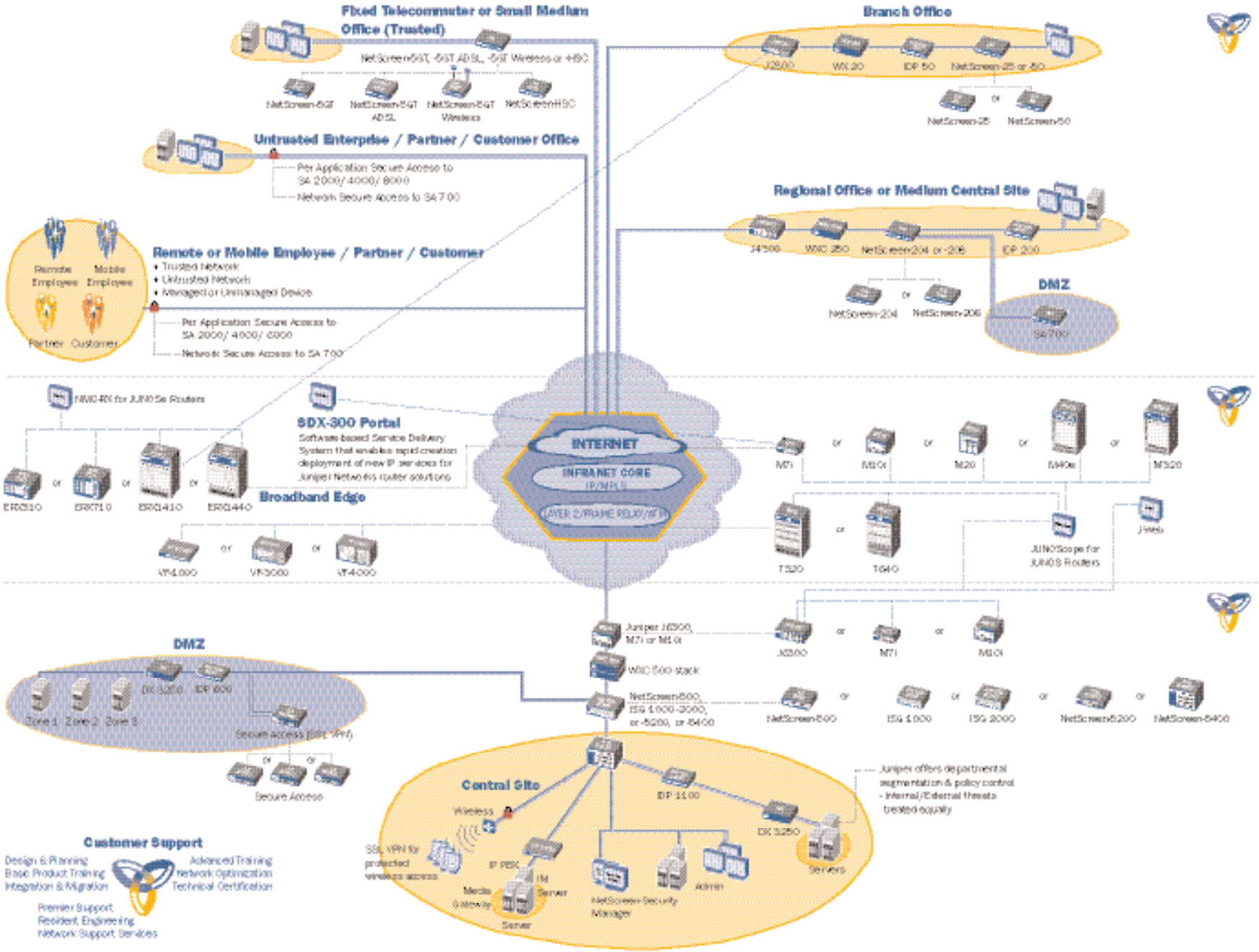
- Enterprise Networking – solutions associated with deploying, securing and maintaining enterprise business-critical networks
- Advanced Security – solutions associated with bringing network and application-level protection to high performance networks
- Service Provider Infrastructure – solutions deployed in the core of large service providers to deliver an assured customer experience on their networks

J-Partner gives you the flexibility to do business with Juniper Networks in the way that best fits your business model.

Maximizing the Total Financial Opportunity – The Juniper TFO

Juniper Networks is committed to the financial health of our partners. The J-Partner Total Financial Opportunity, or TFO, goes beyond pricing and gross margin. We find innovative ways to expand the financial opportunity for you. Beyond product access via specialization and value add pricing, the Juniper Networks TFO includes investment protection for industry certifications earned, flexible service programs, and the J-Rewards personal incentive program.

To learn more about the J-Partner Reseller Program, please visit **www.juniper.net/partners.**



Juniper M-series
M320
M40e
M20
M10i
M7i

Juniper T-series
T640
T320

Juniper J-series
J6300
J4300
J2300

Juniper E-series
ERX-1440
ERX-1410
ERX-710
ERX-310

Firewall & IPSec VPN
NetScreen-5200/5400
ISG 1000
ISG 2000
NetScreen-500
NetScreen-500 GPRS
NetScreen-204/208
NetScreen-25/50
NetScreen-5GT
NetScreen-5GT ADSL
NetScreen-5GT Wireless
NetScreen-5XT
NetScreen-HSC

SSL VPN
SA 700
SA 2000
SA 4000
SA 6000

Network Management
SDX-300
NMC-RX
Junoscope
J-Web
NetScreen-Security Manager
NetScreen-SA Central Manager

IDP 50/ 200/ 600/ 1100
IDP 50
IDP 200
IDP 600
IDP 1100

Session Border Controllers
VF-1000
VF-3000
VF-4000

DX Application Acceleration Platforms
DX 3200/3250
DX 3800/3850
DX 3850/RPS

WX Application Acceleration Platforms
WX 15
WX 20
WX 50
WX 55
WX 100

Routers

Juniper Enterprise Routers at a Glance

Juniper offers a broad portfolio of enterprise routers to meet the complex demands of widely distributed, business-critical applications. Juniper Networks enterprise routing platforms include:

- M7i and M10i high performance enterprise routers focused on data centers, large offices and campus borders which demand very secure, dependable, high-speed (2 Mbps – 2.5 Gbps) WAN connectivity – ideal for 45 Mbps+ requirements
- J2300, J4300, and J6300 enterprise routers focused on the WAN access routing needs of smaller sites such as remote, branch and regional offices (64 Kbps – 45 Mbps)

M-series and J-series routers are based on JUNOS; an advanced modular operating system proven in the most demanding routed networks, and is designed to ensure high reliability, security and performance.

JUNOS Router Software

JUNOS software is the first routing operating system designed specifically for the Internet, and is now deployed in the largest and fastest-growing networks worldwide. Its full suite of industrial-strength standards-based routing protocols, flexible policy language, and leading MPLS implementation efficiently scale to large numbers of network interfaces and routes.

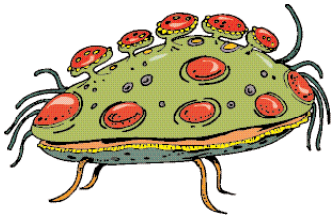
Architecture

The JUNOS architecture is a multi-module design, with each process running in protected memory to guard against system crashes and to ensure runaway applications do not corrupt each other. This modular design makes it significantly easier to restart or upgrade a specific module since a reboot of the entire platform is not required. Introducing new services does not adversely impact the entire operating system, resulting in highly reliable software architecture.

The J-series and M-series platform architecture cleanly separates routing from packet forwarding, and from services. This ensures predictable high performance and resiliency even under the most stressful operating conditions.

JUNIPER ADVANTAGES	KEY DIFFERENTIATORS
Strong Security	• Modular system architecture defends against attacks by protecting processing resources • Access to the router is always available – even while under attack • Additional integrated security services include Network Address Translation (NAT), Access Control Lists (ACLs), stateful inspection firewall and IPSec Encryption
High Uptime	• Network outages minimized by separating software functions into modular components • Minor problems cannot proliferate to full system crashes • Next generation CLI designed to help prevent operational errors, maintaining uptime
Predictable Performance	• Comprehensive, real-time granular control over network traffic, especially important during periods of high congestion • QOS mechanisms to classify, prioritize and schedule traffic to deliver predictable performance
Operations Flexibility	• One software code base across all routing platforms eases operations with straightforward software updates and upgrades • Fast certification of releases and full interoperability between products • Features for small and regional remote offices help lower the operations costs for installing, managing, monitoring and maintaining equipment
Centralized Management	• Juniper Networks JUNOScope provides automated control of a large number of enterprise routers, eliminating the need to manage individual routers • Multiple functions such as configuration management, inventory management and system administration • Reduce time and costs by leveraging an automated and integrated set of management applications

For More Information:
http://www.juniper.net/products/junos/



J-Series Routers

The J-series routers deliver the advanced JUNOS modular operating system in a hardware platform ideal for smaller sites, including remote, branch, and regional offices. The JUNOS software runs many functions independently to deliver high levels of security, uptime and performance with reduced operations effort. The J-series provides enterprises, government organizations, and research and education groups a forward-looking platform to build converged IP and IP/MPLS infrastructures. The modular and coherent design of the JUNOS operating system is fundamentally different from legacy routing systems. By running multiple functions in parallel on assigned processing resources, JUNOS delivers high stability with the flexibility to enable advanced routing, QoS, security, and management policies with predictable performance.

Key Features & Benefits

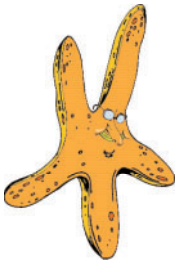
- Comprehensive range of interfaces supporting Serial, E1, NxE1, FE, ISDN, ADSL 2/2 + and DS3/E3
- Wide array of Layer 2 access protocols including Frame Relay, Ethernet, and PPP/HDLC
- Rich and granular QoS and instrumentation for prioritizing mission critical traffic such as voice
- Services features including Network Address Translation (NAT), Stateful firewall, IPSec, and J-Flow accounting
- Single JUNOS image regardless of features activated for reduced operational cost and complexity

When to Sell

- Customer looking to upgrade legacy routers due to performance, stability, or security issues
- Internet Gateway with multi-E1 to DS3 capacity where router and network security is critical
- WAN gateway with multi-E1 to DS3 capacity where QoS performance is critical
- IPSec VPN deployments to the remote or branch office locations
- Deploying applications which require predictable QoS even under load such as voice, video, or mission critical transactional applications

Competitive Products

Cisco 1700/1800, Cisco 2600/2800, Cisco 3600/3700, Allied Telesyn 725, 745, Nortel Passport 2430, 4400, 5430



Product Specs At-A-Glance

PLATFORM	J2300	J4300	J6300
Size	1U	2U	2U
Site Connections	2xE1/Serial/ISDN	2xE1/Serial to 12xE1	2xE1/Serial to DS3
Fixed LAN Ports	2xFE	2xFE	2xFE
WAN Interface Slots	1 fixed primary	6 Open Slots	6 Open Slots
Fixed WAN Interfaces	2xE1 or 2xSerial (integrated ISDN option)	N/a	N/a
WAN Interface Modules	N/a	2xE1, 2xSerial, 2xFE, ISDN, ADSL 2/2 + (Annex A/B)	2xE1, 2xSerial, 2xFE, ISDN, DS3/E3, ADSL 2/2 + (Annex A/B)
Memory (default/max)	256 MB / 1 GB DRAM	256 MB/ 1 GB DRAM	256 MB / 1 GB DRAM
Redundancy	No	No	Power (optional)
Services (IPSec, stateful firewall / NAT, J-Flow, Advanced BGP)	Software	Software	Software

Selected Part Numbers and Ordering Information

J-SERIES BASE SYSTEMS	J-SERIES OPTIONS
J2300 – Fixed chassis includes: • JUNOS (Worldwide version) • 2xE1, or 2xSerial ports with 1 interface port license • Available with integrated ISDN BRI option • 2xFE interfaces & 2xFE licenses • 256 MB DRAM in one slot with one open memory slot • 128 MB Compact Flash • Power supply and country/region-specific power cable **Available Models-** E1: J2300-1E2FEL-S-AC-EU Other power versions –UK, -IT Serial: J2300-1S2FEL-S-AC-EU, Other power versions –UK, -IT ISDN BRI S/T Models - E1: J2300-1E2FE1BL-S-AC-EU Other power versions: -UK, -IT Serial: J2300-1S2FE1BL-S-AC-EU Other power versions: -UK, -IT	**Additional DRAM:** 256 MB (J2300-MEM-256M-S) 512 MB (J2300-MEM-512M-S) **Primary Compact Flash:** Replaces default 256 MB (JX-CF-256M-S) 512 MB (JX-CF-512M-S) 1 GB (JX-CF-1G-S) **Additional Port Licenses:** E1(JX-1E1-LTU) and Serial (JX-1Serial-LTU) **Additional Software Feature Licenses:** IPSEC (J2300-IPSEC-LTU) Stateful Firewall (J2300-SFW-LTU) Advanced BGP (JX-BGP-ADV-LTU) JFlow Accounting (JX-JFlow-LTU) **Serial Cables:** EIA530 cable (DCE & DTE) JX-CBL-EIA530-DCE or -DTE RS232 cable (DCE & DTE) JX-CBL-RS232-DCE or -DTE RS449 cable (DCE & DTE) JX-CBL-RS449-DCE or -DTE V.35 cable (DCE or DTE) JX-CBL-V.35-DCE or -DTE X.21 cable (DCE or DTE) JX-CBL-X.21-DCE or -DTE

Selected Part Numbers and Ordering Information *continued*

J-SERIES BASE SYSTEMS	J-SERIES OPTIONS
J4300 – Modular chassis with 6 slots and no PICs includes: • JUNOS (Worldwide version) • 2 Fast Ethernet ports with licenses • 256 MB DRAM in one slot with one open memory slot • 256 MB primary Compact Flash • Power supply and country/region-specific power cable **Available Models-** J4300-2FEL-S-AC-EU Other power versions: -UK, -IT	**Additional DRAM:** 256 MB (J4300-MEM-256M-S), 512 MB (J4300-MEM-512M-S) **Interface Modules:** 2xE1(JX-2E1-1EL-RJ48-S), 2xSerial (JX-2Serial-1ISL-S) 2xFE (JX-2FE-1FEL-TX-S) 4 x ISDN (Basic Rate ISDN - S Interface JX-4BRI-S-S or Basic Rate ISDN - U Interface JX-4BRI-U-S) 1 x ADSL (Annex A JX-1ADSL-A-S or Annex B JX-1ADSL-B-S) **Additional Port Licenses:** E1 (JX-1E1-LTU), Serial (JX-1Serial-LTU), Ethernet (JX-1FE-LTU) **Primary Compact Flash:** Replaces default, 256 MB (JX-CF-256M-S) 512 MB (JX-CF-512M-S), 1 GB (JX-CF-1G-S) **Secondary Compact Flash:** 128 MB (JX-CF-128M-S), 256 MB (JX-CF-256M-S) 512 MB (JX-CF-512M-S), 1 GB (JX-CF-1G-S) **Additional Software Feature Licenses:** IPSEC (J4300-IPSEC-LTU), Stateful Firewall (J4300-SFW-LTU) Advanced BGP (JX-BGP-ADV-LTU), JFlow Accounting (JX-JFlow-LTU) **Serial Cables:** Same options as J2300
J6300 – Modular chassis with 6 slots and no PICs includes: • JUNOS (Worldwide version) • 2 Fast Ethernet ports with license • 256 MB DRAM in one slot with one open memory slot • 256 MB primary Compact Flash • Power supply and country/region-specific power cable **Available Models-** J6300-2FEL-S-1AC-EU Other power versions: -UK, -IT,	**Additional DRAM:** 256 MB (J6300-MEM-256M-S), 512 MB (J6300-MEM-512M-S) 1 GB (J6300-MEM-1G-S) **Interface Modules:** Same options as J4300 plus, JX-1DS3-S and JX-1E3S **Additional Port Licenses:** E1 (JX-1E1-LTU), Serial (JX-1Serial-LTU), Ethernet (JX-1FE-LTU) **Primary Compact Flash:** Same options as above **Secondary Compact Flash:** Same options as above **Additional Software Feature Licenses:** IPSEC (J6300-IPSEC-LTU), Stateful Firewall (J6300-SFW-LTU) Advanced BGP (JX-BGP-ADV-LTU), JFlow Accounting (JX-JFlow-LTU) **Serial Cables:** Same options as J2300 **Redundant Power:** J6300-PWR-AC-S

For More Information
http://www.juniper.net/products/jseries/

M-Series Routers

The M7i and M10i platforms are ideal enterprise routing solutions for central offices, campus networks and corporate backbones needing 45 Mbps+ or higher connectivity along with rich packet processing services. These platforms provide the key building blocks for high performance IP infrastructure that can be used for consolidation of voice, video, and data onto a single network. The modular and coherent design of the JUNOS operating system is fundamentally different from legacy routing systems. By running multiple functions in parallel on assigned processing resources, JUNOS delivers high stability with the flexibility to enable advanced routing, QoS, security, and management policies with predictable performance.

