ANEXO 1: Glosario de Términos

Se presenta en este anexo el glosario de términos técnicos utilizados en la elaboración de esta tesis.

AMENAZA

Es un peligro potencial para la información o sistemas. Puede utilizar una vulnerabilidad para dañar una empresa o individuo.

ANTISPAM

Es el método para evitar que correo electrónico de tipo “spam” o “correo basura” no llegue a la casilla de correo electrónico de los usuarios.

APPLIANCE

Equipo o sistema de cómputo que se vende listo para usar, en donde el hardware y software están previamente configurados y usualmente utiliza un sistema operativo propietario.

ATAQUE

Es la ejecución de una amenaza. Y puede ser de cuatro tipos. Interrupción, que corresponde a detener el flujo de la información. Intercepción, que corresponde a capturar parte de la información que fluye o está en un repositorio. Modificación, que corresponde a modificar el comportamiento de un sistema o información y Fabricación, que corresponde a falsificar información o una identificación.

CONFIDENCIALIDAD DE LA INFORMACIÓN

Provee la habilidad de asegurar el nivel de acceso a cierta información y previene accesos no autorizados.

CONTRAMEDIDA

Reduce el riesgo de que una vulnerabilidad pueda ser explotada. Las contramedidas que consideramos en la presente investigación son los antivirus, firewalls, redes privadas virtuales, control de acceso y autenticación fuerte.

CONTROLADOR DE DOMINIO

Es el corazón del servicio de directorio de Microsoft. Entre sus funciones están la autenticación de los usuarios, que es que proceso de garantizar o denegar a un usuario el acceso a recursos de una red Microsoft.

COOKIE:

Archivo que se almacena en el disco duro de una computadora para guardar información de un visitante a un sitio web.

DIRECTORIO ACTIVO

Es la versión propietaria del servicio de directorio LDAP desarrollada por Microsoft para su plataforma Windows. Tiene la función de almacenar de manera centralizada y organizada, la información de una empresa. El directorio activo permite establecer políticas a nivel de empresa, desplegar programas y configuraciones de manera global.

DISPONIBILIDAD DE LA INFORMACIÓN

Busca que los sistemas vuelvan a funcionar en el menor tiempo posible y con la mayor cantidad de sus funcionalidades ante cualquier contrariedad.

EXPLOIT

Programa o software que explota la vulnerabilidad de otro programa o sistema para acceder al mismo de forma no autorizada y causar un comportamiento imprevisto.

GRANULARIDAD

Término que refiere a que tan específico de define el nivel de detalle de una política de seguridad. A mayor granularidad, mayor nivel de detalle.

INTEGRIDAD DE LA INFORMACIÓN

Asegura que la información del sistema sea correcta y consistente. Previene la modificación no autorizada de la información.

MALWARE

Programa, software o código malicioso cuyo objetivo es causar daños a una computadora, sistema o red.

NAT

(Network Address Translation). Traducción en tiempo real de las direcciones IP utilizadas en los paquetes que transportan los dispositivos de ruteo como routers o firewalls, cuando cruzan de una red a otra. Existen dos tipos de NAT: estático y dinámico. El NAT estático permite asociar una a una (1:1) una dirección IP de un segmento a otra de un segundo segmento de manera bidireccional. Una NAT dinámica traslada varias direcciones IP de un segmento a otra, en un único sentido.

PAT

(Port Address Translation). Traducción en tiempo real de direcciones IP y puertos TCP o UDP cuando cruzan un dispositivo de ruteo. Con PAT una sola dirección IP de una red se puede convertir a varias de la otra red.

RAID

Arreglo o combinación de discos duros que funcionan conjuntamente alcanzando un tamaño y rendimiento que no se conseguiría con un sólo disco duro grande, y asegura la redundancia de datos para que éstos no se pierdan en caso de falla.

RED LAN

Redes de área local. Físicamente se encuentran en un mismo local o edificio, o se encuentran en locales cercanos.

RED MAN

Redes de área metropolitana. Físicamente conformada por varias redes LAN localizadas en una misma ciudad.

RED WAN

Físicamente está conformada por varias redes LAN y MAN que pueden estar localizadas en diferentes ciudades o países.

RIESGO

Es la posibilidad o probabilidad de que un ente explote o haga uso de una vulnerabilidad.

SEGURIDAD PERIMETRAL

Asume la integración de elementos y sistemas para la protección de perímetros, detección de tentativas de intrusión y/o disuasión de intrusos.

SERVIDORES PUBLICOS

Son aquellos elementos que por la aplicación que se ejecuta en ellos, son accedidos directamente desde el Internet. Puede tratarse de un servidor de correo, un servidor Web o ftp, entre otros.

SERVICIO

Corresponde a la aplicación que se desea publicar hacia Internet. Puede tratarse de un portal Web, correo electrónico, transferencia de archivos, hasta un portal de transacciones bancarias.

SPYWARE

Programa espía que se instala en una computadora con o sin el consentimiento del usuario para recopilar información de los hábitos de navegación que se realizan en ella.

SSH

(Secure Shell). Protocolo cifrado para acceder en forma segura a maquinas remotas a través de una red.

SSL/TLS

(Secure Sockets Layer/Transport Layer Security). Es un protocolo que ofrece un canal seguro para la transferencia de información para aplicaciones de tipo cliente-servidor. Este canal está diseñado para proveer privacidad y autenticación.