Key Features & Benefits

- 16 million packets per second of forwarding and packet processing performance
- Adaptive Services Module (M7i) or Adaptive Services PIC (M7i/M10i) for hardware-based Network Address Translation (NAT), stateful firewall, attack detection, IPSec, and J-Flow accounting
- Comprehensive range of interfaces supporting NxE1, DS3/E3, OC-3/STM-1, Fast Ethernet and Gigabit Ethernet WAN links
- Wide array of Layer 2 access protocols including ATM, Frame Relay, Ethernet, PPP, and HDLC
- Rich and granular QoS and instrumentation for prioritizing real time traffic such as voice and video
- Single JUNOS image regardless of features activated for reduced operational cost and complexity

When to Sell

- Customer looking to upgrade legacy routers due to performance, stability, or security issues
- Internet Gateway with a requirement for >45 Mbps+ where router and network security is critical
- WAN Gateway with a requirement for >45 Mbps+ where QoS performance is critical
- Campus core or backbone router with GE connectivity where layer 3 routing performance and reliability are critical
- Datacenter router with GE connectivity layer 3 performance is important
- Customer needs to run large filter lists (ACLs) while maintaining line rate performance
- VPN Migration — M-series routers support IPSec VPNs and stateful firewall; stand-alone or in combination with Juniper's advanced security appliances.
- VoIP Adoption — M-series platforms support VoIP transport with low jitter and delay, even during periods of heavy traffic load, through the extensive prioritization and QoS mechanisms of JUNOS

Competitive Products

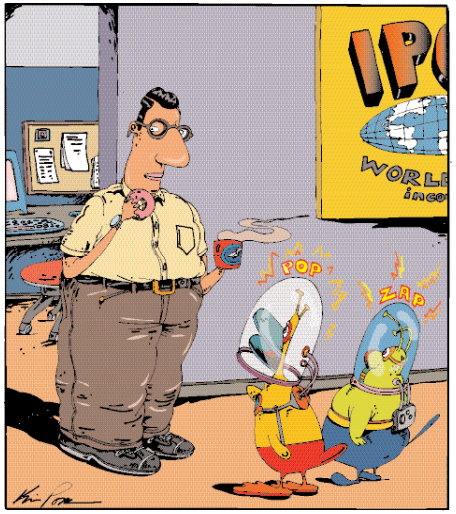
Cisco 72xx, 73xx, 75xx, 76xx

Product Specs At-A-Glance

PLATFORM	M7i	M10i
Size	2U	5U
Site Connections	E1 to GE or OC-12/STM4	E1 to OC-48/STM16
Fixed Interfaces	2xFE or 1 GE (SFP)	None
WAN Interface Slots	4 open PIC slots	8 open PIC slots
WAN Interface Modules	See ordering information	See ordering information
Memory (default/max)	256 / 768 MB DRAM	256 / 768 MB DRAM
Flash	Optional	128M flash + PCMCI adapter for secondary boot media
Redundancy	Power	Power, cooling, forwarding engine, routing engine
Services (IPSec, stateful firewall/NAT, J-Flow, CRTP)	Optional integrated ASM hardware Module	Optional AS PIC hardware module

Ordering Information

For a complete parts list please see the M-series datasheet located at **http://www.juniper.net/products/mseries/100042.html**



"Were from the future Stanley and youre the chosen one. wholl save this sinking network. So, drop the donut and get ahold of Juniper."

M7i Bundles

One chassis, one Fixed Interface Card (FIC) with either 2 x Fast Ethernet or 1 Gigabit Ethernet (GE includes small form factor pluggable optic module with SX optics), one routing engine with 256M DRAM, one compact forwarding engine board with 256M DRAM, one power supply, one fan tray JUNOS software, documentation CD. AC bundles include country-appropriate power cable. The Adaptive Services Module option can be ordered installed on the compact forwarding engine board by using model numbers in the right column.

FIXED INTERFACE CARD WITH FAST ETHERNET	STANDARD	WITH ADAPTIVE SERVICES MODULE
M7i, AC (UK Cable), 2 FE Ports	M7i-AC-2FE-UK-B	M7i-AC-2FE-ASM-UK-B
M7i, AC (IT Cable), 2 FE Ports	M7i-AC-2FE-IT-B	M7i-AC-2FE-ASM-IT-B
M7i, AC (EU Cable), 2 FE Ports	M7i-AC-2FE-EU-B	M7i-AC-2FE-ASM-EU-B
M7i, DC, 2 FE Ports	M7i-DC-2FE-B	M7i-DC-2FE-ASM-B

FIXED INTERFACE CARD WITH GIGABIT ETHERNET AND SFP	STANDARD	WITH ADAPTIVE SERVICES MODULE
M7i, AC (UK Cable), 1 GE Port (w/SFP SX)	M7i-AC-1GE-UK-B	M7i-AC-1GE-ASM-UK-B
M7i, AC (IT Cable), 1 GE Port (w/SFP SX)	M7i-AC-1GE-IT-B	M7i-AC-1GE-ASM-IT-B
M7i, AC (EU Cable), 1 GE Port (w/SFP SX)	M7i-AC-1GE-EU-B	M7i-AC-1GE-ASM-EU-B
M7i, DC, 1 GE Port (w/SFP SX)	M7i-DC-1GE-B	M7i-DC-1GE-ASM-B

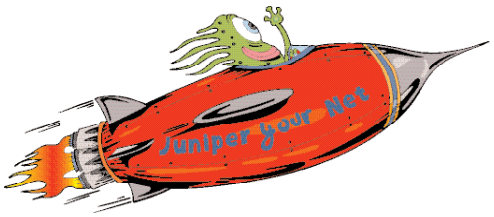
M10i bundles

Each bundle includes chassis, one routing engine with 256M DRAM (2 for redundant), one compact forwarding engine board with 256M DRAM (two for redundant), one high availability chassis manager board (two for redundant), two fan trays, two power supplies (three for AC redundancy, four for DC redundancy), JUNOS software, documentation CD. AC bundles include country-appropriate power cables.

M10i	NON-REDUNDANT	REDUNDANT
M10i, AC (UK Cable)	M10i-AC-UK-B	M10i-AC-HA-UK-B
M10i, AC (IT Cable)	M10i-AC-IT-B	M10i-AC-HA-IT-B
M10i, AC (EU Cable)	M10i-AC-EU-B	M10i-AC-HA-EU-B
M10i, DC	M10i-DC-B	M10i-DC-HA-B

M10i/M7i Spares

M10i/M7i Forwarding Engine Spare	FEB-M10i-M7i-S
M7i Forwarding engine Spare with built-in Services Module	FEB-M7i-SVCS-S
Routing Engine board spare. Flash media kit sold separately	RE-400-256-WW-S
M10i Chassis Spare	CHAS-MP-M10i-S
M7i Chassis Spare, 1 built-in GE port	CHAS-MP-M7i-1GE-S
M7i Chassis Spare, 2 built-in FE ports	CHAS-MP-M7i-2FE-S
High Availability Chassis Manager Board for M10i	HCM-M10i-S
M10i/M7i AC Power Supply Spare	PWR-M10i-M7i-AC-S
M10i/M7i DC Power Supply Spare	PWR-M10i-M7i-DC-S
M7i Fan Tray Spare	FANTRAY-M7i-S
M10i Fan Tray Spare	FANTRAY-M10i-S
Flash media kit with 256 MB flash drive and PCMCIA adapter	CF-ADAP-256M-S
Optional RE Memory Upgrade: 256 MB DRAM Module	MEM-RE-256-S



M10i/M7i Physical Interface Cards

ETHERNET	
1-port Gigabit Ethernet IQ PIC (Requires SFP)	PE-1GE-SFP-QPP
1-port Gigabit Ethernet PIC (Requires SFP)	PE-1GE-SFP
12-port 10/100 TX Ethernet PIC. Includes 3-meter RJ21 cable	PE-12FE-TX
4-port Fast Ethernet PIC, TX interface, RJ45 connector	PE-4FE-TX
ATM	
1-port OC-12/STM4 ATM2 IQ PIC, Single mode, IR	PE-1OC12-ATM2-SMIR
2-port OC-3/STM1 ATM2 IQ PIC, Multi mode	PE-2OC3-ATM2-MM
2-port OC-3/STM1 ATM2 IQ PIC, Single mode, IR	PE-2OC3-ATM2-SMIR
4-port DS3 ATM2 IQ PIC (ships with cable)	PE-4DS3-ATM2
2-port E3 ATM2 IQ PIC (ships with cable)	PE-2E3-ATM2
POS	
1-port SONET/SDH OC12/STM4 PIC, Single-Mode, IR	PE-1OC12-SON-SMIR
2-ports SONET/SDH OC3/STM1 PIC, Single-Mode, IR	PE-2OC3-SON-SMIR
2-ports SONET/SDH OC3/STM1 PIC, Multi-mode	PE-2OC3-SON-MM
CLEAR CHANNEL	
4-port DS3 PIC (and cables) with PIC ejector	PE-4DS3
2-port DS3 PIC (and cables) with PIC ejector	PE-2DS3
4-port E3 IQ PIC	PE-4E3-QPP
2-port E3 PIC (and cables) with PIC ejector	PE-2E3
4-port E1 PIC (75-ohm BNC connectors) (ships with cables)	PE-4E1-COAX
4-port E1 PIC (120-ohm RJ48 connectors)	PE-4E1-RJ48
4-port T1 PIC, (120-ohm, RJ48 connectors)	PE-4T1-RJ48
2-port EIA-530 PIC (DB-25 Connector)	PE-2EIA530
CHANNELIZED	
1-port Channelized STM1 to DS0 IQ PIC, SM, IR	PE-1CHSTM1-SMIR-QPP
4-port Channelized DS3 to DS0 IQ PIC, BNC	PE-4CHDS3-QPP
10-port Channelized E1 to DS0 IQ PIC, RJ48	PE-10CHE1-RJ48-QPP
SERVICES	
Adaptive Services II PIC	PE-AS2
Link Services PIC, 4 ML bundles, 256 LFI links, Tunnel Services	PE-LS-4
Tunnel Services PIC with PIC ejector	PE-TUNNEL

For additional physical interface cards please see
www.juniper.net/products/modules/

Interface Accessories

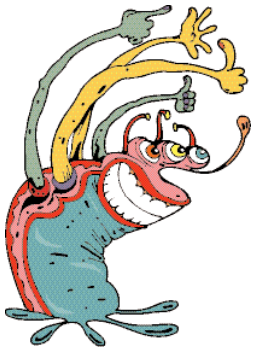
EIA-530 to V.35 cable (DTE) for M-series	CBL-EIA530-V35-DTE
EIA-530 to X.21 cable (DTE) for M-series	CBL-EIA530-X21-DTE
3-meter VHDCI to RJ21 Ethernet cable spare for PE-12FE-TX.	CBL-RJ21-MDI-S
3-meter VHDCI to RJ21 Ethernet cable spare for PE-12FE-TX	CBL-RJ21-MDIX-S
10-ft SMZ to BNC coaxial cable spare, for DS3/E3 PICs	CBL-SMZ-BNC-M-S
SFP 1000Base-LX Gigabit Ethernet Optic Module	SFP-1GE-LX
SFP 1000Base-SX Gigabit Ethernet Optic Module	SFP-1GE-SX
SFP 1000Base-T Gigabit Ethernet Module (for Cat 5 cable)	SFP-1GE-T

Software Licenses for the Adaptive Services Module/PICs

M7i can be ordered with the optional built in Adaptive Services Module (ASM), which comes with the stateful firewall/NAT software license for free (S-NAT-FW-MULTI). Additional licenses must be purchased. The Adaptive Services PIC or the Adaptive Services II PIC can be purchased for use with either M7i or M10i, all licenses for these PICs must be purchased.

J- Flow	S-ACCT
CRTP	S-CRTP
L2TP LNS license for M7i	S-LNS
NAT/FW Multi-instance	S-NAT-FW-MULTI
NAT/FW Single-instance	S-NAT-FW-SINGLE
IPSec	S-ES

For More Information:
http://www.juniper.net/products/mseries/



Firewall / IPSec VPN Products

The Juniper Networks integrated firewall / IPSec VPN security devices are purpose-built to perform essential security functions. These integrated devices combine a Stateful Inspection firewall with Deep Inspection technology for application-level protection, IPSec virtual private networking (VPN) capabilities, and denial of service (DoS) mitigation functions. Plus they are all manageable by a policy-based central management system, NetScreen-Security Manager. They are available in a range of devices built to meet the throughput requirements of enterprises of all sizes.

CUSTOMER NETWORK	PRODUCTS TO RECOMMEND	ENTERPRISE CLASS FEATURES
Small Office / Remote Office / Retail Outlet / Fixed Telecommuters	NetScreen-HSC NetScreen-5GT NetScreen-5GT ADSL NetScreen-5GT Wireless NetScreen-5XT	• Integrated security devices with Stateful and Deep Inspection firewall, IPSec VPN, Antivirus and Web Filtering • Rapid Deployment to quickly get a new device up and running • Device redundancy and resiliency for high availability • Secure 802.11 b/g wireless access for enterprise remote offices (NetScreen-5GT Wireless)
Regional Office / Branch Office / Medium Enterprise	NetScreen-25 NetScreen-50 NetScreen-204 NetScreen-208	• Denial of service attack protection • Application-level security with Deep Inspection and Web Filtering • Transparent mode to drop device into existing network with minimal changes • Dynamic routing support to reduce reliance on manual intervention
Medium & Large Enterprise Central Sites / Carrier Networks / Data Centers	NetScreen-500 ISG series NetScreen-5200 NetScreen-5400	• Purpose-built high-performance, scalable and flexible security solutions • Interface flexibility for varying network connectivity requirements • Customizable security zones to increase interface density • Comprehensive high availability solution for sub-second fail-over • Virtual System support for partitioning devices into multiple security domains • Application-level security with Deep Inspection or integrated IDP (ISG 2000 and ISG 1000)

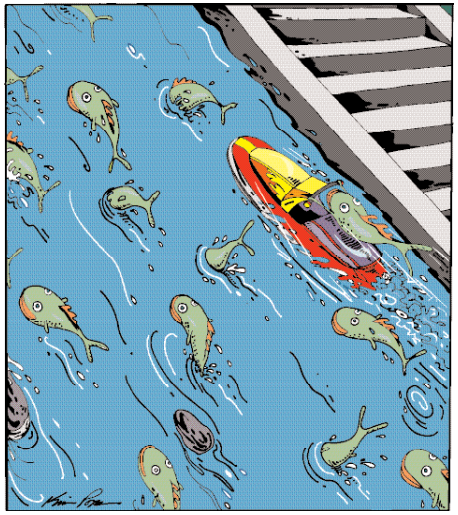
NetScreen ScreenOS Software

A controlling element of the Juniper Networks firewall / IPSec VPN devices is the operating system, ScreenOS, a real-time, security-specific operating system.

Key features and benefits

- Security specific real-time operating system that eliminates vulnerabilities found in general purpose operating systems
- Designed from the ground up to perform computationally intensive security functions without compromising throughput
- Stateful, protocol-level intelligence to prevent attacks in VoIP and other new technologies
- Integrated application-level attack protection with Deep Inspection, Antivirus and Web Filtering (not available on all products)
- Same operating system across the entire firewall / IPSec VPN product line means less training time for security administrators
- Certified by Common Criteria and ICSA

For More Information:
http://www.juniper.net/products/integrated/



Tired of a constant upstream battle with his company concerning change, Tad took it upon himself.

Small Office / Remote Office Security Solutions

Enterprises require integrated security products for their small offices, retail outlets, and fixed telecommuters that don't compromise on security, manageability, resiliency or price. Juniper Networks has the most robust portfolio of security solutions for the small office / remote office in the industry, providing solutions with superior security, central management and deployment, resiliency and high availability, all at competitive prices.

These solutions include the NetScreen-Hardware Security Client, NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-5GT Wireless and NetScreen-5XT.

Key Features & Benefits

- Integrated Deep Inspection firewall for application-level attack protection
- Integrated Antivirus at the network edge to stop viruses before they spread (NetScreen-HSC, NetScreen-5GT, NetScreen-5GT ADSL and NetScreen-5GT Wireless only)
- Integrated Web Filtering available to set policies on corporate web use (NetScreen-HSC and NetScreen-5GT)
- Rapid Deployment to quickly get a new device up and running for a telecommuter or small office without onsite IT staff and minimal effort
- Restricted security zones (home / work zones) to separate corporate traffic and resources from non-business activity
- Integrated ADSL modem eliminates the need for an external ADSL modem reducing upfront hardware and ongoing operational costs (NetScreen-5GT ADSL only)
- Device Redundancy for high availability and to minimize the potential for a single point of failure (NetScreen-5GT, NetScreen-5GT Wireless and NetScreen-5GT ADSL with Extended license only)
- Support for dial-backup or backup Ethernet ports for redundant Internet connections when network uptime is business critical
- Reduction in failover time of a VPN connection with redundant VPN tunnels and VPN monitoring
- Policy-based management for centralized, end-to-end lifecycle management

Licenses available on Juniper Networks Small Office / Remote Office Security Solutions

	NETSCREEN -HSC	NETSCREEN -5GT	NETSCREEN -5GT ADSL	NETSCREEN -5GT WIRELESS	NETSCREEN -5XT
10-user	No	Yes	Yes	Yes	Yes
Plus or Elite	Yes	Yes	Yes	Yes	Yes
Extended	No	Yes	Yes	Yes	No
Deep Inspection Signatures	Yes	Yes	Yes	Yes	Yes
Antivirus	Included*	Yes	Yes	Yes	No
Web Filtering	Yes	Yes	No	No	No

* The NetScreen-HSC Plus will support an embedded AV engine at a future date.

Juniper Networks Quick Reference Guide
Firewall / IPSec VPN Products 21
Firewall / IPSec VPN Products

Product Specs At-A-Glance

FEATURE / CAPACITY	NETSCREEN-HSC 5-USER/ PLUS	NETSCREEN-5GT 10-USER/ PLUS AND EXTENDED	NETSCREEN-5GT ADSL 10-USER/ PLUS AND EXTENDED	NETSCREEN-5GT WIRELESS USER/PLUS AND EXTENDED	NETSCREEN-5XT 10-USER/ ELITE
Number of Interfaces	5 10/100 Ethernet	5 10/100 Ethernet	5 10/100 Ethernet + 1 ADSL	5 10/100 Ethernet + 1 Wireless port with up to 4 SSIDs, 1 ADSL port (optional)	5 10/100 Ethernet
Maximum Number of IP Addresses in Trusted Interfaces	5 / Unrestricted	10 / Unrestricted Unrestricted on the Extended Version	10 / Unrestricted Unrestricted on the Extended Version	10 / Unrestricted Unrestricted on the Extended Version	10 / Unrestricted
Maximum Throughput	50M FW 10M 3DES VPN	75M FW 20M 3DES VPN	75M FW 20M 3DES VPN	75M FW 20M 3DES VPN	70M FW 20M 3DES VPN
Number of Sessions	1,000	2,000 4,000 on Extended version	2,000 4,000 on Extended version	2,000 4,000 on Extended version	2,000
Maximum Number of VPN Tunnels	2	10 25 on Extended version	10 25 on Extended version	10 25 on Extended version	10
Maximum Number of Policies	50	100	100	100	100
Maximum Number of Security Zones	2 (3 with home/ work zones)	2 (3 with home/ work zones) Trust/Untrust/ DMZ on Extended Version	2 (3 with home/ work zones) Trust/Untrust/ DMZ on Extended Version	2 (3 with home/ work zones) Trust/Untrust/ DMZ on Extended Version	2 (3 with home/ work zones)
Maximum Number of Virtual Routers	2	3	3	3	2
Routing Protocol Support	RIPv1/v2	RIPv1/v2, OSPF, BGP	RIPv1/v2, OSPF, BGP	RIPv1/v2, OSPF, BGP	OSPF, BGP, RIPv1/v2
Dial Backup Support	No	Yes	Yes	Yes	Yes
High Availability	No	No Yes on Extended version	No Yes on Extended version	No Yes on Extended version	No
Redundant Connections with Dual Untrust Support	Yes	Yes	Yes	Yes	Yes
Embedded Antivirus	Yes/Future	Yes	Yes	Yes	No
Integrated Web Filtering	Yes	Yes	No	No	No
External Web Filtering	Yes	Yes	Yes	Yes	Yes

Juniper Networks NetScreen-Hardware Security Client

The Juniper Networks NetScreen-Hardware Security Client (NetScreen-HSC) is the most cost effective integrated security solution for the fixed telecommuter and small remote office combining Stateful Firewall, Deep Inspection Firewall, Antivirus and Web Filtering. It can easily be deployed and managed in large deployments with Juniper Networks NetScreen-Security Manager and the Rapid Deployment capabilities, eliminating expensive staging steps.

When to Sell

- When integrated best of breed security functionality, reduced network complexity and low-cost are requirements
- Large scale fixed telecommuter / small remote office deployments where central management and configuration is a requirement
- Large scale deployments where minimal IT resources are available at the remote locations

Competitive Products

Cisco PIX 501, Check Point VPN-1 Edge, Check Point on Nokia IP40, Fortinet FG50A, SonicWall TZ170, TELE3, WatchGuard V10 and Firebox-X Edge

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-HSC with AV		
NetScreen-HSC	UK power supply	NS-HSC-003-AV
NetScreen-HSC	Europe power supply	NS-HSC-005-AV
Juniper Networks NetScreen-HSC (Plus)*		
NetScreen-HSC Plus	UK power supply	NS-HSC-103
NetScreen-HSC Plus	Europe power supply	NS-HSC-105

* The NetScreen-HSC Plus will support an embedded AV engine at a future date.

For More Information:
http://www.juniper.net/products/integrated/dsheet/110014.pdf

Juniper Networks NetScreen-5GT

The Juniper Networks NetScreen-5GT is a feature rich enterprise-class network security solution that integrates multiple security functions—Stateful and Deep Inspection firewall, IPSec VPN, Denial of Service protection, Antivirus and Web Filtering. The NetScreen-5GT is fully capable of securing a remote office, retail outlet, or a broadband telecommuter.

When to Sell

- For a fixed telecommuter / small remote office (NetScreen-5GT 10/Plus) or Large Remote Office / Small Company (NetScreen-5GT Extended)
- When integrated security functionality - Stateful and Deep Inspection firewall, IPSec VPN, Denial of Service protection, Antivirus and Web Filtering – are requirements
- When superior price/performance is a requirement
- When dial-back up is a requirement
- When device redundancy or network segmentation is a requirement (Extended license required)

Competitive Products

Cisco PIX 501, PIX 506E, Check Point VPN-1 Edge, Check Point on Nokia IP40, Fortinet FG50A, FG60, SonicWall TZ170, SOHO3, WatchGuard V10 and Firebox-X Edge

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-5GT 10 User*		
NetScreen-5GT	UK linear supply	NS-5GT-003
NetScreen-5GT	Europe linear supply	NS-5GT-005
Juniper Networks NetScreen-5GT Plus (unrestricted users)*		
NetScreen-5GT Plus	UK power cord	NS-5GT-103
NetScreen-5GT Plus	European power cord	NS-5GT-105
Juniper Networks NetScreen-5GT Extended*		
NetScreen-5GT Extended	UK power cord	NS-5GT-203
NetScreen-5GT Extended	European power cord	NS-5GT-205
Rack mount kit for 2 NetScreen-5GTs		NS-5GT-RMK

*For antivirus products add -AV to the above NetScreen-5GT SKU (NS-5GT-101-AV).

For More Information:
http://www.juniper.net/products/integrated/dsheet/110001.pdf

Juniper Networks NetScreen-5GT ADSL

The Juniper Networks NetScreen-5GT ADSL is a feature rich network security solution that integrates multiple security functions—Stateful and Deep Inspection firewall, IPSec VPN, Denial of Service protection and Antivirus—with an ADSL interface.

When to Sell

- To service provider or MSSP for a managed secure broadband service – integrated ADSL modem reduces CAPEX
- When integrated security functionality (Deep Inspection, Antivirus) are required with an integrated ADSL modem

Competitive Products

Cisco PIX 501, PIX 506E, Cisco 831, CheckPoint VPN-1 Edge, Check Point on Nokia IP40, Fortinet FG50A, FG60, SonicWall TZ170, SOHO TZW, WatchGuard V10 and Firebox-X Edge

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-5GT ADSL 10 User* Annex A		
NetScreen-5GT ADSL	UK supply	NS-5GT-013-A
NetScreen-5GT ADSL	Europe supply	NS-5GT-015-A
Juniper Networks NetScreen-5GT ADSL Plus (unrestricted users)* Annex A		
NetScreen-5GT ADSL Plus	UK power cord	NS-5GT-113-A
NetScreen-5GT ADSL Plus	European power cord	NS-5GT-115-A
Juniper Networks NetScreen-5GT ADSL Extended* Annex A		
NetScreen-5GT ADSL Extended	UK power cord	NS-5GT-213-A
NetScreen-5GT ADSL Extended	European power cord	NS-5GT-215-A
Juniper Networks NetScreen-5GT ADSL 10 User* Annex B		
NetScreen-5GT ADSL	UK supply	NS-5GT-013-B
NetScreen-5GT ADSL	Europe supply	NS-5GT-015-B
Juniper Networks NetScreen-5GT ADSL Plus (unrestricted users)* Annex B		
NetScreen-5GT ADSL Plus	UK power cord	NS-5GT-113-B
NetScreen-5GT ADSL Plus	European power cord	NS-5GT-115-B
Juniper Networks NetScreen-5GT ADSL Extended* Annex B		
NetScreen-5GT ADSL Extended	UK power cord	NS-5GT-213-B
NetScreen-5GT ADSL Extended	European power cord	NS-5GT-215-B

*For antivirus products add -AV to the above NetScreen-5GT sku (NS-5GT-011-A-AV).

For More Information:
http://www.juniper.net/products/integrated/dsheet/110027.pdf

Juniper Networks NetScreen-5GT Wireless

The Juniper Networks NetScreen-5GT Wireless brings enterprise level security applications, routing protocols and resiliency features to remote offices, retail outlets or broadband telecommuters that want to deploy 802.11 b/g networks in a secure manner. The NetScreen-5GT Wireless offers administrators up to four configurable Wireless Security Zones each with a unique SSID that can be used to provision appropriate levels of security for different types of users. The NetScreen-5GT Wireless also possesses the broadest range of wireless specific security support to help protect wireless communications and network resources. Wireless specific security includes:

- Security/Privacy: WEP, WPA (AES or TKIP), IPSec VPN
- Authentication: PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x

The broad range of supported wireless security also helps ensure policy consistency and interoperability with other wireless solutions that may be deployed throughout the enterprise. The NetScreen-5GT Wireless includes standard Ethernet connectivity with ADSL as a hardware option.

When to Sell

- For a fixed telecommuter / remote office / retail outlet requiring deployment of secure wireless access
- When integrated security functionality - Stateful and Deep Inspection firewall, IPSec VPN, Denial of Service protection and Antivirus – with wireless access is a requirement
- Requirement for a broad set of wireless-specific security and authentication mechanisms
- Need to assign appropriate levels of security to different user groups using Security Zones

Competitive Products

Cisco 831 + 1100 access point, Cisco PIX firewall + 1100 access point, Check Point 400W, Fortinet FG60WiFi, SonicWall TZ170 Wireless, WatchGuard Firebox-X Edge

For More Information:
http://www.juniper.net/products/integrated/dsheet/

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
Juniper Networks NetScreen-5GT Wireless 10 User	
NetScreen-5GT Wireless World - UK Power Cord	NS-5GT-023
NetScreen-5GT Wireless World - Europe Power Cord	NS-5GT-025
Juniper Networks NetScreen-5GT Wireless Plus	
NetScreen-5GT Wireless World - UK Power Cord	NS-5GT-123
NetScreen-5GT Wireless World - Europe Power Cord	NS-5GT-125
Juniper Networks NetScreen-5GT Wireless Extended	
NetScreen-5GT Wireless World - UK Power Cord	NS-5GT-223
NetScreen-5GT Wireless World - Europe Power Cord	NS-5GT-225
Juniper Networks NetScreen-5GT Wireless ADSL 10 User	
NetScreen-5GT Wireless ADSL World - UK Power Cord	NS-5GT-033-x
NetScreen-5GT Wireless ADSL World - Europe Power Cord	NS-5GT-035-x
Juniper Networks NetScreen-5GT Wireless ADSL Plus	
NetScreen-5GT Wireless ADSL World - UK Power Cord	NS-5GT-133-x
NetScreen-5GT Wireless ADSL World - Europe Power Cord	NS-5GT-135-x
Juniper Networks NetScreen-5GT Wireless ADSL Extended	
NetScreen-5GT Wireless ADSL World - UK Power Cord	NS-5GT-233-x
NetScreen-5GT Wireless ADSL World - Europe Power Cord	NS-5GT-235-x

-x must be replaced with an -A for Annex A units or a -B for annex B units

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

Due to lapses in Security, Sheep Inc. became easy pickings for undesirables.

Juniper Networks NetScreen-5XT

The Juniper Networks NetScreen-5XT is a feature rich enterprise-class network security solution integrating Stateful Inspection and Deep Inspection firewall, IPSec VPN, and DoS mitigation technology.

When to Sell

- For a fixed telecommuter / small remote office
- Government deployments where Common Criteria and/or FIPS certifications are a requirement

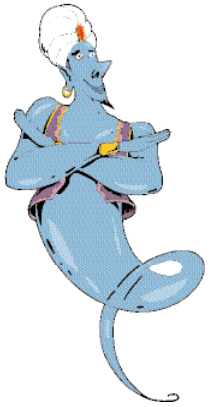
Competitive Products

Cisco PIX 501, 506E, CheckPoint VPN-1 Edge, Check Point on Nokia IP40, Fortinet FG60, FG50A, SonicWall TZ170, SOHO3, WatchGuard V10 and Firebox-X Edge

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-5XT 10 User		
NetScreen-5XT	UK power cord	NS-5XT-003
NetScreen-5XT	European power cord	NS-5XT-005
Upgrade from NetScreen-5XT 10-user to Elite		NS-5XT-ELU
Juniper Networks NetScreen-5XT Elite (unrestricted users)		
NetScreen-5XT Elite	UK power cord	NS-5XT-103
NetScreen-5XT Elite	European power cord	NS-5XT-105
Rack mount kit for 2 NetScreen-5XTs		NS-5XT-RMK

For More Information:
http://www.juniper.net/products/integrated/dsheet/110002.pdf



Regional Office / Medium Enterprise Security Solutions

The Juniper Networks integrated security solutions for the regional office, branch office or medium enterprise provide superior price/performance with extremely robust security features.

These solutions include the NetScreen-25, NetScreen-50, NetScreen-204 and NetScreen-208.

Key Features & Benefits

- Integrated Deep Inspection firewall for application-level attack protection
- Integrated Web Filtering available to set policies on corporate web use (NetScreen-25 & NetScreen-50 only)
- Denial of service protection to protect against more than 30 different attacks, both internal and external
- Comprehensive high availability solution for sub-second fail-over between interfaces or devices (HA Lite only on NetScreen-25)
- Dynamic routing support to reduce reliance on manual intervention to establish a new route
- Reduction in failover time of a VPN connection with redundant VPN tunnels and VPN monitoring
- Transparent mode where the device functions as a Layer 2 IP security bridge with minimal change to the existing network
- Virtual Router support to map internal, private or overlapped IP addresses to a new IP address
- Customizable security zones to increase interface density without additional hardware expenditures
- Manageable through graphical WebUI, CLI or central management system, NetScreen-Security Manager
- Policy-based management for centralized, end-to-end lifecycle management

Product Specs At-A-Glance – Advanced Feature Set

ADVANCED FEATURE/CAPACITY	NETSCREEN-25 ADVANCED	NETSCREEN-50 ADVANCED	NETSCREEN-204 ADVANCED	NETSCREEN-208 ADVANCED
Number of Interfaces	4 10/100	4 10/100	4 10/100	8 10/100
Maximum Throughput	100M FW 20M 3DES VPN	170M FW 45M 3DES VPN	400M FW 200M 3DES VPN	550M FW 200M 3DES VPN
Maximum Number of Sessions	32,000	64,000	128,000	128,000
Maximum Number of VPN Tunnels	125 + 100 dial up	500 + 400 dial up	1,000	1,000
Maximum Number of Policies	500	1,000	4,000	4,000
Maximum Number of Virtual LANs	8	8	32 default, up to 32 additional	32 default, up to 32 additional
Maximum Number of Security Zones	4	4	4 default, up to 10 additional	8 default, up to 10 additional
Maximum Number of Virtual Routers	3	3	3 default, up to 5 additional	3 default, up to 5 additional
Routing Protocols Supported	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2
High Availability Modes Supported	HA Lite	Active/Passive	Active/Passive Active/Active	Active/Passive Active/Active Active/Active Full Mesh
Deep Inspection	Yes	Yes	Yes	Yes
Integrated / Redirect Web Filtering	Yes / Yes	Yes / Yes	No / Yes	No / Yes

Product Specs At-A-Glance – Baseline Feature Set

BASELINE FEATURE/CAPACITY	NETSCREEN-25 BASELINE	NETSCREEN-50 BASELINE	NETSCREEN-204 BASELINE	NETSCREEN-208 BASELINE
Sessions	24,000	48,000	64,000	64,000
Site-to-site tunnels	50	150	500	500
Remote-access tunnels	Shared with site-to-site	Shared with site-to-site	N/A	N/A
VLANs	0	0	0[2]	0[2]
Routing Protocols Supported	RIPv1/v2	RIPv1/v2	RIPv1/v2	RIPv1/v2
High Availability (HA)	HA Lite[1]	HA Lite[1]	Active/Passive	Active/Passive
Deep Inspection	No	No	No	No
Integrated / Redirect Web Filtering	Yes / Yes	Yes / Yes	No / Yes	No / Yes

1 HA Lite provides configuration synchronization only (does not provide session or tunnel synchronization).
2 Virtualization key option – add 32 VLANs, 5 Virtual Routers and 10 Security Zones

Juniper Networks NetScreen-25 / NetScreen-50

The Juniper Networks NetScreen-25 and NetScreen-50 offer complete security solutions for enterprise branch and remote offices as well as small and medium size companies. They provide solutions for perimeter security with multiple DMZs, VPNs for wireless LAN security, or protection of internal networks.