VPN

Red privada virtual. Tecnología para unir dos redes seguras a través de una red insegura (como por ejemplo: Internet).

VULNERABILIDAD

Es un software, hardware o procedimiento defectuoso que puede proporcionar una puerta abierta para accesos no autorizados

ANEXO 2: Hojas Técnicas de los productos que conforman la solución de seguridad

Se presenta en este anexo las hojas técnicas de las soluciones, equipos y software, que conforman la solución propuesta.

SSG5 AND SSG20 SECURE SERVICES GATEWAYS

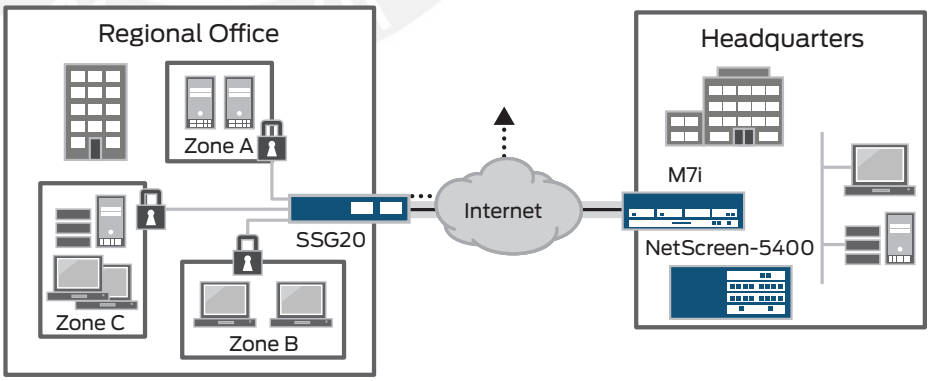
Product Overview

The Juniper Networks SSG5 and SSG20 Secure Services Gateways are purpose-built security appliances that deliver a perfect blend of performance, security, routing and LAN/WAN connectivity for small branch offices, fixed telecommuters and small standalone business deployments. Traffic flowing in and out of the branch office or business is protected from worms, spyware, trojans, and malware by a complete set of Unified Threat Management security features that include stateful firewall, IPsec VPN, intrusion prevention system (IPS), antivirus (includes antispyware, anti-adware, antiphishing), antispam and Web filtering.

Product Description

The Juniper Networks® SSG5 and SSG20 Secure Services Gateways are high-performance security platforms for small branch office and standalone businesses that want to stop internal and external attacks, prevent unauthorized access and achieve regulatory compliance. Both the SSG5 and SSG20 deliver 160 Mbps of stateful firewall traffic and 40 Mbps of IPsec VPN traffic.

Security: Protection against worms, viruses, trojans, spam, and emerging malware is delivered by proven unified threat management (UTM) security features that are backed by best-in-class partners. To address internal security requirements and facilitate regulatory compliance, the SSG5 and SSG20 both support an advanced set of network protection features such as security zones, virtual routers and VLANs that allow administrators to divide the network into distinct secure domains, each with its own unique security policy. Policies protecting each security zone can include access control rules and inspection by any of the supported UTM security features.



The SSG20 deployed at a branch office for secure Internet connectivity and site-to-site VPN to corporate headquarters. Internal wired and wireless resources are protected with unique security policies applied to each security zone.

Connectivity and Routing: The SSG5 has seven on-board 10/100 interfaces with optional fixed WAN ports. The SSG20 has five 10/100 interfaces with two I/O expansion slots for additional WAN connectivity. The broad array of I/O options coupled with WAN protocol and encapsulation support in the routing engine make both the SSG5 and the SSG20 a solution that can easily be deployed as a traditional branch office router or as a consolidated security and routing device to reduce CapEx and OpEx. Both the SSG5 and SSG20 support 802.11 a/b/g as a factory configured option supported by a wide array of wireless specific security features.

Access Control Enforcement: The SSG5 and SSG20 interact as enforcement points in a Juniper Networks Unified Access Control deployment with the simple addition of the IC Series UAC appliance. The IC Series functions as a central policy management engine, interacting with the SSG5 or SSG20 to augment or replace the firewall-based access control with a solution that grants/denies access based on more granular criteria that include endpoint state and user identity in order to accommodate the dramatic shifts in attack landscape and user characteristics.

World Class Support: From simple lab testing to major network implementations, Juniper Networks Professional Services will collaborate with your team to identify goals.

Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFIT
High performance	Purpose-built platform is assembled from custom-built hardware, powerful processing and a security-specific operating system.	Delivers performance headroom required to protect against internal and external attacks now and into the future.
Best-in-class UTM security features	UTM security features (antivirus, antispam, Web filtering, IPS) stop all manner of viruses and malware before they damage the network.	Ensures that the network is protected against all manner of attacks.
Integrated antivirus	Annually licensed antivirus engine is based on Kaspersky Lab engine.	Stops viruses, spyware, adware and other malware.
Integrated antispam	Annually licensed anti-spam offering is based on Sophos technology.	Blocks unwanted email from known spammers and phishers.
Integrated Web filtering	Annually licensed Web filtering solution is based on Websense SurfControl technology.	Controls/blocks access to malicious Web sites.
Integrated IPS (Deep Inspection)	Annually licensed IPS engine.	Prevents application-level attacks from flooding the network.
Fixed Interfaces	Seven fixed 10/100 interfaces on the SSG5, and five fixed 10/100 interfaces on the SSG20. The SSG5 is factory configured with either RS232 Serial/AUX or ISDN BRI S/T or V.92 fixed WAN backup. Both models include one console port and one auxiliary port.	Provides high-speed LAN connectivity, redundant WAN connectivity and flexible management.
Network segmentation	Security zones, virtual LANs and virtual routers allow administrators to deploy security policies to isolate guests, wireless networks and regional servers or databases.	Facilitates deployment of internal security to prevent unauthorized access, contain attacks and assist in achieving regulatory compliance.
Interface modularity	Two interface expansion slots (SSG20 only) supporting optional ADSL 2+, T1, E1, ISDN BRI S/T, Serial, SFP and v.92 Mini physical interface modules (Mini-PIMs).*	Delivers combination of LAN and WAN connectivity on top of unmatched security to reduce costs and extend investment protection.
Robust routing engine	Proven routing engine supports OSPF, BGP, and RIP v1/2.	Enables the deployment of a consolidated security and routing device, thereby lowering operational and capital expenditures.
802.11 a/b/g wireless-specific security features	Wireless-specific privacy and authentication features augment the UTM security capabilities to protect wireless traffic.	Provides additional device consolidation opportunities (WLAN access point, security, routing) for small office environment.

*Serial and SFP Mini-PIMs only supported in ScreenOS 6.0 or greater releases

FEATURE	FEATURE DESCRIPTION	BENEFIT
Juniper Networks Unified Access Control enforcement point	Interacts with the centralized policy management engine (IC Series) to enforce session-specific access control policies using criteria such as user identity, device security state and network location.	Improves security posture in a cost-effective manner by leveraging existing customer network infrastructure components and best-in-class technology.
Management flexibility	Use any one of three mechanisms, command line interface (CLI), WebUI or Juniper Networks Network and Security Manager (NSM) to securely deploy, monitor and manage security policies.	Enables management access from any location, eliminating onsite visits thereby improving response time and reducing operational costs.
World-class professional services	From simple lab testing to major network implementations, Juniper Networks Professional Services will collaborate with your team to identify goals, define the deployment process, create or validate the network design and manage the deployment.	Transforms the network infrastructure to ensure that it is secure, flexible, scalable and reliable.

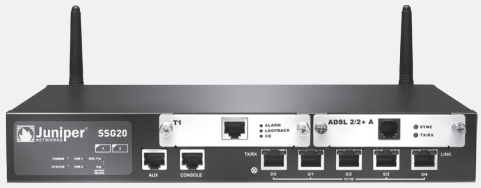
Product Options

OPTION	OPTION DESCRIPTION	APPLICABLE PRODUCTS
DRAM	The SSG5 and SSG20 are available with either 128 MB or 256 MB of DRAM.	SSG5 and SSG20
Unified Threat Management/Content Security (high memory option required)	The SSG5 and SSG20 can be configured with any combination of the following best-in-class UTM and content security functionality: antivirus (includes anti-spyware, antiphishing), IPS (Deep Inspection), Web filtering and/or antispam.	High memory SSG5 or SSG20 only
I/O options	Two interface expansion slots supporting optional ADSL 2+, T1, E1, ISDN BRI S/T, Serial, SFP and v.92 Mini physical interface modules (Mini-PIMs).	SSG20 only
802.11 a/b/g connectivity	The SSG5 and SSG20 can be factory configured for 802.11 a/b/g wireless LAN connectivity.	SSG5 and SSG20
Extended license	Key capacities can be increased (sessions, VPN tunnels, VLANs) and stateful high availability (HA) support for firewall and VPN can be added.	SSG5 and SSG20

SSG5

SSG5 WIRELESS

SSG20



SSG20 WIRELESS

Specifications[1]

	SSG5 BASE/EXTENDED	SSG20 BASE/EXTENDED
Maximum Performance and Capacity[2]		
ScreenOS® version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (Large packets)	160 Mbps	160 Mbps
Firewall performance (IMIX)[3]	90 Mbps	90 Mbps
Firewall packets per second (64 byte)	30,000 PPS	30,000 PPS
Advanced Encryption Standard (AES) 256+SHA-1 VPN performance	40 Mbps	40 Mbps
3DES encryption +SHA-1 VPN performance	40 Mbps	40 Mbps
Maximum concurrent sessions	8,000/16,000	8,000/16,000
New sessions/second	2,800	2,800
Maximum security policies	200	200
Maximum users supported	Unrestricted	Unrestricted
Network Connectivity		
Fixed I/O	7x10/100	5x10/100
Mini-Physical Interface Module (Mini-PIM) slots	0	2
WAN interface options	Factory configured: RS232 Serial AUX or ISDN BRI S/T or V.92	Mini-PIMs: 1xADSL 2+, 1xT1, 1xE1, V.92, ISDN BRI S/T, 1xSFP, 1xSerial
Firewall		
Network attack detection	Yes	Yes
DoS and DDoS protection	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Brute force attack mitigation	Yes	Yes
SYN cookie protection	Yes	Yes
Zone-based IP spoofing	Yes	Yes
Malformed packet protection	Yes	Yes
Unified Threat Management[4]		
IPS (Deep Inspection firewall)	Yes	Yes
Protocol anomaly detection	Yes	Yes
Stateful protocol signatures	Yes	Yes
IPS/DI attack pattern obfuscation	Yes	Yes
Antivirus	Yes	Yes
Instant message AV	Yes	Yes
Signature database	200,000+	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM	POP3, HTTP, SMTP, IMAP, FTP, IM
Antispyware	Yes	Yes
Anti-adware	Yes	Yes
Anti-keylogger	Yes	Yes
Anti-spam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering[5]	Yes	Yes
VoIP Security		
H.323. Application-level gateway (ALG)	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
Network Address Translation (NAT) for VoIP protocols	Yes	Yes