NetScreen-25 offers 100 Mbps of firewall and 20 Mbps of 3DES or AES VPN performance, with support for 32,000 concurrent sessions, 125 site-to-site VPN tunnels, and 100 VPN users	NetScreen-50 is a high performance security appliance, offering 170 Mbps of firewall and 45 Mbps of 3DES or AES VPN performance, with support for 64,000 concurrent sessions, 500 site-to-site VPN tunnels, and 400 VPN users.

When to Sell

- Need for fully integrated security solution for enterprise branch and remote offices, as well as small and medium size companies
- Need for application-level protection with integrated Deep Inspection or Web Filtering
- When high availability and resiliency are requirements
- Perimeter security solutions for multiple DMZs, VPNs for wireless LAN security, or protection of internal networks

Competitive Products

Cisco PIX 506E, Check Point on Nokia IP130, Fortinet FG100A, FG200A, SonicWall PRO3060, TELE3, PRO230, WatchGuard V60 and Firebox-X

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-50 w/AC power supply		
NetScreen-50	UK power cord	NS-050-003
NetScreen-50f*	UK power cord	NS-050-103
NetScreen-50	European power cord	NS-050-005
NetScreen-50f*	European power cord	NS-050-105
Juniper Networks NetScreen-50 w/DC power supply		
NetScreen-50 w/DC power supply DC power		NS-050-001-DC
Juniper Networks NetScreen-25 w/AC power supply		
NetScreen-25	UK power cord	NS-025-003
NetScreen-25	European power cord	NS-025-005
Baseline Products		
NetScreen-50 Baseline	UK power cord	NS-050B-003
NetScreen-50 Baseline	European power cord	NS-050B-005
NetScreen-50 Baseline to Advanced Upgrade		NS-050-UPG-A
NetScreen-25 Baseline	UK power cord	NS-025B-003
NetScreen-25 Baseline	European power cord	NS-025B-005
NetScreen-25 Baseline to Advanced Upgrade		NS-025-UPG-A

*"f" products do not include VPN functionality (international only)

For More Information: **http://www.juniper.net/products/integrated/dsheet/110003.pdf**

Juniper Networks NetScreen-204 / NetScreen-208

The Juniper Networks NetScreen-204 and NetScreen-208 are two of the most versatile security appliances available today, easily integrating into many different environments, including medium and large enterprise offices, e-business sites, data centers, and carrier infrastructures. In addition to physical interface density, the NetScreen-200 Series optionally supports virtualization, including VLAN support and additional custom security zones and virtual routers.

NetScreen-204 offers four 10/100 Mbps interfaces with firewall functions at wire speed (400 Mbps).	NetScreen-208 offers eight 10/100 Mbps interfaces with firewall functions at wire speed (550 Mbps).

When to Sell

- Medium and large enterprise branch offices, e-business sites, data centers, and carrier infrastructures
- Where network segmentation, high availability and/or dynamic routing are requirements
- Perimeter security solutions for multiple DMZs, VPNs for wireless LAN security, or protection of internal networks

Competitive Products

Cisco PIX 515E-UR/R, Check Point on Nokia IP 350, Fortinet FG300A, FG400A, FG500A, SonicWall PRO5060, PRO4060, PRO230 and WatchGuard V80

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-208 w/ AC power supply		
NetScreen-208	UK power cord	NS-208-003
NetScreen-208	European power cord	NS-208-005
Juniper Networks NetScreen-208 w/ DC power supply		
NetScreen-208	DC power	NS-208-001-DC
Juniper Networks NetScreen-204 w/ AC power supply		
NetScreen-204	UK power cord	NS-204-003
NetScreen-204	European power cord	NS-204-005
Juniper Networks NetScreen-204 w/ DC power supply		
NetScreen-204	DC power	NS-204-001-DC
Juniper Networks NetScreen-200 Series Virtualization		
NetScreen-200	Virtualization Key*	NS-200-VIRT
Baseline Products		
NetScreen-208 Baseline	UK power cord	NS-208B-003
NetScreen-208 Baseline	European power cord	NS-208B-005
NetScreen-204 Baseline	UK power cord	NS-204B-003
NetScreen-204 Baseline	European power cord	NS-204B-005

*Virtualization Key adds 32 VLANs, 5 additional virtual routers, and 10 additional security zones. Only available with NetScreen ScreenOS 4.0.2 and later.

For More Information: **http://www.juniper.net/products/integrated/dsheet/110004.pdf**

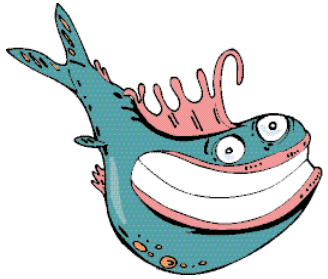
Central Office / Large Enterprise Security Solutions

Juniper Networks offers a line of purpose built, high-performance integrated security systems designed to deliver flexible and scalable solutions for large enterprise, carrier, and data center networks. These modular chassis-based systems offer virtual systems, robust high availability as well as interface flexibility. The Juniper Networks-ISG Series can be upgraded with integrated, best-in-class Intrusion Detection and Prevention (IDP) running on the security modules to stop worms, Trojans, Spyware, malware and other emerging attacks from penetrating and proliferating across the networks.

This line of products includes the NetScreen-500, ISG Series, NetScreen-5200 and NetScreen-5400.

Key Features & Benefits

- Comprehensive high availability solution for sub-second fail-over between interfaces or devices
- Full mesh configurations to allow for redundant physical paths in the network thereby providing maximum resiliency and uptime
- Virtual System support allowing devices to be partitioned into multiple security domains, each with a unique set of administrators, policies, VPNs, and address books
- Interface flexibility for varying network connectivity requirements and future growth requirements
- Virtual router support hides private IP addresses and allows multiple customers to use the same IP address without conflict
- Customizable security zones to increase interface density without additional hardware expenditures
- Transparent mode where the device functions as a Layer 2 IP security bridge with minimal change to the existing network
- Policy-based management via graphical WebUI, CLI or central management system, NetScreen-Security Manager, delivers flexible administrative alternatives.
- Optional IDP upgrade for the ISG 1000 and ISG 2000 provides the ability to stop Trojans, Spyware and malware on high speed networks up to 2 Gbps
- Application-level protection through Deep Inspection or through optional IDP upgrade on the ISG 1000 and ISG 2000



Product Specs At-A-Glance – Advanced Feature Set

ADVANCED FEATURE/CAPACITY	NETSCREEN-500 ADVANCED	ISG 1000 ADVANCED	ISG 2000 ADVANCED
Number of Interfaces	Up to 8 10/100 or 8 Mini-GBIC or 4 GBIC	4 fixed 10/100/1000 ports, up to 4 mini GBIC (SX or LX), up to 8 10/100/1000, up to 20 10/100	Up to 8 Mini-GBIC (SX or LX), up to 8 10/100/1000, up to 28 10/100
Maximum Throughput	700M FW 250 3DES VPN	1G FW 1G 3DES VPN	2G FW 1G 3DES VPN
Maximum Number of Sessions	250,000	250,000	512,000
Maximum Number of VPN Tunnels	5,000	2,000*	10,000*
Maximum Number of Policies	20,000	10,000	30,000
Maximum Number of Virtual Systems	25	10**	50**
Maximum Number of Virtual LANs	100 per physical port	250	500
Maximum Number of Security Zones	8 default, up to 50 additional	20 default up to 40** additional	26 default, up to 126** additional
Maximum Number of Virtual Routers	2 default, up to 25 additional	3 default, upgradeable to 13**	3 default, upgradeable to 53**
High Availability Modes Supported	Active/Passive Active/Active Active/Active Full Mesh	Active/Passive Active/Active	Active/Passive Active/Active
Routing Protocols Supported	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2
Deep Inspection	Yes	Yes†	Yes†
Integrated / Redirect Web Filtering	No / Yes	No / Yes	No/Yes
Integrated IDP	No	Optional upgrade	Optional upgrade

* Shared among all virtual systems ** Additional license required

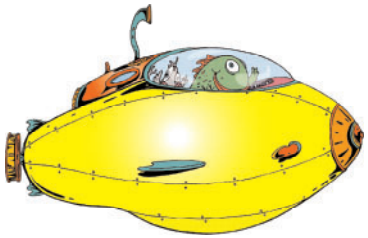
† Deep Inspection is automatically disabled when integrated IDP is installed

Product Specs At-A-Glance – Baseline Feature Set

BASELINE FEATURE/CAPACITY	NETSCREEN-500 BASELINE	ISG 1000 BASELINE	ISG 2000 BASELINE
Sessions	128,000	125,000	256,000
Concurrent VPN Tunnels	1,000	1,000	1,000
VLANs	100	50	100
Routing Protocols Supported	RIPv1/v2	RIPv1/v2	RIPv1/v2
High Availability	Active/Passive	Active/Passive	Active/Passive
Deep Inspection	No	No	No
Integrated / Redirect Web Filtering	No / Yes	No / Yes	No / Yes
Integrated IDP	No	No	No

Product Specs At-A-Glance

FEATURE/CAPACITY	NETSCREEN-5200	NETSCREEN-5400
Number of Interfaces	8 Mini-GBIC or 2 Mini-GBIC + 24 10/100	24 Mini-GBIC or 6 Mini-GBIC + 72 10/100
Maximum Throughput	4G FW 2G 3DES VPN	12G FW 6G 3DES VPN
Maximum Number of Sessions	1,000,000	1,000,000
Maximum Number of VPN Tunnels	25,000	25,000
Maximum Number of Policies	40,000	40,000
Maximum Number of Virtual Systems	500	500
Maximum Number of Virtual LANs	4,000	4,000
Maximum Number of Security Zones	16 default, up to 1000 additional	16 default, up to 1000 additional
Maximum Number of Virtual Routers	3 default, up to 500 additional	3 default, up to 500 additional
High Availability Modes Supported	Active/Passive Active/Active Active/Active Full Mesh	Active/Passive Active/Active Active/Active Full Mesh
Routing Protocols Supported	OSPF, BGP, RIPv1/v2	OSPF, BGP, RIPv1/v2
Deep Inspection	Yes	Yes
Integrated / Redirect Web Filtering	No / Yes	No / Yes



Juniper Networks NetScreen-500

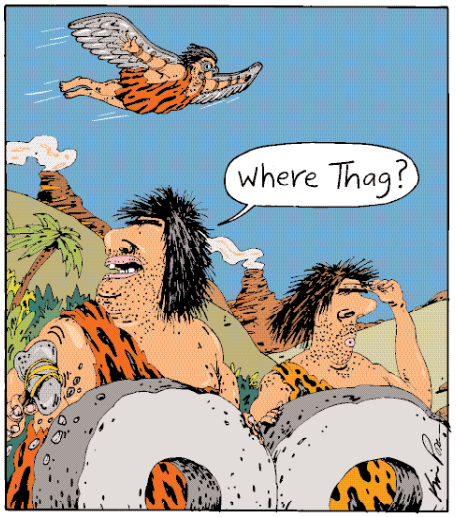
The Juniper Networks NetScreen-500 is a purpose-built, security system designed to provide a flexible, high performance solution. The NetScreen-500 security system integrates firewall, DoS, VPN and traffic management functionality. Combined with a flexible and resilient hardware architecture, the NetScreen 500 exceeds most enterprises' typical traffic conditions. It is well suited to match the peak load and strong deterrence requirements of the most demanding environments.

When to Sell

- For medium and large enterprise central sites and service providers
- High-performance, scalable and flexible security solution required
- High availability for resiliency and virtual systems for departmental firewalls required

Competitive Products

Cisco PIX 525-UR/R, PIX 535-UR/R, Check Point on Nokia IP710, IP380, Fortinet FG500A, FG800, FG1000, FG3000, SonicWall PRO5060, and WatchGuard V100



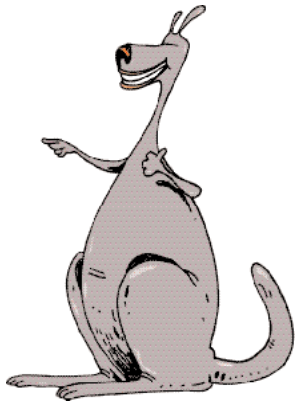
A born leader, Thag moves his company out of the Stone Age.

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-500SP Bundles		
NetScreen-500 System	SX GBIC, AC power	NS-500SP-GB1-AC
NetScreen-500 System	SX GBIC, DC power	NS-500SP-GB1-DC
NetScreen-500 System	SX dual-GBIC, AC power	NS-500SP-GB2-AC
NetScreen-500 System	SX dual-GBIC, DC power	NS-500SP-GB2-DC
Juniper Networks NetScreen-500ES Bundles		
NetScreen-500 System	2 SX GBIC modules, 2 AC power supplies	NS-500ES-GB1-AC
NetScreen-500 System	2 SX GBIC modules, 2 DC power supplies	NS-500ES-GB1-DC
NetScreen-500 System	2 SX dual-GBIC modules, 2 AC power supplies	NS-500ES-GB2-AC
NetScreen-500 System	2 SX dual-GBIC modules, 2 DC power supplies	NS-500ES-GB2-DC
NetScreen-500 System	3 dual-10/100 modules, 2 AC power supplies	NS-500ES-FE1-AC
NetScreen-500 System	3 dual-10/100 modules, 2 DC power supplies	NS-500ES-FE1-DC
NetScreen-500 System	2 dual-10/100 modules, 1 AC power supply	NS-500ES-FE2-AC
NetScreen-500 System	2 dual-10/100 modules, 1 DC power supply	NS-500ES-FE2-DC
Juniper Networks NetScreen-500 Baseline Systems		
NetScreen-500 System	2 dual-10/100 modules, 1 AC power supply	NS-500B-FE2
NetScreen-500 System	2 SX GBIC modules, 1 AC power supply	NS-500B-GB1
Juniper Networks NetScreen-500 Virtual System Upgrades		
Upgrade to 5 Virtual Systems		NS-500-VSYS-5
Upgrade from 5 to 10 Virtual Systems		NS-500-VSYS-10
Upgrade from 10 to 25 Virtual Systems		NS-500-VSYS-25

SP Systems include 25 Virtual Systems and 2 power supplies
ES Systems include 0 Virtual Systems

For More Information:
http://www.juniper.net/products/integrated/dsheet/110005.pdf



Juniper Networks ISG Series with IDP

The Juniper Networks Integrated Security Gateway (ISG) Series delivers unmatched firewall, VPN, and IDP performance through a combination of a fourth generation security ASIC, the GigaScreen3, high speed microprocessors and pluggable security modules each with their own processing and memory. The Juniper Networks ISG 1000 and ISG 2000—with integrated, best-in-class Intrusion Detection and Prevention (IDP) running on the security modules—stops worms, Trojans, Spyware, malware and other emerging attacks from penetrating and proliferating across the network.

A stateful inspection firewall, along with an IPSec VPN and robust networking capabilities, complements the integrated IDP functionality to deliver secure, reliable connectivity for critical, high-traffic network segments.

ISG 1000 is a fully integrated FW/VPN/IDP system with gigabit performance, a modular architecture and rich virtualization capabilities. The base FW/VPN system comes with four fixed 10/100/1000 interfaces and two additional I/O modules for interface expansion. The ISG 1000 also supports two security modules for IDP integration.	ISG 2000 is a fully integrated FW/VPN/IDP system with multi-gigabit performance, a modular architecture and rich virtualization capabilities. The base FW/VPN system allows for up to four I/O modules and three security modules for IDP integration.

When to Sell

- Medium and large enterprise, carrier and data center networks where linear performance across all packet sizes is required
- In environments where advanced applications that are sensitive to latency and inconsistent throughput such as VoIP and streaming media are being deployed
- Customer needs an fully integrated FW/VPN and IPS appliance providing network and application security for perimeter and high speed internal network deployments.
- Needs a solution that will meet future security requirements and leverage their investment
- High availability for resiliency and virtual systems for departmental firewalls required
- Optional IDP upgrade provides ability to stop Trojans, Spyware and malware on high speed networks up to 2Gbps
- Fully managed by NetScreen-Security Manager for centralized and unified policy management, network settings, and device configuration across all the security components

Competitive Products

Cisco PIX 535-UR/R, Check Point on Nokia IP1220, IP740, IP710, Fortinet FG1000, FG3000, FG3600, SonicWall PRO5060 and WatchGuard V200

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
ISG 2000 and ISG 1000 Systems	
NS-ISG-2000 System (inc AC power supplies, No I/O cards)	NS-ISG-2000
NS-ISG-2000 System (inc DC power supplies, No I/O cards)	NS-ISG-2000-DC
NS-ISG-2000 Baseline System (inc AC power supplies, No I/O cards)	NS-ISG-2000B
NS-ISG-2000 Baseline System (inc DC power supplies, No I/O cards)	NS-ISG-2000B-DC
NS-ISG-1000 System (inc AC power supply, No I/O cards)	NS-ISG-1000
NS-ISG-1000 System (inc DC power supply, No I/O cards)	NS-ISG-1000-DC
NS-ISG-1000 Baseline System (inc AC power supply, No I/O cards)	NS-ISG-1000B
NS-ISG-1000 Baseline System (inc DC power supply, No I/O cards)	NS-ISG-1000B-DC
Integrated IDP Upgrades	
Security module for IDP on ISG 1000 and ISG 2000 systems	NS-ISG-SEC
IDP Upgrade Kit, including IDP License Key, additional memory, and 5-device NSM (ISG 1000)	NS-ISG-1000-IKT
IDP Upgrade Kit, including IDP License Key, additional memory, and 5-device NSM (ISG 2000)	NS-ISG-2000-IKT
ISG 2000 and ISG 1000 I/O Modules	
I/O Module - Dual Port Mini GBIC-SX	NS-ISG-SX2
I/O Module - Dual Port Mini GBIC-LX	NS-ISG-LX2
I/O Module - 4 Port 10/100 Fast Ethernet	NS-ISG-FE4
I/O Module - 8 Port 10/100 Fast Ethernet	NS-ISG-FE8
I/O Module - Dual Port 10/100/1000 Gig Ethernet	NS-ISG-TX2
ISG 2000 and ISG 1000 Software Options	
VSYS Upgrade 0 to 5 (ISG 2000)	NS-ISG-2000-VSYS-5
VSYS Upgrade 5 to 25 (ISG 2000)	NS-ISG-2000-VSYS-25
VSYS Upgrade 25 to 50 (ISG 2000)	NS-ISG-2000-VSYS-50
VSYS Upgrade 0 to 25 (ISG 2000)	NS-ISG-2000-VSYS-025
VSYS Upgrade 0 to 50 (ISG 2000)	NS-ISG-2000-VSYS-050
VSYS Upgrade 0 to 5 (ISG 1000)	NS-ISG-1000-VSYS-5
VSYS Upgrade 5 to 10 (ISG 1000)	NS-ISG-1000-VSYS-10
ISG 2000 and ISG 1000 Spares	
SX transceiver (mini-GBIC)	NS-SYS-GBIC-MSX
LX transceiver (mini-GBIC)	NS-SYS-GBIC-MLX
ISG 2000 AC power supply	NS-ISG-2000-PWR-AC2
ISG 2000 DC power supply	NS-ISG-2000-PWR-DC2
ISG 1000 AC power supply	NS-ISG-1000-PWR-AC
ISG 1000 DC power supply	NS-ISG-1000-PWR-DC
Fan module	NS-ISG-FAN
Rack Mount Kit (19 in., all mounting hardware)	NS-ISG-2000-RCK-01
Rack Mount Kit (23 in., all mounting hardware)	NS-ISG-2000-RCK-02
Blank Interface Panel	NS-ISG-IPAN2
ISG 2000 Blank Power Supply Cover	NS-ISG-2000-PPAN2

Every Virtual System includes 1 additional virtual router and 2 additional security zones, usable in the virtual or root system.

For More Information: **http://www.juniper.net/products/integrated/dsheet/110035.pdf**

Juniper Networks Quick Reference Guide
Firewall / IPSec VPN Products 39
Firewall / IPSec VPN Products

Juniper Networks NetScreen-5200 / NetScreen-5400

The Juniper NetScreen-5000 Series are purpose built, high-performance security systems. Designed to deliver a new level of high-peformance capabilities with integrated firewall, DoS and DDoS protection, VPN, and traffic management functionality. Built around Juniper's third generation security ASIC and distributed system architecture, the NetScreen-5000 Series offers excellent scalability and flexibility while providing high levels of security through Juniper Networks custom operating system, NetScreen ScreenOS. Both products employ a switch fabric for data exchange and separate multi-bus channel for control information, delivering scalable performance for the most demanding environments.

NetScreen-5200 is a 2-slot modular chassis.	NetScreen-5400 is a 4 slot modular chassis.

When to Sell

- For large enterprise, carrier, and data center networks
- When multi-gigabit performance for both firewall and VPN is required
- High availability for resiliency and virtual systems for departmental firewalls required

Competitive Products

Cisco PIX 535-UR/R; Check Point on Nokia IP1220, IP1260, IP2250; Fortinet FG3000, FG3600, FG4000; SonicWall PRO5060, and WatchGuard V200

Selected Part Numbers and Ordering Information

PRODUCT		PART NUMBER
Juniper Networks NetScreen-5200 bundles		
NetScreen-5200	1 2G24FE SPM, 0 VSYS, AC	NS-5200-P00A-S00
NetScreen-5200	1 2G24FE SPM, 0 VSYS, DC	NS-5200-P00D-S00
NetScreen-5200	1 8G SPM, 0 VSYS, AC	NS-5200-P01A-S00
NetScreen-5200	1 8G SPM, 0 VSYS, DC	NS-5200-P01D-S00
NetScreen-5200	1 8G SPM, 100 VSYS, AC	NS-5200-P01A-S01
NetScreen-5200	1 8G SPM, 100 VSYS, DC	NS-5200-P01D-S01
NetScreen-5200	1 8G SPM, 500 VSYS, AC	NS-5200-P01A-S02
NetScreen-5200	1 8G SPM, 500 VSYS, DC	NS-5200-P01D-S02
Juniper Networks NetScreen-5200 bundles with Management 2		
NetScreen-5200	5200, 2G24FE, AC, no VSYS, MGT2	NS-5200-P10A-S00
NetScreen-5200	5200, 2G24FE, DC, no VSYS, MGT2	NS-5200-P10D-S00
NetScreen-5200	5200, 8G, AC, no VSYS, MGT2	NS-5200-P11A-S00
NetScreen-5200	5200, 8G, DC, no VSYS, MGT2	NS-5200-P11A-S00

PRODUCT		PART NUMBER
Juniper Networks NetScreen-5400 bundles		
NetScreen-5400	1 2G24FE SPM, 0 VSYS, AC	NS-5400-P00A-S00
NetScreen-5400	1 2G24FE SPM, 0 VSYS, DC	NS-5400-P00D-S00
NetScreen-5400	1 8G SPM, 0 VSYS, AC	NS-5400-P01A-S00
NetScreen-5400	1 8G SPM, 0 VSYS, DC	NS-5400-P01D-S00
NetScreen-5400	1 8G SPM, 100 VSYS, AC	NS-5400-P01A-S01
NetScreen-5400	1 8G SPM, 100 VSYS, DC	NS-5400-P01D-S01
NetScreen-5400	1 8G SPM, 500 VSYS, AC	NS-5400-P01A-S02
NetScreen-5400	1 8G SPM, 500 VSYS, DC	NS-5400-P01D-S02
Juniper Networks NetScreen-5400 bundles with Management 2		
NetScreen-5400	5400, 2G24FE, AC, no VSYS, MGT2	NS-5400-P10A-S00
NetScreen-5400	5400, 2G24FE, DC, no VSYS, MGT2	NS-5400-P10D-S00
NetScreen-5400	5400, 8G, AC, no VSYS, MGT	NS-5400-P11A-S00
NetScreen-5400	5400, 8G, DC, no VSYS, MGT2	NS-5400-P11D-S00
Juniper Networks NetScreen-5000 Virtual System Upgrades		
NetScreen-5000	VSYS Upgrade 0 to 5	NS-5000-VSYS-5
NetScreen-5000	VSYS Upgrade 5 to 25	NS-5000-VSYS-25
NetScreen-5000	VSYS Upgrade 25 to 50	NS-5000-VSYS-50
NetScreen-5000	VSYS Upgrade 50 to 100	NS-5000-VSYS-100
NetScreen-5000	VSYS Upgrade 100 to 250	NS-5000-VSYS-250
NetScreen-5000	VSYS Upgrade 250 to 500	NS-5000-VSYS-500
NetScreen-5000	VSYS Upgrade 0 to 500	NS-5000-VSYS
Juniper Networks NetScreen-5000 Components		
Management Module		NS-5000-MGT
Management Module 2		NS-5000-MGT2
8G (8 mini-GBIC) Secure Port Module		NS-5000-8G
2G24FE (2 mini-GBIC24 10/100) Secure Port Module		NS-5000-2G24FE
mini-GBIC transceiver - SX		NS-SYS-GBIC-MSX
mini-GBIC transceiver - LX		NS-SYS-GBIC-MLX
Juniper Networks NetScreen-5200 Components		
NetScreen-5200	Chassis	NS-5200-CHA
NetScreen-5200	AC Power Supply	NS-5200-PWR-AC
NetScreen-5200	DC Power Supply	NS-5200-PWR-DC
NetScreen-5200	Fan Assembly	NS-5200-FAN
Juniper Networks NetScreen-5400 Components		
NetScreen-5400	Chassis	NS-5400-CHA
NetScreen-5400	AC Power Supply	NS-5400-PWR-AC
NetScreen-5400	DC Power Supply	NS-5400-PWR-DC
NetScreen-5400	Fan Assembly	NS-5400-FAN

For More Information:
http://www.juniper.net/products/integrated/dsheet/110007.pdf

Juniper Networks NetScreen-Remote VPN & NetScreen-Remote Security Client

Juniper Networks enables enterprises to quickly and securely connect their remote users to the corporate resources they need to be productive. With the number of remote users enterprises potentially have to secure, they can't afford to have a solution that is difficult to deploy and configure. Understanding this, Juniper Networks has created a solution that is very easy to deploy and maintain. Enterprises can use the Juniper Networks NetScreen-Remote VPN client for VPN functionality or combine VPN and personal firewall functionality with the Juniper Networks NetScreen-Remote Security Client to ensure the information remains private and the network secure against unauthorized users.

Key Features & Benefits

- Interoperable with IPSec compliant communication devices
- Support for the highest levels of encryption and authentication algorithms
- Integrated with personal firewall for stronger security

When to Sell

- Customer requests an IPSec remote access solution

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
NetScreen-Remote Security Client – 10 User License	NS-R8P-010
NetScreen-Remote Security Client – 100 User License	NS-R8P-100
NetScreen-Remote Security Client – 1,000 User License	NS-R8P-110
NetScreen-Remote VPN Client – 10 User License	NS-R8A-010
NetScreen-Remote VPN Client – 100 User License	NS-R8A-100
NetScreen-Remote VPN Client – 1,000 User License	NS-R8A-110

For More Information:
http://www.juniper.net/products/integrated/dsheet/110012.pdf

SSL VPN

Juniper Networks SSL VPNs lead the market with a complete range of products, tailored to meet the needs for companies of all sizes. Juniper Networks SSL VPNs are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks SSL VPN appliances combine the overall benefit of a lower total cost of ownership compared to traditional IPSec client solutions, with unique end-to-end security features.

Juniper Networks SSL VPN Appliance Line

CUSTOMER NETWORK	PRODUCTS TO RECOMMEND	ENTERPRISE CLASS FEATURES
Small to mid-sized companies	Juniper Networks Secure Access 700	• Secure access for remote/mobile employees, with no client software • Plug-n-play deployment • Robust security features
Small to mid-sized enterprises	Juniper Networks Secure Access 2000	• Secure LAN, intranet and extranet access for employees, business partners and customers • Dynamic access privilege management, with 3 access methods • Simplified administration available via Central Manager
Mid-sized to large enterprises	Juniper Networks Secure Access 4000	• Scalable platform enables medium to large enterprises to offer secure extranet, intranet and LAN access from one platform. • Enterprise performance/high availability • Dynamic access privilege management, with 3 access methods • Simplified administration available via Central Manager
Large and multinational enterprises	Juniper Networks Secure Access 6000	• High performance platform for the largest and most complex secure extranet, intranet and LAN access deployments • Hardware-based SSL acceleration and HTTP compression • Dynamic access privilege management with 3 access methods • Simplified administration available via Central Manager

Note: FIPS compliant platforms are also available.

License Options

The Juniper Networks SA 2000, SA 4000 and SA 6000 are available either Advanced or Baseline licensing options to support different levels of deployment requirements. The Advanced feature set provides additional sophisticated capabilities including Secure Access Central Manager, as listed with the product datasheet http://www.juniper.net/products/ssl/management.html.

The Baseline feature set provides an entry-level solution for customer environments where features, such as client software, server changes, DMZ build-outs or software agent deployments are not critical requirements.

Juniper Networks Secure Access 700

The Juniper Networks Secure Access 700 SSL VPN appliance provides small to medium enterprises a secure, cost-effective way to deploy instant remote access to the corporate network using just a web browser. This architecture eliminates the high cost of installing, configuring and maintaining client software on every device. SSL delivery also eliminates the network interoperability issues encountered with traditional remote access products, allowing remote users reliable and ubiquitous access from external networks. The SA 700 comes with Juniper's Network Connect access method, which creates a secure network-layer connection via a lightweight, dynamic download. The SA 700 can also be upgraded to include Juniper's Core Clientless access method, which enables connections from any PC anywhere to Web-enabled applications. Built on Juniper's market-leading SSL VPN platform, the SA 700 delivers enterprise-strength AAA (authentication, authorization, auditing), comprehensive endpoint defense and a core security architecture that has been thoroughly audited by third parties.

Key Features & Benefits

- Designed for small to mid-sized companies to provide instant secure access to remote or mobile employees
- Lower Total Cost of Ownership
  - Plug-n-play appliance that installs in minutes with minimal IT knowledge required
  - No client software deployment or maintenance
  - Simple end user and administrator interfaces facilitate quick and easy use
  - No network interoperability issues
- End-to-End Security
  - Complete, secure access to LAN resources, ensuring that the endpoint device, data in transit and internal resources are secure
  - Seamless integration with broad range of authentication methods and protocols

When to Sell

- Small to medium enterprise with between 10 and 25 concurrent users
- No need for business partner or customer access
- Customer looking for a plug-n-play appliance without client software or changes to infrastructure
- Enterprise has limited IT department, budget and rack space
- Need to eliminate NAT or firewall traversal issues
- No need for Secure Meeting or Central Manager functionality

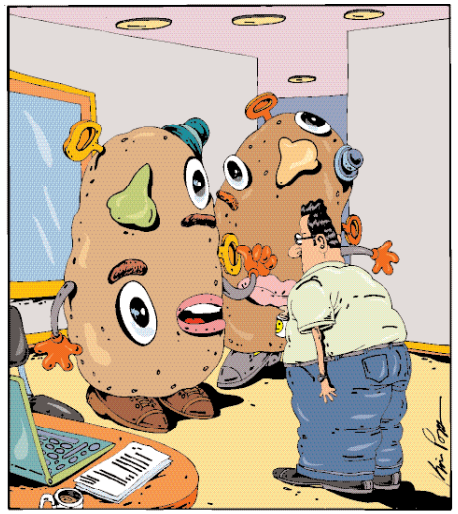
Competitive Products

Aventail EX-750, Cisco ASA 5510, Cisco VPN Concentrator 3005, F5 FirePass 1000, Net6 (Citrix) HV 2000, Nokia IP 130

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
Secure Access 700 Base System	SA700
Secure Access 700 for 10 simultaneous users	SA700-ADD-10U
Secure Access 700 for 15 simultaneous users	SA700-ADD-15U
Secure Access 700 for 25 simultaneous users	SA700-ADD-25U
Core Clientless Web Access	SA700-CORE
Secure Access Accessories	
Secure Access Rack Mount Kit – 1U	SA-ACC-RCKMT-KIT-1U
Secure Access Rack Mount Kit – 2U	SA-ACC-RCKMT-KIT-2U
Secure Access AC Power Cord UK	SA-ACC-PWR-AC-UK
Secure Access AC Power Cord Europe	SA-ACC-PWR-AC-EUR

For More Information: **http://www.juniper.net/products/ssl/dsheet/100124.pdf**



"Things have to change around here Larry—this network's turning Phil and me into nervous wrecks."

Juniper Networks Secure Access 2000

The Juniper Networks Secure Access 2000 SSL VPN enables small-to-medium-sized companies to deploy cost effective remote and extranet access, as well as intranet security. Users can access the corporate network and applications from any standard Web browser. The SA 2000 uses SSL, the security protocol found in all standard Web browsers, as a secure access transport mechanism. The use of SSL eliminates the need for client software deployment, changes to internal servers and costly ongoing maintenance. Juniper's Secure Access appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups with no infrastructure changes, no DMZ deployments and no software agents. This functionality also allows companies to secure access to the corporate intranet, so that administrators can restrict access to different employee, contractor or visitor populations, based on the resources that they need.

The SA 2000 comes with the streamlined feature set that an enterprise would need to deploy secure remote access, as well as a basic customer/ partner extranet or secure intranet. The Advanced license enables additional sophisticated features that meet the needs of more complex deployments with diverse audiences and use cases, as well as Central Manager.