	SSG5 BASE/EXTENDED	SSG20 BASE/EXTENDED
IPsec VPN		
Auto-Connect VPN	Yes	Yes
Concurrent VPN tunnels	25/40	25/40
Tunnel interfaces	10	10
DES encryption (56-bit), 3DES encryption (168-bit) and Advanced Encryption Standard (AES) (256-bit)	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes
Manual key, Internet Key Exchange (IKE), IKEv2 with EAP public key infrastructure (PKI) (X.509)	Yes	Yes
Perfect forward secrecy (DH Groups)	1,2,5	1,2,5
Prevent replay attack	Yes	Yes
Remote access VPN	Yes	Yes
Layer2 Tunneling Protocol (L2TP) within IPsec	Yes	Yes
IPsec Network Address Translation (NAT) traversal	Yes	Yes
Redundant VPN gateways	Yes	Yes
User Authentication and Access Control		
Built-in (internal) database - user limit	100	100
Third-party user authentication	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes	Yes
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
802.1X authentication	Yes	Yes
Unified Access Control (UAC) enforcement point	Yes	Yes
PKI Support		
PKI Certificate requests (PKCS 7 and PKCS 10)	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes
Online Certificate Status Protocol (OCSP)	Yes	Yes
Certificate Authorities supported	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI
Self-signed certificates	Yes	Yes
Virtualization		
Maximum number of security zones	8	8
Maximum number of virtual routers	3/4	3/4
Maximum number of VLANs	10/50	10/50
Routing		
BGP instances	3/4	3/4
BGP peers	10/16	10/16
BGP routes	1,024	1,024
OSPF instances	3	3
OSPF routes	1,024	1,024
RIP v1/v2 instances	16	16
RIP v2 routes	1,024	1,024
Static routes	1,024	1,024
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
Equal-cost multipath (ECMP)	Yes	Yes

Specifications (continued)

	SSG5 BASE/EXTENDED	SSG20 BASE/EXTENDED
Routing (continued)		
Multicast	Yes	Yes
Reverse Path Forwarding (RPF)	Yes	Yes
Internet Group Management Protocol (IGMP) (v1, v2)	Yes	Yes
IGMP Proxy	Yes	Yes
PIM single mode	Yes	Yes
PIM source-specific multicast	Yes	Yes
Multicast inside IPsec tunnel	Yes	Yes
ICMP Router Discovery Protocol (IRDP)	Yes	Yes
Encapsulations		
Point-to-Point Protocol (PPP)	Yes	Yes
Multilink Point-to-Point Protocol (MLPPP)	N/A	Yes
Frame Relay	Yes	Yes
Multilink Frame Relay (MLFR) (FRF 15, FRF 16)	Yes	Yes
HDLC	Yes	Yes
IPv6		
Dual stack IPv4/IPv6 firewall and VPN	Yes	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes	Yes
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes	Yes
RIPng	Yes	Yes
BGP	Yes	Yes
Transparent mode	Yes	Yes
NSRP	Yes	Yes
DHCPv6 Relay	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode[6]	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes
Address Translation		
Network Address Translation (NAT)	Yes	Yes
Port Address Translation (PAT)	Yes	Yes
Policy-based NAT/PAT (L2 and L3 mode)	Yes	Yes
Mapped IP (MIP) (L3 mode)	300	300
Virtual IP (VIP) (L3 mode)	4/5	4/5
MIP/VIP Grouping (L3 mode)	Yes	Yes
Dual untrust	Yes	Yes
Bridge groups*	Yes	Yes
IP Address Assignment		
Static	Yes	Yes
DHCP, PPPoE client	Yes	Yes
Internal DHCP server	Yes	Yes
DHCP relay	Yes	Yes
Traffic Management Quality of Service (QoS)		
Guaranteed bandwidth	Yes - per policy	Yes - per policy
Maximum bandwidth	Yes - per policy	Yes - per policy
Ingress traffic policing	Yes	Yes
Priority-bandwidth utilization	Yes	Yes
Differentiated Services stamping	Yes - per policy	Yes - per policy

*Bridge groups supported only on uPIMs in ScreenOS 6.0 and greater releases

	SSG5 BASE/EXTENDED	SSG20 BASE/EXTENDED
High Availability (HA)[7]		
Active/Active - L3 mode	Yes	Yes
Active/Passive -Transparent & L3 mode	Yes	Yes
Configuration synchronization	Yes	Yes
Session synchronization for firewall and VPN	Yes	Yes
Session failover for routing change	Yes	Yes
VRRP	Yes	Yes
Device failure detection	Yes	Yes
Link failure detection	Yes	Yes
Authentication for new HA members	Yes	Yes
Encryption of HA traffic	Yes	Yes
System Management		
WebUI (HTTP and HTTPS)	Yes	Yes
Command line interface (console)	Yes	Yes
Command line interface (telnet)	Yes	Yes
Command line interface (SSH)	Yes v1.5 and v2.0 compatible	Yes v1.5 and v2.0 compatible
Network and Security Manager (NSM)	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
Rapid deployment	Yes	Yes
Administration		
Local administrator database size	20	20
External administrator database support	RADIUS, RSA SecurID, LDAP	RADIUS, RSA SecureID, LDAP
Restricted administrative networks	6	6
Root Admin, Admin and Read Only user levels	Yes	Yes
Software upgrades	TFTP, WebUI, NSM, SCP, USB	TFTP, WebUI, NSM, SCP, USB
Configuration rollback	Yes	Yes
Logging/Monitoring		
Syslog (multiple servers)	Yes - up to 4 servers	Yes - up to 4 servers
Email (two addresses)	Yes	Yes
NetIQ WebTrends	Yes	Yes
SNMP (v2)	Yes	Yes
SNMP full custom MIB	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes
External Flash		
Additional log storage	USB 1.1	USB 1.1
Event logs and alarms	Yes	Yes
System configuration script	Yes	Yes
ScreenOS Software	Yes	Yes

	SSG5 BASE/EXTENDED	SSG20 BASE/EXTENDED
Dimensions and Power		
Dimensions (W x H x D)	8.8 x 1.6 x 5.6 in (22.2 x 4.1 x 14.3 cm)	11.6 x 1.8 x 7.4 in (29.5 x 4.5 x 18.7 cm)
Weight	2.1 lb (0.95 kg)	3.3 lb (1.5 kg)
Rack mountable	Yes	Yes
Power supply (AC)	100-240 VAC	100-240 VAC
Maximum thermal output	122.8 BTU/Hour	122.8 BTU/Hour
Certifications		
Safety certifications	CSA, CB	CSA, CB
EMC certifications	FCC class B, CE class B, A-Tick, VCCI class B	FCC class B, CE class B, A-Tick, VCCI class B
Mean Time Between Failures (MTBF)		
Non-wireless	40.5 years	35.8 years
Wireless	22.8 years	28.9 years
Security Certifications		
Common Criteria: EAL4	Yes	Yes
FIPS 140-2: Level 2	Yes	Yes
ICSA Firewall and VPN	Yes	Yes
Operating Environment		
Operating temperature	32º to 104º F (0º to 40º C)	32º to 104º F (0º to 40º C)
Non-operating temperature	-4º to 149º F (-20º to 65º C)	-4º to 149º F (-20º to 65º C)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing
Wireless Radio Specifications (Wireless Models Only)		
Transmit power	Up to 200 mW	Up to 200 mW
Wireless standards supported	Dual Radio 802.11 a + 802.11b/g	Dual Radio 802.11 a + 802.11b/g
Site survey	Yes	Yes
Maximum configured SSIDs	16	16
Maximum active SSIDs	4	4
Atheros SuperG	Yes	Yes
Atheros eXtended Range (XR)	Yes	Yes
Wi-Fi Certified®	Yes	Yes
Wireless Security (Wireless Models Only)		
Wireless privacy	WPA, WPA2 (AES or TKIP), IPsec VPN, WEP	WPA, WPA2 (AES or TKIP), IPsec VPN, WEP
Wireless authentication	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x
MAC access controls	Permit or Deny	Permit or Deny
Client isolation	Yes	Yes
Antenna Option (Wireless Models Only)		
Diversity antenna	Included	Included
Directional antenna	Optional	Optional
Omni-directional antenna	Optional	Optional

(1) Some features and functionality only supported in releases greater than ScreenOS 5.4.

(2) Performance, capacity and features listed are based upon systems running ScreenOS 6.2 and are the measured maximums under ideal testing conditions unless otherwise noted. Actual results may vary based on ScreenOS release and deployment. For a complete list of supported ScreenOS versions for SSG Series gateways, please visit the Juniper Customer Support Center (www.juniper.net/customers/support/) and click on ScreenOS Software Downloads

(3) IMIX stands for Internet mix and is more demanding than a single packet size as it represents a traffic mix that is more typical of a customer's network. The IMIX traffic used is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic.

(4) UTM Security features (IPS/Deep Inspection, antivirus, antispam and Web filtering) are delivered by annual subscriptions purchased separately from Juniper Networks. Annual subscriptions provide signature updates and associated support. The high memory option is required for UTM Security features.

(5) Redirect Web filtering sends traffic from the firewall to a secondary server. The redirect feature is free, however it does require the purchase of a separate Web filtering license from either Websense or SurfControl.

(6) NAT, PAT, policy-based NAT, virtual IP, mapped IP, virtual systems, virtual routers, VLANs, OSPF, BGP, RIPv2, active/active HA and IP address assignment are not available in layer 2 transparent mode.

(7) Active/passive and active/active HA requires the purchase of an Extended License. In addition to the HA features, an Extended License key increases a subset of the capacities as outlined below. Active/active HA is only supported in ScreenOS 6.0 or greater releases.