Key Features & Benefits

- Lower Total Cost of Ownership
  - Secure remote access with no client software deployments or changes to servers and virtually no ongoing maintenance
  - Secure extranet access with no DMZ buildout, server hardening resource duplication, or incremental deployments to add applications or users
- End-to-End Security
  - Numerous security options from the end-user device to the application data and servers
  - Juniper's Endpoint Defense Initiative includes native functionality, as well as client- and server-side APIs for effective enforcement and unified administration of best-of-breed endpoint security
- Rich Access Privilege Management Capabilities
  - Dynamic, controlled access at the URL, file, application and server level, based on a variety of session-specific variables including identity, device, security control and network trust level
- Provision by Purpose
  - Three different access methods allow administrators to balance security and access on a per-user, per-session basis
- High Availability
  - Cluster pair deployment option for high availability across the LAN and the WAN
- Streamlined Manageability
  - Central management option for unified administration
  - User self service features enhance productivity while lowering administrative overhead

When to Sell

- For small to medium enterprises with between 25 and 100 concurrent users
- Seeking secure remote access for employees, as well as business partners and/or customers
- Need for granular access controls at the file, URL, application and server levels
- Require cluster pair deployment for high availability
- Need for Central Manager functionality

Competitive Products

Aventail EX-1500, Cisco ASA 5510, Cisco VPN 3000, F5 FirePass, NetScaler (Citrix) Secure Remote Access

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
Secure Access 2000 Base System	SA2000
Secure Access 2000 User Licenses	
Secure Access 2000 for an additional 25 Simultaneous Users	SA2000-ADD-25U
Secure Access 2000 for an additional 50 Simultaneous Users	SA2000-ADD-50U
Secure Access 2000 for an additional 100 Simultaneous Users	SA2000-ADD-100U
Secure Access 2000 Feature Licenses	
Secure Application Manager and Network Connect	SA2000-SAMNC
Advanced for SA 2000	SA2000-ADV
Secure Meeting for SA 2000	SA2000-MTG
Secure Access 2000 Clustering Licenses	
Clustering: Allow 25 additional Users	SA2000-CL-25U
Clustering: Allow 50 additional Users	SA2000-CL-50U
Clustering: Allow 100 additional Users	SA2000-CL-100U
Secure Access 2000 Lab Unit Licenses	
Lab Unit License: 10 simultaneous users/ all features	SA2000-LAB
Lab Unit License: Clustering	SA2000-LAB-CL
Secure Access Accessories	
Secure Access Rack Mount Kit – 1U	SA-ACC-RCKMT-KIT-1U
Secure Access Rack Mount Kit – 2U	SA-ACC-RCKMT-KIT-2U
Secure Access AC Power Cord UK	SA-ACC-PWR-AC-UK
Secure Access AC Power Cord Europe	SA-ACC-PWR-AC-EUR

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

For More Information:
http://www.juniper.net/products/ssl/dsheet/100126.pdf

Juniper Networks Secure Access 4000

The Juniper Networks SA 4000 SSL VPNs enable mid-to-large-sized organizations to provide cost effective remote and partner extranet access from any standard Web browser. Based on the award-winning Instant Virtual Extranet (IVE) platform, the SA 4000 appliances feature rich access privilege management functionality that can be used to create secure customer/partner extranets with no infrastructure changes, no DMZ deployments and no software agents. This functionality also allows the enterprise to secure access to the corporate intranet, so that different employee and visitor populations can utilize exactly the resources they need while adhering to enterprise security policies. Built-in compression for all traffic types speeds performance, and SSL acceleration is available via a software license for more demanding environments.

The SA 4000 comes with the streamlined feature set that an enterprise would need to deploy secure remote access, as well as a basic customer/partner extranet or secure intranet. The Advanced license enables additional sophisticated features that meet the needs of more complex deployments with diverse audiences and use cases, as well as Central Manager.

Key Features & Benefits

- Rich Access Privilege Management Capabilities
  - Dynamic, controlled access at the URL, file, application and server level, based on a variety of session-specific variables including identity, device, security control and network trust level
- Provision by Purpose
  - Three different access methods allow administrators to balance security and access on a per-user, per-session basis
- End-to-End Layered Security
  - Numerous security options from the end user device, to the application data and servers
  - Juniper's Endpoint Defense Initiative includes native functionality as well as client- and server-side APIs for effective enforcement and unified administration of best-of-breed endpoint security
- High Availability
  - Cluster pair deployment option for high availability across the LAN and the WAN
- Lower Total Cost of Ownership
  - Secure remote access with no client software deployments or changes to servers and virtually no ongoing maintenance
  - Secure extranet access with no DMZ buildout, server hardening resource duplication, or incremental deployments to add applications or users
- Streamlined Manageability
  - Central management option for unified administration
  - User self service features enhance productivity while lowering administrative overhead

When to Sell

- For medium to large enterprises with between 50 and 1000 concurrent users
- Seeking secure remote access for employees, as well as business partners and/or customers
- Need for granular access controls at the file, URL, application and server levels
- Require cluster pair deployment for high availability
- Need for Central Manager functionality

Competitive Products

Aventail EX-1500, Cisco ASA 5510, Cisco VPN 3000, F5 FirePass, NetScaler (Citrix) Secure Remote Access

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
Secure Access 4000 Base System	SA4000
Secure Access 4000 User Licenses	
Secure Access 4000 for an additional 50 Simultaneous Users	SA4000-ADD-50U
Secure Access 4000 for an additional 100 Simultaneous Users	SA4000-ADD-100U
Secure Access 4000 for an additional 250 Simultaneous Users	SA4000-ADD-250U
Secure Access 4000 for an additional 500 Simultaneous Users	SA4000-ADD-500U
Secure Access 4000 for an additional 1000 Simultaneous Users	SA4000-ADD-1000U
Secure Access 4000 Feature Licenses	
Secure Application Manager and Network Connect	SA4000-SAMNC
Advanced for SA 4000	SA4000-ADV
Secure Meeting	SA4000-MTG
SSL Acceleration License	SA4000-SSL
Instant Virtual Systems	SA4000-IVS
Secure Access 4000 Clustering Licenses	
Clustering: Allow 50 additional Users	SA4000-CL-50U
Clustering: Allow 100 additional Users	SA4000-CL-100U
Clustering: Allow 250 additional Users	SA4000-CL-250U
Clustering: Allow 500 additional Users	SA4000-CL-500U
Clustering: Allow 1000 additional Users	SA4000-CL-1000U
Secure Access 4000 Lab Unit Licenses	
Lab Unit License: 10 simultaneous users/ all features	SA4000-LAB
Lab Unit License: Clustering	SA4000-LAB-CL
Secure Access Accessories	
Secure Access Rack Mount Kit - 1U	SA-ACC-RCKMT-KIT-1U
Secure Access Rack Mount Kit - 2U	SA-ACC-RCKMT-KIT-2U
Secure Access AC Power Cord UK	SA-ACC-PWR-AC-UK
Secure Access AC Power Cord Europe	SA-ACC-PWR-AC-EUR

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

For More Information:
http://www.juniper.net/products/ssl/dsheet/100125.pdf

Juniper Networks Secure Access 6000

The Juniper Networks Secure Access 6000 SSL VPN is designed for medium to large enterprises, and features best-in-class performance, scalability and redundancy for organizations with high volume secure access and authorization requirements. The SA 6000 hardware platform is designed to scale to the largest enterprise deployments and optimize application delivery, with available options that include redundant hot swappable hard disks, power supplies and fans, as well as GBIC-based multiple Ethernet ports for the creation of separate physical networks and redundant or meshed configurations. The SA 6000 also features a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes, as well as built in compression for all traffic.

Like all products built on the Instant Virtual Extranet (IVE) platform, the SA 6000 uses Secure Socket Layer (SSL) available in all Web browsers as a means of secure transport. This enables the enterprise to provide remote access to mobile employees and contractors without deploying client software, as well secure extranet or intranet access with no DMZ buildout, server hardening, Web agent deployments or ongoing maintenance.

The Secure Access 6000 comes with the streamlined feature set that an enterprise would need to deploy secure remote access, as well as a basic customer/partner extranet or secure intranet. The Advanced license enables additional sophisticated features that meet the needs of more complex deployments with diverse audiences and use cases, as well as Central Manager.

Key Features & Benefits

- Rich Access Privilege Management Capabilities
  - Dynamic, controlled access at the URL, file, application and server level, based on a variety of session-specific variables including identity, device, security control and network trust level
- Provision by Purpose
  - Three different access methods allow administrators to balance security and access on a per-user, per-session basis
- End-to-End Layered Security
  - Numerous security options from the end user device, to the application data and servers
  - Juniper's Endpoint Defense Initiative includes native functionality as well as client- and server-side APIs for effective enforcement and unified administration of best-of-breed endpoint security
- Performance Scalability
  - A variety of hardware-based performance enhancing features, including SSL acceleration and clustering, provide optimal scalability
- High Availability
  - Cluster pair deployment option, for high availability across the LAN and the WAN
- Streamlined Manageability
  - Central management option for unified administration
  - User self service features enhance productivity while lowering administrative overhead
- Lower Total Cost of Ownership
  - Secure remote access with no client software deployments or changes to servers and virtually no ongoing maintenance
  - Secure extranet access with no DMZ buildout, server hardening resource duplication or incremental deployments to add applications or users

When to Sell

- For large and multinational enterprises with between 100 and 2,500 concurrent users in a single appliance and thousands of users across the enterprise serviced with clustering capabilities
- Seeking secure remote access for employees, as well as business partners and/or customers
- Need for remote access controls at the file, URL, application and server levels
- Where multi-unit clustering is a requirement for scalability of secure LAN, WAN, intranet and extranet access
- Need for Central Manager functionality

Competitive Products

Aventail EX-1500, Cisco ASA 5510, Cisco VPN 3000, F5 FirePass, NetScaler (Citrix) Secure Remote Access

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
Secure Access 6000 Base System	SA6000
Secure Access 6000 User Licenses	
Secure Access 6000 for an additional 100 Simultaneous Users	SA6000-ADD-100U
Secure Access 6000 for an additional 250 Simultaneous Users	SA6000-ADD-250U
Secure Access 6000 for an additional 500 Simultaneous Users	SA6000-ADD-500U
Secure Access 6000 for an additional 1000 Simultaneous Users	SA6000-ADD-1000U
Secure Access 6000 for an additional 2500 Simultaneous Users	SA6000-ADD-2500U
Secure Access 6000 for an additional 5000 Simultaneous Users	SA6000-ADD-5000U
Secure Access 6000 Feature Licenses	
Secure Application Manager and Network Connect	SA6000-SAMNC
Advanced for SA 6000	SA6000-ADV
Secure Meeting	SA6000-MTG
Instant Virtual Systems	SA6000-IVS
Secure Access 6000 Clustering Licenses	
Clustering: Allow 100 additional Users	SA6000-CL-100U
Clustering: Allow 250 additional Users	SA6000-CL-250U
Clustering: Allow 500 additional Users	SA6000-CL-500U
Clustering: Allow 1000 additional Users	SA6000-CL-1000U
Clustering: Allow 2500 additional Users	SA6000-CL-2500U
Clustering: Allow 5000 additional Users	SA6000-CL-5000U
Secure Access 6000 Lab Unit Licenses	
Lab Unit License: 10 simultaneous users/all features	SA6000-LAB
Lab Unit License: Clustering	SA6000-LAB-CL
Secure Access Accessories	
Field Upgradeable Secondary Power Supply	SA6000-PS
Field Upgradeable Secondary Hard Disk	SA6000-HD
Field Upgradeable (by Authorized VAR only) Additional 2 GB Memory	SA6000-MEM
Field Upgradeable Fan	SA6000-FAN
Secure Access Rack Mount Kit – 1U	SA-ACC-RCKMT-KIT-1U
Secure Access Rack Mount Kit – 2U	SA-ACC-RCKMT-KIT-2U
Secure Access AC Power Cord UK	SA-ACC-PWR-AC-UK
Secure Access AC Power Cord Europe	SA-ACC-PWR-AC-EUR

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

For More Information: **http://www.juniper.net/products/ssl/dsheet/100127.pdf**

Intrusion Detection and Prevention (IDP)

The Juniper Networks Intrusion Detection and Prevention products (Juniper Networks IDP) integrate application and network visibility with incident investigation and remediation to help customers quickly and confidently deploy inline attack prevention. When deployed inline, Juniper Networks IDP effectively identifies and stops network and application level attacks before they inflict any damages, minimizing the time and costs associated with intrusions.

The Juniper Networks IDP product line includes the IDP 50, IDP 200, IDP 600 and the IDP 1100. All of the products contain the full IDP features and are managed using the same management interface.

Key Features & Benefits

- Stops worms, Trojans, Spyware, keyloggers, and other malware from penetrating the network and spreading via multi-method detection system that includes stateful signatures, protocol anomalies and backdoor detection
- Extensive signature customization to improve the ability to detect unique attacks and tailor the signature specific to the customer's requirements
- Closed loop investigation process to quickly see the big picture and then drill down to the appropriate level of detail to make informed security decisions
- Enterprise Security Profiler to gain insight into network and attack activity that accelerates inline deployment and facilitates attack investigation
- Policy Editor to create and deploy granular security policies based on what traffic to look at, what attacks to look for in that traffic, and how to respond when an attack has been detected
- Log Viewer to investigate specific security incidents with the ability to customize the way information is processed within the system
- Centralized rule-based management approach to simplify deployment, configuration and maintenance
- Fully customizable reporting to generate up to the minute status on network activity
- IDP clustering to enable stateful, standalone high availability minimizing the risk of a single point of failure and maximizing network protection

When to Sell

- The IDP family is an ideal solution for customers that:
  - — Want true inline application level attack prevention that is easy to manage
  - — Need comprehensive attack coverage of current and emerging attacks such as Spyware and malware
  - — Are under-staffed and need the ability to monitor network changes and rapidly make necessary changes
- IDP 50: For environments with low bandwidth requirements
- IDP 200: For medium sized central sites and/or large branch office environments
- IDP 600C/600F: For larger central sites and/or large branch office environments
- IDP 1100C/1100F: For large central sites and data center environments

Competitive Products

Enterasys Dragon, Intruvert, ISS Proventia, NFR, Sourcefire, Tipping Point UnityOne

Product Specs At-A-Glance

	IDP 50	IDP 200	IDP 600C/F	IDP 1100C/F
Maximum Throughput	Up to 50 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
Maximum Number of Sessions	10,000	70,000	220,000	500,000
Operational Modes	Passive sniffer, inline bridge, inline Proxy-ARP, and inline router			
Detection Mechanisms	8 including Stateful Signatures and backdoor detection			
Signature Updates	Yes: signature updates provided daily, as well as in emergency			
Interfaces				
Traffic Ports	2 10/100/1000	8 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit + 2 10/100/1000	10 10/100/1000 or 8 FiberSX Gigabit + 2 10/100/1000
Management	1 10/100/1000	1 10/100/1000	1 10/100/1000	1 10/100/1000
HA	N/A	1 10/100/1000	1 10/100/1000	1 10/100/1000
Physical Redundancy				
Redundant Power	No	Optional	Yes	Yes
RAID	No	No	Yes	Yes
High Availability Support	Fail-Open	Stand alone fail-over, load sharing, HA clustering and 3rd party fail-over*		

*Integrated Bypass for all 10/100/1000 traffic ports. The fiber gigabit interfaces require 3rd party Bypass unit which is purchased separately.

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
IDP 50 Intrusion Detection and Prevention Appliance	NS-IDP-50
IDP 200 Intrusion Detection and Prevention Appliance	NS-IDP-200
IDP 600C Intrusion Detection and Prevention Appliance	NS-IDP-600C
IDP 600F Intrusion Detection and Prevention Appliance	NS-IDP-600F
IDP 1100C Intrusion Detection and Prevention Appliance	NS-IDP-1100C
IDP 1100F Intrusion Detection and Prevention Appliance	NS-IDP-1100F
Accessories/Spares	
IDP AC Power Supply (IDP 200, 600 and 1100 only)	NS-IDP-PWR-AC-003
IDP Rail Kit	NS-IDP-RCK-03
IDP SCSI Hard Drive (IDP 600 and 1100 only)	NS-IDP-HD-003

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

For More Information:
http://www.juniper.net/products/intrusion/

Application Acceleration Platforms

The Juniper Networks application acceleration platforms provide secure and assured application delivery by improving the performance of client-server and web-enabled business applications for central sites, branch offices, and remote users. The platforms play a critical role in today's extended enterprise by delivering LAN-like performance to users around the globe who access centralized applications.

There are two families of application acceleration platforms.

- The DX platforms reside in the data center in front of web and application servers, where they act as data-center accelerators to offload application servers from administrative tasks, freeing the devices to concentrate on serving application data quickly
- The WX/WXC application acceleration platforms optimize WAN resources to improve the performance of mission-critical applications over the WAN as well as to facilitate application rollouts, data center and server consolidation, disaster recovery and back-up, and regulatory compliance

Key Features & Benefits

- The DX and WX/WXC platforms help organizations achieve tremendous productivity gains across the full range of TCP- and web-based business applications by eliminating the performance restrictions of the data center and wide-area network within the extended enterprise
- The DX and WX/WXC application acceleration platforms reduce capital expenses by enabling data center consolidation, reducing the amount of servers, application licenses, and WAN communications services required to support the enterprise
- The DX and WX/WXC application acceleration platforms reduce operational expenses by simplifying server administration and backup, enhancing existing WAN services, and significantly reducing support requirements for branch offices
- The WX Central Management System (CMS) software provides detailed visibility into the WAN and the performance of centralized applications being accessed by users in branch offices
- Dramatically enhance the performance of web-based applications by offloading services, freeing servers to focus on providing content and improving response times for headquarters, branch-office and remote users
- Facilitate new application deployments by making more efficient use of existing WAN and data center resources, avoiding the need to invest in additional infrastructure to maintain performance levels for remote and branch-office users
- Support server centralization and data center consolidation initiatives by accelerating application performance over the WAN, enabling users throughout the extended enterprise – including remote and branch offices – to access centralized applications at LAN speeds
- Enhance disaster recovery and data replication efforts by enabling more frequent and efficient backups to be performed around the clock over the WAN without impacting user access or productivity
- Facilitate compliance with Federal regulations such as Sarbanes-Oxley by allowing easy and reliable backups of critical data such as e-mail and financial records

DX Application Acceleration Platforms

Juniper Networks DX application acceleration platforms offload security, encryption, compression, and connection and session management functions from web and application servers, accelerating the performance of web-based applications for headquarters, branch-office, remote, and mobile users. The DX platforms also simplify data center architectures by incorporating SSL encryption, application firewall, accounting/authentication/authorization, auto-adaptive compression, TCP offload, bi-directional HTTP rewrite, caching, and server load balancing (SLB) capabilities in a single device, eliminating the need for multiple point products.

The DX application acceleration platforms are based on the DX Framework, which provides a blueprint for building the ideal application front-end solution. The DX Framework integrates specific security, acceleration, availability, and visibility and control features that distinguish the DX platform. By incorporating this critical functionality and providing unprecedented web performance and application availability in an easy-to-manage, flexible appliance, the DX application acceleration platform is the cornerstone of the new data center.

Key Features & Benefits

- Offers wide range of functionality – load balancing, compression, SSL, TCP offload, HTML rewrite, accounting/authentication/authorization, application firewall – and supports client IP transparency to simplify configuration and installation
- Multiplexing engine offloads servers, reducing connections by a ratio of up to 1,000:1
- HTTP-aware compression automatically detects which standard (GZIP, deflate, etc.) browsers support for best possible performance
- Compresses all HTML, SHTML, DHTML, JHTML, PHTML, Javascript, J2EE, JSP, CSS stylesheets, XML, SOAP
- Compresses all Microsoft Office documents
- Optional 3G Caching improves server performance and scalability by serving straight from internal, memory-resident cache
- LDAP and RADIUS Authentication Caching caches successful login attempts to reduce load on the authentication server, dramatically improving performance of authentication and authorization
- AutoSSL™ feature rewrites HTML “on the fly” to secure content without modifying the application
- Bi-directional HTTP rewrite delivers better performance and greater security without having to change the application
- Scriptable server health checks provide application-level verification
- Global Server Load Balancing (GSLB) allows load-balancing between multiple distributed data centers, not just servers in a single data center, for disaster recovery purposes
- Defends against SYN flood and denial of service (DoS) attacks
- Protocol scrubbing (HTTP and TCP) prevents passing packet fragments and ensures only valid, well-formed HTTP/S requests reach servers
- Native HTTP protocol communication dynamically inspects, verifies, and re-writes client requests or server responses

- Transaction assurance detects transaction errors by incorrect content within the page itself or error code
- SLA monitoring and analysis tracks, monitors, and logs server response time and client download time for each HTTP/S request and response
- ActiveN feature supports self-healing mesh of up to 64 DX platforms actively processing traffic to one or more VIPS with cascading failover and linear scaling up to 64 Gbps
- Supports full Layer 4 server load balancing of HTTP, HTTPS (SSL), FTP, and most TCP and UDP protocols; and full Layer 7 load balancing based on any request method, protocol version, URL, cookie, other header, POST data, header or body content, SOAP, or XML contents
- Monitors and records more than 200 real-time statistics by second, minute, hour, day, month, year
- Browser-based administrative interface (HTTP, HTTPS) enables simplified configuration and management

When to Sell

- Businesses using the web-enabled interface of packaged business applications (PeopleSoft, SAP, Oracle, JD Edwards, Siebel, Microsoft SharePoint, OWA or custom tools)
- Businesses with multiple TCP application servers that need to be load-balanced for redundancy and high-availability
- Companies reliant on the Internet to support business operations
- Environments that need to support a growing user base without investing in additional data center resources such as web and application servers or appliance point products
- Web-based businesses that depend on quality user experiences to drive revenue

Competitive Products

F5 - 1500 IP/3400 IP/6400 IP Application Switch and TrafficShield, **Cisco (FineGround)** - 11000 & 11500 Series, Global Site Selector 4480 and FineGround Velocity, **Citrix (NetScaler)** - Request Switch 9000 iON Series Secure Application Gateway/Switch, **Radware** - Web Server Director, CertainT 100 and Cache Server Director, **Array Networks** - Netcontinuum NC-1000 and **Teros** - Web Application Firewall

Product Specs At-A-Glance

	DX 3200	DX 3250	DX 3600	DX 3650	DX 3650-FIPS	DX 3670
Application Clusters (VIPs) Supported	64	64	128	128	128	128
Servers per Application Cluster	32	32	64	64	64	64
SSL Transactions per Second	3,000	5,000	5,000	9,000	5,000	18,000
New SSL Connections per Second	250	800	500	1,600	500 (FIPS card specification)	11,000
Simultaneous Connections	50,000	50,000	50,000	500,0000	500,0000	500,0000
FIPS 140-2 Level 3 Certified	No	No	No	No	Yes	No
Network Interface Options	100TX (x2)	100TX (x2)	a) GbE-TX (x4) b) GbE-TX (2x) and GigE Fiber (x2)	a) GbE-TX (4x) b) GbE-TX (2x) and GigE Fiber (x2)	GbE-TX (2x)	1GbE-TX (2x)
Form Factor	1U	1U	2U	2U	2U	2U

Selected Part Numbers and Ordering Information

PRODUCT	PRODUCT PLATFORM	PART NUMBER
Data Center Acceleration Baseline Products		
Entry-level AFE w/ 10/100 copper interfaces	DX-3200	DX-3200-N-2C
AFE w/ high-speed SSL and 10/100 copper interfaces	DX-3250	DX-3250-S-2C
AFE w/ 1Gb copper interfaces, dual PS	DX-3600	DX-3600-N-4G
AFE w/ 1Gb copper and fiber interfaces, dual PS	DX-3600	DX-3600-N-2G2F
FIPS Level 3 certified AFE w/ high-speed SSL, 1Gb interfaces, dual PS	DX-3650	DX-3650-F-2G
AFE w/ high-speed SSL, 1Gb copper interfaces, dual PS	DX-3650	DX-3650-S-4G
AFE w/ high-speed SSL, 1Gb fiber and copper interfaces, dual PSModule	DX-3650	DX-3650-S-2G2F
AFE w/ ultra high-speed SSL, 1GB copper interfaces, dual PS	DX-3670	DX-3670-U-2G
Data Center Acceleration Software Baseline Products		
High-speed 3G RAM-based cache. Requires OverDrive to be purchased	All Platforms	DX-CACHING-LTU
Adaptive Content Processing Module	All Platforms	DX-OVERDRIVE-LTU
Spare		
Single field-replaceable power supply module for 2U units (3670, 3650 FIPS, 3650, 3600)	DX- 3650, DX-3650 FIPS, DX-3600	DX-PWR-S

For More Information: **http://www.juniper.net/products/appaccel/dca/dsheet/100121.pdf**

WX/WXC Application Acceleration Platforms

The Juniper Networks WX and WXC application acceleration platforms help IT speed the performance of business-critical applications over the WAN, resulting in a more LAN-like experience for branch-office users. By accelerating application performance throughout the extended enterprise, the WX and WXC platforms help IT achieve critical business initiatives such as application rollouts, data center consolidation and server centralization, disaster recovery and back-up, and regulatory compliance.

The WX and WXC platforms are based on the unique WX Framework, which provides the foundation for the WAN acceleration and optimization solutions. The WX Framework integrates several interdependent technologies such as next-generation compression and sequence caching, TCP and application-specific acceleration, bandwidth management and path optimization, and visibility technologies into a single platform. In the past, IT needed a variety of discrete point products to deploy these capabilities throughout their WAN. By consolidating these complementary technologies in a single device, the WX and WXC platforms deliver a comprehensive solution that helps IT meet their business goals.

Both the WX and WXC platforms deliver the full value of the integrated WX Framework with the exception of sequence caching, which requires an on-board hard drive. This is the function designated by the "C" in the WXC platforms.

WX Platforms

The market-leading WX application acceleration platforms offer a highly scalable solution for increasing WAN capacity and improving application delivery by eliminating redundant transmissions, accelerating TCP and application-specific protocols, prioritizing and allocating access to bandwidth, and ensuring maximum availability at sites with multiple WAN links. The WX platforms are best known for their pioneering memory-based compression and TCP acceleration capabilities, resulting in a 10-fold increase in WAN capacity and a dramatic improvement in application performance.

The products also feature application-specific acceleration for Microsoft Exchange, Windows file services, and web applications, providing a more LAN-like experience for users accessing these applications over a WAN. The combination of increased bandwidth and faster response times delivers customers a very rapid and quantified return on investment.

The WX product family includes the WX 15, WX 20, WX 50, WX 60, WX 100, and WX Stack. These platforms provide compressed output ranging from 64 Kbps to 155 Mbps and support two to 2,000 remote sites each. Multiple communities of WX platforms can be configured to support an unlimited number of locations. The WX platforms also interoperate with the WXC application acceleration platforms, contributing to a complete, integrated WAN acceleration and optimization solution.

WXC Platforms

The WXC platforms feature all the same capabilities as the WX platform, plus a unique capability called Network Sequence Caching that dramatically speeds the transfer of large files by eliminating the transmission of repetitive data sequences. To enable the sequence caching feature, all WXC platforms include on-board hard drives that supply the memory capacity required to store longer data sequences for longer periods of time. As a result, the WXC platforms can recognize and eliminate very large redundant data patterns seen days or even weeks earlier, reducing WAN traffic levels by as much as 100 fold. The WXC platforms support disk capacity from 40 GB to 3 TB and WAN links from 128 Kbps to 155 Mbps.

The WXC platforms, which interoperate with the WX application acceleration platforms, scale from 128 Kbps to 155 Mbps, with hard-drive capacity from 40 GB to 3 TB. The WXC family includes the WXC 250, the WXC 500 and the WXC Stack, which pairs WXC 500 platforms with a WX 100 platform to extend support for sequence caching to 155 Mbps bandwidth levels.

The WX and WXC platforms make it easy and cost-effective for IT to provide the enterprise-class application delivery needed to support new applications and remote access to centralized resources.

Key Features & Benefits

- WX and WXC platforms are based on the WX operating system (WX OS) software, which enables the integrated technologies of the WX Framework
- Patented Molecular Sequence Reduction™ (MSR™) compression provides up to a 10-fold increase in WAN capacity by recognizing repeated data patterns and replacing them with labels for transmission over the WAN
- Network Sequence Caching technology (WXC only) utilizes hard drives to store Gigabytes of data patterns, enabling the detection and elimination of particularly large patterns separated by days or even weeks
- Packet Flow Acceleration™ (PFA™) technology accelerates performance for the broad range of TCP-based applications by eliminating one round-trip time from connection setup, terminating TCP and using a more efficient transport protocol between WX/WXC devices, and using recovery packets to reconstruct lost transmissions on "lossy" networks
- Application Flow Acceleration™ (AppFlow™) technology provides application-specific acceleration for Layer 7 protocols such as the Messaging Application Programming Interface (MAPI) for Microsoft Exchange, the Common Internet File System (CIFS) for Windows file services, and HTTP for web-based communications
- Quality of Service (QoS) and bandwidth-management tools prioritize mission-critical or time-sensitive application traffic to ensure bandwidth availability
- The Policy-based Multipath™ function enables IT to assign applications to specific paths in locations served by two WAN links; if performance falls below a predetermined threshold, traffic is automatically diverted to the other path to ensure key performance metrics are always met
- Integrated WebView software supports device-level management and configuration
- WX Central Management System (CMS) software works in conjunction with the WX and WXC platforms to provide IT with a systemwide view of application performance over the WAN to quickly identify, diagnose, and resolve problems
- Stack configuration allows a WXC device to serve as a client of the WX 100, extending support for sequence caching to 3 TB of hard-drive capacity and 155 Mbps bandwidth levels

Application Acceleration Platforms

When to Sell

- Businesses experiencing poor application performance over the WAN
- Customers needing to roll-out new application but can't or don't want to invest in WAN infrastructure upgrade
- IT departments with strategic initiatives to centralize servers or consolidate data centers
- Enterprises with large numbers of distributed branch offices
- Companies that need to increase productivity of branch-office workers relying on centralized applications and data
- Businesses needing reliable and robust data replication and back-up resources for disaster recovery and to comply with federal regulations

Competitive Products

Expand - Accelerator, Server Accelerator and HTTPS Accelerator, **Packeteer** - PacketShaper, **Riverbed** - Steelhead 510/1010/2010/3010/5010, **Swan Labs (F5)** - NetCelera Enterprise and App. Shaping Solution, **Cisco (FineGround)** Velocity and Velocity-FS, **Orbital Data** - Orbital 5500, **Tacit** - I-shared Appliance and I-shared Server, **Citrix (NetScaler)** - 9950 Secure Application Switch and **Ipanema** - ip/engine and IP/boss

Product Specs At-A-Glance

WX FAMILY SPECIFICATIONS	WX 15	WX 20	WX 50	WX 60	WX 100	WX STACK
Performance						
Total reduction throughput speed	64 Kbps to 1 Mbps	64 Kbps to 2 Mbps	256 Kbps to 20 Mbps	512 Kbps to 20 Mbps	1 Mbps to 20 Mbps	34 Mbps to 155 Mbps
Connections supported	Up to 2	Up to 15	Up to 120	Up to 150	Up to 320	Up to 2,000
Connections						
Number of network interfaces	Two 10/100 copper ports	Two 10/100 copper ports	Two 10/100 copper ports	Two 10/100/ 1000 copper ports	Two 10/100/ 1000 copper or LC multimode fiber ports	WX Stack includes 1 WX 100 and up to 6 WX clients (excluding WX 15s and WX 20s)
Cluster ports	N/A	N/A	N/A	N/A	Six 10/100/ 1000 copper ports	
Power						
Dual, hot-swappable power supplies	No	No	No	No	Yes	

Product Specs At-A-Glance

WXC FAMILY SPECIFICATIONS	WXC 250	WXC 500	WXC STACK
Performance			
Total reduction throughput speed	128 Kbps to 2 Mbps	512 Kbps to 20 Mbps	34 Mbps to 155 Mbps
Connections supported	Up to 15	Up to 60	Up to 510
Disk capacity	40 GB	500 GB	Up to 3 TB
Connections			
Network interfaces	Two copper 10/100 ports	Two copper 10/100/1000 ports	WXC Stack includes 1 WX 100 and up to 6 WXC 500s

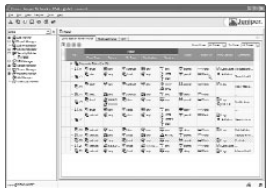
Selected Part Numbers and Ordering Information

PRODUCT	PRODUCT PLATFORM	PART NUMBER
WAN Acceleration Baseline Products		
WX 15, incl. RTU SW License to 64 Kbps	WX 15	WX 15
WX 20, incl. RTU SW License to 64K	WX 20	WX 20
WX 50, incl. RTU SW License to 256K	WX 50	WX 50
WX 60, GigE, incl. RTU SW License to 512K	WX 60	WX 60
WX 100C, incl. RTU SW License to 1 Mbps	WX 100	WX 100C
WX 100F, incl. RTU SW License to 1 Mbps	WX 100	WX 100F
WXC 250, incl. RTU SW License to 128 Kbps	WXC 250	WXC 250
WXC 500, incl. RTU SW License to 512 Kbps	WXC 500	WXC 500
CMS with RTU up to 10 devices	CMS	CM-CM

For More Information: **http://www.juniper.net/products/appaccel/wan**

Application Acceleration Platforms

Juniper Networks NetScreen-Security Manager



Juniper Networks NetScreen-Security Manager takes a new approach to security management by providing IT departments with an easy-to-use solution that controls all aspects of the Juniper Networks firewall / IPSec VPN devices including device configuration, network settings, and security policy. Unlike some solutions that require the use of multiple management tools to control a single device, NetScreen-Security Manager enables IT departments to control the entire device lifecycle with a single, centralized solution.

The NetScreen-Statistical Report Server is the statistical archival and reporting tool for NetScreen-Security Manager. The Statistical Report Server is used to store statistical information from the managed firewall / IPSec VPN devices in the network, and then generate reports from this data enabling further viewing and analysis of the information about a security deployment.