IPS (Deep Inspection firewall) Signature Packs

Signature packs provide the ability to tailor the attack protection to the specific deployment and/or attack type. The following signature packs are available for the SSG5 and SSG20:

SIGNATURE PACK	TARGET DEPLOYMENT	DEFENSE TYPE	TYPE OF ATTACK OBJECT
Base	Branch offices, small/medium businesses	Client/server and worm protection	Range of signatures and protocol anomalies
Client	Remote/branch offices	Perimeter defense, compliance for hosts (desktops, etc.)	Attacks in the server-to-client direction
Server	Small/medium businesses	Perimeter defense, compliance for server infrastructure	Attacks in the client-to-server direction
Worm mitigation	Remote/branch offices of large enterprises	Most comprehensive defense against worm attacks	Worms, trojans, backdoor attacks

Firewall Extended Licenses

EXTENDED LICENSE FEATURE	SSG20 AND SSG5
Sessions	Increases max from 8,000 to 16,000
VPN tunnels	Increases max from 25 to 40
VLANs	Increases max from 10 to 50
VoIP calls	Increases max from 64 to 96
High availability	Adds support for stateful active/active or active/passive with ScreenOS 6.0 and above

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Ordering Information

MODEL NUMBER	DESCRIPTION
SSG5	
SSG-5-SB	SSG5 with 128 MB Memory, RS232 Serial backup interface
SSG-5-SB-BT	SSG5 with 128 MB Memory, ISDN BRI S/T backup interface
SSG-5-SB-M	SSG5 with 128 MB Memory, v.92 backup interface
SSG-5-SB-W-xx	SSG5 with 128 MB Memory, RS232 Serial backup interface, 802.11a/b/g Wireless
SSG-5-SB-BTW-xx	SSG5 with 128 MB Memory, ISDN BRI S/T backup interface, 802.11a/b/g Wireless
SSG-5-SB-MW-xx	SSG5 with 128 MB Memory, v.92 backup interface, 802.11a/b/g Wireless
SSG-5-SH	SSG5 with 256 MB Memory, RS232 Serial backup interface
SSG-5-SH-BT	SSG5 with 256 MB Memory, ISDN BRI S/T backup interface
SSG-5-SH-M	SSG5 with 256 MB Memory, v.92 backup interface
SSG-5-SH-W-xx	SSG5 with 256 MB Memory, RS232 Serial backup interface, 802.11a/b/g Wireless
SSG-5-SH-BTW-xx	SSG5 with 256 MB Memory, ISDN BRI S/T backup interface, 802.11a/b/g Wireless
SSG-5-SH-MW-xx	SSG5 with 256 MB Memory, v.92 backup interface, 802.11a/b/g Wireless
SSG20	
SSG-20-SB	SSG20 with 128 MB Memory, 2-port Mini-PIM slots
SSG-20-SB-W-xx	SSG20 with 128 MB Memory, 2-port Mini-PIM slots, 802.11a/b/g Wireless
SSG-20-SH	SSG20 with 256 MB Memory, 2-port Mini-PIM slots
SSG-20-SH-W-xx	SSG20 with 256 MB Memory, 2-port Mini-PIM slots, 802.11a/b/g Wireless
SSG20 I/O Options	
JXM-1SERIAL-S	1-port Serial Mini Physical Interface Module*
JXM-1SFP-S	1-port SFP Mini Physical Interface Module**
JXM-1T1-S	1-port T1 Mini Physical Interface Module
JXM-1E1-S	1-port E1 Mini Physical Interface Module
JXM-1ADSL2-A-S	1-port ADSL2+ Annex A Mini Physical Interface Module
JXM-1ADSL2-B-S	1-port ADSL2+ Annex B Mini Physical Interface Module
JXM-1V92-S	1-port v.92 Mini Physical Interface Module
JXM-1BRI-ST-S	1-port ISDN S/T BRI Mini Physical Interface Module
JX-SFP-1GE-LX	Small Form Factor Pluggable 1000BASE-LX Gigabit Ethernet Optical Transceiver Module
JX-SFP-1GE-SX	Small Form Factor Pluggable 1000BASE-SX Gigabit Ethernet Optical Transceiver Module
JX-SFP-1GE-T	Small Form Factor Pluggable 1000BASE-T Gigabit Ethernet Copper Transceiver Module
JX-SFP-1FE-FX	Small Form Factor Pluggable 100BASE-FX Fast Ethernet Optical Transceiver Module

MODEL NUMBER	DESCRIPTION
SSG5 / SSG20 Accessories and Upgrades	
SSG-5-ELU	Extended license upgrade key for SSG5
SSG-20-ELU	Extended license upgrade key for SSG20
SSG-5-20-MEM-256	SSG5 and SSG20 256 MB memory upgrade module
SSG-5-RMK	SSG5 rack mount kit - holds 2 units
SSG-20-RMK	SSG20 rack mount kit
SSG-ANT	SSG Series wireless replacement antenna
SSG-ANT-DIR	SSG5 and SSG20 dual band directional antenna
SSG-ANT-OMNI	SSG5 and SSG20 dual band omni-directional antenna
SSG-CBL-ANT-10M	10 meters (30 feet) low loss cable for SSG-ANT-XXX
Unified Threat Management/Content Security (High Memory Option Required)	
NS-K-AVS-SSG5 NS-K-AVS-SSG20	Antivirus (incl. antispyware, antiphishing)
NS-DI-SSG5 NS-DI-SSG20	IPS (Deep Inspection)
NS-WF-SSG5 NS-WF-SSG20	Web Filtering
NS-SPAM2-SSG5 NS-SPAM2-SSG20	Anti-spam
NS-RBO-CS-SSG5 NS-RBO-CS-SSG20	Remote Office Bundle (Includes AV, DI, WF)
NS-SMB2-CS-SSG5 NS-SMB2-CS-SSG20	Main Office Bundle (Includes AV, DI, WF, AS)