Key Features & Benefits

- Intuitive GUI simplifies complex tasks such as device configuration, policy creation, and VPN deployment
- Delegation of administrative roles provides information access to those who need it
- Object locking allows multiple administrators to safely modify different policies or devices concurrently
- Full High Availability with automatic synchronization and failover
- Device templates to minimize configuration errors by managing any or all aspects of a device or group of devices via a template
- VPN manager to accelerate VPN deployments by creating all the necessary rules after a basic topology has been defined
- Log viewing allows logs stored within the system to be viewed in real time with filters to allow an administrator to perform rapid analysis of security status and events
- Statistical Report Server: Up to 40 different reports in 4 categories cover a full range of data points that can be used for historical analysis to make sound business decisions moving forward
- Statistical Report Server: Report filter can be set up based on specific devices or device groups, or timeframe for a customized viewpoint.

When to Sell

- Customer has a large-scale security deployment to manage
- Wants one central interface for configuration, management and reporting of devices
- Wants to ensure policy enforcement from the corporate headquarters
- Has different administrators that manage different aspects of the company's network security
- Needs to provide reports to different levels within the organization
- Needs to reduce provisioning, configuration and troubleshooting time as well as the associated costs

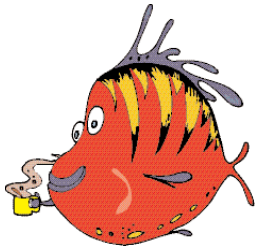
Competitive Products

Check Point SmartCenter and Provider-1, Cisco VPN and Security Management Solution (VMS), Fortinet FortiManager, SonicWALL Global Management System (GMS), WatchGuard System Manager (Firebox III and Firebox X products), WatchGuard Central Policy Manager (vClass products)

Product Specs At-A-Glance

USER INTERFACE	
Operating System Support	Microsoft® Windows® 2000, Windows NT, Windows XP, and Red Hat Linux® 8.0, Red Hat Linux 9.0, Red Hat Enterprise 3.0
Minimum CPU	400 mHz Pentium II or equivalent
Minimum RAM	256 MB RAM, 512 MB recommended
Minimum Available Disk Space	100 MB
Minimum Connectivity to Server	384 kbps (DSL) or LAN
Management Server (GUI Server and Device Server combined)	
Operating System Support	Solaris® 8, Solaris 9, Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise 3.0
Minimum CPU	1 GHz
Minimum RAM	1 GB
Minimum Hard Disk	10K rpm disk with at least 18 GB disk space (logs are estimated to be an average of 100 bytes each)
Minimum NIC	100 Mbs
Maximum devices managed per server	2000*
Juniper Networks Firewall / IPSec VPN Device & Software Support	
Device Support	NetScreen-Hardware Security Client, NetScreen-5XP, NetScreen-5XT, NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, ISG 1000, ISG 2000, NetScreen-5200, NetScreen-5400
ScreenOS Support	ScreenOS 5.1.0*, ScreenOS 5.0.0, ScreenOS 5.0-GPRS, ScreenOS 4.0.3, ScreenOS 4.0.1, ScreenOS 4.0.1-SBR, ScreenOS 4.0.1-MCAST, ScreenOS 4.0.0, ScreenOS 4.0.0 DIAL2

*Using NetScreen-Security Manager Feature Pack 3



Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
NetScreen-Security Manager, 10 devices	NS-SM-10
NetScreen-Security Manager, 25 devices	NS-SM-25
NetScreen-Security Manager, 50 devices	NS-SM-50
NetScreen-Security Manager, 100 devices	NS-SM-100
NetScreen-Security Manager, 200 devices	NS-SM-200
NetScreen-Security Manager, 500 devices	NS-SM-500
NetScreen-Security Manager, 1000 devices	NS-SM-1000
NetScreen-Statistical Report Server	NS-SM-SRS

This is only a subset of all part numbers available for this product. For the latest part number and pricing information, please see the Juniper Networks price list.

For More Information:
http://www.juniper.net/products/integrated/dsheet/110018.pdf

"Sid, I think our security has been compromised, what do you think?... Sid?"

Juniper Networks NetScreen-SA Central Manager

The Juniper Networks Secure Access family of appliances has consistently led the SSL VPN market, providing secure access to remote/mobile employees, business partners, and customers. As SSL VPN deployments grow both in cluster size and in breadth of geographic reach, so too has the challenge in providing streamlined, efficient management. Juniper Networks has extended its core competence in the SSL VPN marketplace with the introduction of the Juniper Networks NetScreen-SA Central Manager, a robust product with an intuitive web-based UI designed to facilitate the task of configuring, updating and monitoring Secure Access appliances whether within a single cluster or across a global cluster deployment.

Key Features & Benefits

- System dashboard for an at-a-glance graphical representation of system-wide activities.
- Local back-up and restore eliminates time-intensive process of saving files, downloading to ftp site, then uploading files when needed
- Back-up essential for quick disaster recovery – configurations can be restored in seconds instead of in minutes
- Push technology eliminates incomplete security policy enforcement by sending information to other gateways or clusters
- Consistent security policy enforcement with synchronization to automate propagation of changes within a cluster
- Comprehensive, actionable auditing with rich log filtering capabilities for quick searches of critical events
- Custom log filters, so events can be viewed in the most pertinent context for each admin

When to Sell

- Customer has a large-scale secure access solution to manage and needs a disaster recovery plan
- Wants to maintain a consistent security policy across the enterprise
- Needs a system-wide view of the deployment to see the impact of activity as well as which applications are being utilized

Competitive Products

F5, Nokia

Selected Part Numbers and Ordering Information

PRODUCT	PART NUMBER
NetScreen-SA Central Manager for Secure Access Appliances	
NetScreen-SA Central Manager for 1 device	NS-SA-CM
NetScreen-SA Central Manager for 2 devices in a single cluster	NS-SA-CM2
NetScreen-SA Central Manager for 3 devices in a single cluster	NS-SA-CM3
NetScreen-SA Central Manager for 4 devices in a single cluster	NS-SA-CM4
NetScreen-SA Central Manager for Secure Meeting Appliances	
NetScreen-SM Central Manager for 1 device	NS-SM-CM
NetScreen-SM Central Manager for 2 devices in a single cluster	NS-SM-CM2

For More Information: **http://www.juniper.net/products/ssl/management.html**

Management

WX Central Management System Software

The WX Central Management System™ (CMS™) software offers a powerful, intuitive solution for centrally managing, monitoring and configuring WX and WXC application acceleration platforms distributed throughout an enterprise.

The WX CMS software provides unprecedented visibility into how applications are performing over the WAN, offering detailed information about traffic patterns, bandwidth consumption, and other performance trends that IT can use to maximize WAN resources.

The software also helps IT learn how users and applications are interacting over the WAN, reporting on bandwidth consumption, top talkers, and how Quality of Service (QoS) policies are impacting overall application throughput. Armed with this insight, IT can quickly pinpoint trouble spots, determine whether the WAN is at fault, and drill down to identify and resolve performance, capacity or bandwidth problems.

The WX CMS software also provides visibility into each element of the WX Framework™. With WX CMS software, IT can manage additional WAN capacity created by Molecular Sequence Reduction™ (MSR™) and Network Sequence Caching technologies, see the impact that Packet Flow Acceleration™ (PFA™) and Application Flow Acceleration™ (AppFlow™) technologies have on application performance, allocate bandwidth and prioritize applications through QoS, and direct applications over multiple WAN links with the Policy-based Multipath feature.

Key Features & Benefits

- Provides multi-level visibility into WAN applications and performance
- Executive Summary reports provide at-a-glance views of key traffic, performance, and reduction results
- "My WAN" dashboard allows IT staff to create customized views reporting performance metrics of devices and sites most important to them
- Drill-down reports available by site, device, and link provide details on WAN throughput, latency, packet loss, path monitoring, top talkers, and other statistics
- Automatic data collection feature polls for statistics on traffic, reduction, QoS, and acceleration results
- Global policies allows network managers to centrally manage and modify global configuration settings on all WX/WXC devices
- Global monitoring enables IT to observe all WX/WXC devices, including status reports providing at-a-glance summaries of health, configuration status, and compression and acceleration statistics
- Monitoring data stored for up to one year
- Auto-deployment enables remote WX and/or WXC devices to download configuration data from central WX CMS server without the need for local IT assistance
- Configuration templates enable quick replication to dozens or hundreds of WX/WXC platforms
- Reuse of deployed configurations enable rapid deployment of new WX/WXC devices
- View and compare configurations allow line-by-line comparisons to highlight differences
- Track configuration changes capability simplifies troubleshooting

When to Sell

- Any WX and/or WXC deployment
- WX/WXC deployments where customers need global view into application performance over the WAN
- Geographically dispersed WX/WXC deployments where IT needs a centralized view into WAN performance
- Environments encompassing locations where IT resources are limited or non-existent to assist with the deployment and configuration process
- Any WX/WXC environment where IT needs to monitor bandwidth usage for future expansion and/or capacity planning purposes
- Companies that need to generate customized WAN performance reports covering specific time periods

Competitive Products

Packeteer - Policy Center and Report Center, **Riverbed** - Central Management Console (CMC), **Swan Labs (F5)** - NetCelera Enterprise Manager and **Expand Networks** - ExpandView

Product Specs At-A-Glance

REQUIREMENTS AND SCALABILITY				
Platform:	Windows Server 2000 SP3 or Windows Server 2003			
Web browser:	IE 5.5 or 6.0			
Number of simultaneous users:	50			
Number of WX/C devices:	2,000			
WX/C devices supported:	All platforms running WX OS v5.x or higher			
	# Devices	Pentium 4 CPU (GHz)	RAM	Disk Space (GB)
	Under 100	2.0+	768 MB	40+
	100-500	2.8+	1.5 GB	60+
	500-1,000	3.0+	2.0 GB	80+
	1,000-1,500	3.2+	3.0 GB	100+
	1,500-2,000	3.2+ dual CPU	4.0 GB	120+

Selected Part Numbers and Ordering Information

DESCRIPTION	PART NUMBER
WX Central Management System (CMS)	
CMS Media Kit (incl. CDs and Documentation)	CM-CM
CMS Baseline RTU for 10 devices	CMS-CM-0-10
CMS Baseline RTU for 25 devices	CMS-CM-0-25
CMS Baseline RTU for 50 devices	CMS-CM-0-50
CMS Baseline RTU for 100 devices	CMS-CM-0-100
CMS Baseline RTU for 200 devices	CMS-CM-0-200
CMS Baseline RTU for 300 devices	CMS-CM-0-300
CMS Baseline RTU for 400 devices	CMS-CM-0-400
CMS Baseline RTU for 500 devices	CMS-CM-0-500
CMS Baseline RTU for 750 devices	CMS-CM-0-750
CMS Baseline RTU for 1000 devices	CMS-CM-0-1000
CMS Baseline RTU for 1500 devices	CMS-CM-0-1500
CMS Baseline RTU for 2000 devices	CMS-CM-0-2000

For More Information: **http://www.juniper.net/products/appaccel/wan/wxcms**

Management

Juniper Networks Frequently asked Questions

Why recommend Juniper Networking solutions?

Juniper Networks brings a new pace of innovation to the industry through purpose-built platforms and sophisticated software. It is recognized as a center of excellence in the development of silicon and software that support high-performance, intelligent networks, and remains at the forefront of industry initiatives that drive the continuing transformation of these networks and the businesses they support.

Does Juniper Networks have a Sales Incentive program?

Yes. The J-Rewards program rewards you for the value you add to selling and supporting Juniper Networks solutions. It is available exclusively to members of the J-Partner Program, whether you are a sales representative or sales engineer. You can earn and accumulate points quickly by selling Juniper Networks which can quickly turn into fantastic rewards.

For more information go to **http://www.juniper.net/jrewards/**

What about Reseller Training?

Juniper Networks Partner Training delivers the training and knowledge requested by our authorized Partners. The comprehensive curriculum includes Sales and Technical Essentials designed to highlight products and solutions. These on-demand training modules have 'learning maps' to help you determine your technology, platforms and solutions training needs.

For more information go to **http://www.juniper.net/training/**

What about Customer and Support Services?

Juniper Networks provides a comprehensive and flexible portfolio of industry leading technical support, professional services, and education programs that help customers gain the maximum value from their network investments. The full range of service elements within our three Customer Services families – Transition, Operation, and Optimization – allows you to not just respond to market factors, but anticipate them.

Juniper Networks portfolio of support services provides the backup support that large networks demand and lets customers select from a variety of options that augment their in-house technical expertise. For more Information see the Partner Center Customer Support pages at: (Partner Center login required)

https://www.juniper.net/partners/partner_center/content/reseller/cs/services/

What if I need more information?

Juniper Networks provides a comprehensive set of literature to spark ideas, provide frameworks and ensure that you have the technical information you need to design, select, implement and sell Juniper Networks. Please see below a list of useful URLs and the J-partner help desk telephone number and e-mail address.

Home Page: **http://www.juniper.net**

Product Information: **http://www.juniper.net/products/**

Solutions Information: **http://www.juniper.net/solutions/**

Technical Support: **http://www.juniper.net/support/**

J-Partner Center: **http://www.juniper.net/partners/**

Certification Requirements: **http://www.juniper.net/training/certification/**

Find a Partner: **http://www.juniper.net/partners/find_partner.html**

Partner Registration: **http://www.juniper.net/partners/partner_channels.html**

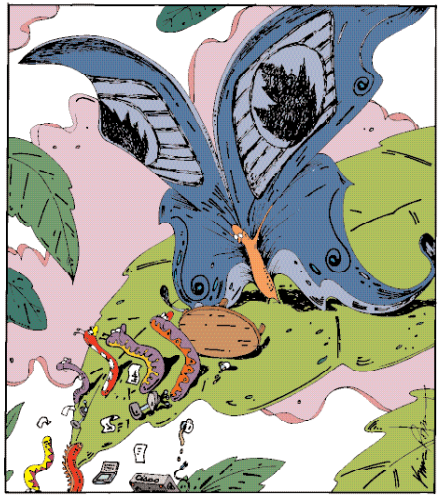
Product End of Life Matrix: **http://www.juniper.net/support/eol/**

Training: **http://www.juniper.net/training/**

Sales Offices Contact Info: **http://www.juniper.net/company/contactus/sales.html**

J-partner helpdesk: **+ 31 20 712 58 57**

Email: **insidesales-emea@juniper.net.**



Tired of his company's prevailing resistant to change attitude, Bob finally decided he'd had enough.

Product Warranty Information

JUNIPER PRODUCT	WARRANTY START DATE*	HARDWARE**	SOFTWARE	JUNIPER TECHNICAL ASSISTANCE (JTAC)***
All Juniper E-, M-, T-, and J-Series	Juniper product date-of-ship	1 year 20-day return-to-factory (RTF) return/replace	90 days software media for JUNOS(e) products	1 year online support for RMA processing only
NetScreen FW/VPN and Secure Access Products	Juniper product date-of-ship	1 year 20-day return-to-factory (RTF) return/replace	1x software update or upgrade	1 year online support for RMA processing only
NetScreen AV Products	Juniper product date-of-ship	1 year 20-day return-to-factory (RTF) return/replace	1 year - ScreenOS AV Signature Service DI Signature Service	1 year online support for RMA processing only
NetScreen IDP	Juniper product date-of-ship	1 year 20-day return-to-factory (RTF) return/replace	1x software update or upgrade	1 year online support for RMA processing only
DX application acceleration platforms	Juniper product date-of-ship	1-year 20-day return-to-factory (RTF) return/replace	90 days software media	1 year online support for RMA processing only
WX/WXC application acceleration platforms	Juniper product date-of-ship	1-year 20-day return-to-factory (RTF) return/replace	90 days software media	1 year online support for RMA processing only
NetScreen Remote	Juniper product date-of-ship	Not Applicable	1x software update or upgrade	Not Applicable

*90 days will be added for any product shipped via channel on the back-end systems
**The 20 day clock starts once product has been received by Juniper; Ship time is not part of 20 days
***For customers that require troubleshooting, install/config assistance should purchase a support contract

This is intended as a summary only. Please refer to the current published version of the Juniper Networks Warranty policy located at: **http://www.juniper.net/support/warranty/**

General Disclaimer

Although Juniper Networks has attempted to provide accurate information in this Guide, Juniper Networks assumes no responsibility for the accuracy of the information. Juniper Networks may change the programs or products mentioned at any time without prior notice. Mention of non-Juniper Networks products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

Many of the Juniper Networks products and services identified in this Guide are provided with written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this Guide shall be deemed to expand, alter, or modify any warranty or license provided by Juniper Networks with any Juniper Networks product, or to create any new or additional warranties or licenses.

About Juniper Networks, Inc.

Juniper Networks is the leader in enabling secure and assured communications over a single IP network. The company's purpose-built, high performance IP platforms enable customers to support many different services and applications at scale. Service providers, enterprises, governments and research and education institutions worldwide rely on Juniper Networks to deliver products for building networks that are tailored to the specific needs of their users, services and applications. Juniper Networks' portfolio of proven networking and security solutions supports the complex scale, security and performance requirements of the world's most demanding networks. Additional information can be found at **www.juniper.net.**

Europe, Middle East, Africa Regional Sales Headquarters
Juniper Networks (UK) Limited
Guildford Road
Leatherhead
Surrey, KT22 9JH
United Kingdom
Phone: 44 (0) 1372 385500
Fax: 44 (0) 1372 385501

Printed in the UK Stock No: 080570-003 12/05