- Note: The appropriate power cord is included based upon the sales order "Ship To" destination.
- Note: XX denotes region code for wireless devices. Not all countries are supported. Please see Wireless Country Compliance Matrix for certified countries.
- Note: For renewal of Content Security Subscriptions, add "-R" to above SKUs.
- Note: For 2 year Content Security Subscriptions, add "-2" to above SKUs.
- Note: For 3 year Content Security Subscriptions, add "-3" to above SKUs.

About Juniper Networks

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

* The Serial Mini-PIM is only supported in ScreenOS 6.0 or greater releases
** The SFP Mini-PIM is only supported in ScreenOS 6.0 or greater releases

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

1000176-005-EN Dec 2009

SA SERIES SSL VPN APPLIANCES

SA2500, SA4500, SA6500

Product Overview

The Juniper Networks SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes. With the SA6500, Juniper continues to demonstrate its SSL VPN market leadership by delivering a highly scalable solution based on real-world performance Juniper Networks SA Series SSL VPN Appliances lead the SSL VPN market with a complete range of remote access appliances. The SA Series now includes Junos Pulse which provides a simple, intuitive client that provides secure, authenticated access for remote users from any Web-enabled device to corporate resources. The SA Series combines the security of SSL with standards-based access controls, granular policy creation, and unparalleled flexibility. The result provides ubiquitous security for all enterprise tasks with options for increasingly stringent levels of access control to protect the most sensitive applications and data. Juniper Networks SA Series SSL VPN Appliances deliver lower total cost of ownership over traditional IPsec client solutions and unique end-to-end security features.

Product Description

The Juniper Networks® SA2500, SA4500, and SA6500 SSL VPN Appliances meet the needs of companies of all sizes. With the SA6500, Juniper continues to demonstrate its SSL VPN market leadership by delivering a highly scalable solution based on real-world performance testing. SA Series SSL VPN Appliances use SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks SA Series also offers sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without requiring infrastructure changes, demilitarized zone (DMZ) deployments, or software agents.

The SA Series now includes Juniper Networks Junos® Pulse, a dynamic, integrated, multi-service network client for mobile and non-mobile devices. Junos Pulse enables optimized, accelerated anytime, anywhere access to corporate data. Pulse enables secure SSL access from a wide range of mobile and non-mobile devices, including smartphones, netbooks, notebooks, Wi-Fi or 3G-enabled devices. Junos Pulse delivers enterprises improved productivity and secure, ubiquitous access to corporate data and applications, anytime, anywhere. For more details on Junos Pulse, please visit **www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/**.

Architecture and Key Components

The SA2500 SSL VPN Appliance enables small- to medium-size businesses (SMBs) to deploy cost-effective remote and extranet access, as well as intranet security. Users can access the corporate network and applications from any machine over the Web. The SA2500 offers high availability (HA) with seamless user failover. And because the SA2500 runs the exact same software as the larger SA4500 and SA6500, even smaller organizations gain the same high-performance, administrative flexibility, and end user experience.

The SA4500 SSL VPN Appliance enables mid-to-large size organizations to provide cost-effective extranet access to remote employees and partners using only a Web browser. SA4500 features rich access privilege management functionality that can be used to create secure customer/partner extranets. This functionality also allows the enterprise to secure access to the corporate intranet, so that different employee and visitor populations can use exactly the resources they need while adhering to enterprise security policies. Built-in compression

for all traffic types speeds performance, and hardware-based SSL acceleration is available for more demanding environments. The SA4500 also offers HA with seamless user failover.

The SA6500 SSL VPN Appliance is purpose-built for large enterprises and service providers. It features best-in-class performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. Additionally, the SA6500 offers HA with seamless user failover. The SA6500 also features a built-in compression for Web and files, and a state-of-the-art SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes.

Because each of the SA Series SSL VPN Appliances runs on the same software, there is no need to compromise user or administrator experience based on which one you choose. All devices offer leading performance, stability, and scalability. Therefore, deciding which device will best fit the needs of your organization is easily determined by matching the required number of concurrent users, and perhaps system redundancy and large-scale acceleration options, to the needs of your growing remote access user population.

- **SA2500**: Supports SMBs as a cost-effective solution that can easily handle up to 100 concurrent users on a single system or two-unit cluster.
- **SA4500**: Enables mid-to-large size organizations to grow to as many as 1,000 concurrent users on a single system and offers the option to upgrade to hardware-based SSL acceleration for those that demand the most performance available under heavy load.
- **SA6500**: Purpose-built for large enterprises and service providers, the SA6500 features best-in-class performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements, with support for as many as 10,000 concurrent users on a single system or tens of thousands of concurrent users across a four-unit cluster.

SA6500 Standard Features

- Dual, mirrored hot swappable Serial Advanced Technology Attachment (SATA) hard drives
- Dual, hot swappable fans
- Hot swappable power supply
- 4 gigabyte SDRAM
- 4-port copper 10/100/1000 interface card
- 1-port copper 10/100/1000 management interface
- Hardware-based SSL acceleration module

SA6500 Optional Features

- Second power supply or DC power supply available
- 4-port small form-factor pluggable (SFP) interface card

Features and Benefits

Junos Pulse

Junos Pulse is an integrated, multi-service network client enabling anytime, anywhere connectivity, security, and acceleration with a simplified user experience that requires minimal user interaction. Junos Pulse makes secure network and cloud access easy through virtually any device – mobile or non-mobile, Wi-Fi or 3G-enabled, managed or unmanaged – over a broad array of computing and mobile operating systems. The following table provides the key features and benefits of Junos Pulse working with the SA Series appliances.

FEATURES	BENEFITS
Layer 3 SSL VPN (Network Connect)	• Layer 3 VPN connectivity with granular access control • SSL mode only; no ESP (Encapsulating Security Payload) mode
Location awareness	• Seamless roaming from remote access (to Juniper SA Series) to local LAN access (via Juniper UAC) • Junos Pulse can be pre-configured by admins to automatically prompt end-users for credentials to authenticate to the SA Series when they are remote
Endpoint security	• Full Host Checker capability to check endpoint security • Enhanced Endpoint Security delivers on-the-fly malware protection, pre-connection scanning policies, and real-time protection supported by both the SA Series and UAC
Split tunneling options (enable or disable without route monitoring)	• Key split tunneling options of Network Connect supported • Enforces secure, granular access control
Flexible launch options (standalone client, browser-based launch)	• Users can easily launch Junos Pulse via the web from the SA Series landing page • Remote users can simply launch Junos Pulse from their desktop
Pre-configuration options (pre-configured installer to contain list of SA Series appliances)	• Admins can pre-configure a Junos Pulse deployment with a list of corporate SA Series appliances for end-users to choose from
Connectivity options (max/idle session timeouts, automatic reconnect, logging)	• Admins can set up flexible connectivity options for remote users

For more details on Junos Pulse, please visit **www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/**.

High Scalability Support on SA6500 SSL VPN Appliance

The SA6500 is designed to meet the growing needs of large enterprises and service providers with its ability to support thousands of users accessing the network remotely. The following list shows the number of concurrent users that can be supported on the SA6500 platform:

- Single SA6500: Supports up to 10,000 concurrent users
- Two-unit cluster of SA6500s: Supports up to 18,000 concurrent users
- Three-unit cluster of SA6500s: Supports up to 24,000 concurrent users
- Four-unit cluster of SA6500s: Supports up to 30,000 concurrent users

All performance testing is done based on real-world scenarios with simulation of traffic based on observed customer networks.

End-to-End Layered Security

The SA2500, SA4500, and SA6500 provide complete end-to-end layered security, including endpoint client, device, data, and server layered security controls.

Table 1: End-to-End Layered Security Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Antimalware support with Enhanced Endpoint Security	Dynamically download Webroot's market-leading antimalware software to enforce endpoint security on devices which may not be corporate-assigned computers being used for network access.	Protects endpoints from infection in real-time from antimalware and thereby protects corporate resources from harm during network access. Enables dynamic enforcement of antimalware protection on unmanaged assets, such as PC's of external partners, customers or suppliers.
SMS auto-remediation	Automatically remediates non-compliant endpoints by updating software applications that do not comply to corporate security policies. Dynamically initiates an update of these software applications on the endpoint using Microsoft's SMS protocol.	Improves productivity of remote users who will gain immediate access to the corporate network without having to wait for periodic updates of software applications, and ensures compliance with corporate security policies.
Host Checker	Client computers can be checked both prior to and during a session to verify an acceptable device security posture requiring installed/running endpoint security applications (antivirus, firewall, other). Also supports custom built checks including verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certificates, and more. Includes cache cleaner that erases all proxy downloads and temp files at logout.	Verifies/ensures that endpoint device meets corporate security policy requirements before granting access, remediating devices, and quarantining users when necessary. Also, ensures no potentially sensitive data is left behind on the endpoint device.
Host Checker API	Created in partnership with best-in-class endpoint security vendors. Enables enterprises to enforce an endpoint trust policy for managed PCs that have personal firewall, antivirus clients, or other installed security clients, and quarantine non-compliant devices.	Uses current security policies with remote users and devices; easier management.
Trusted Network Connect (TNC) support on Host Checker	Allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions.	Enables customers to leverage existing investments in endpoint security solutions from third-party vendors.
Policy-based enforcement	Allows the enterprise to establish trustworthiness of non-API compliant hosts without writing custom API implementations or locking out external users, such as customers or partners that run other security clients.	Enables access to extranet endpoint devices like PCs from partners that may run different security clients than that of the enterprise.
Hardened security appliance	Designed on a purpose-built operating system.	Not designed to run any additional services and is thus less susceptible to attacks; no backdoors to exploit or hack.
Security services with kernel-level packet filtering and safe routing	Undesirable traffic is dropped before it is processed by the TCP stack.	Ensures that unauthenticated connection attempts such as malformed packets or denial of service (DoS) attacks are filtered out.
Secure virtual workspace	A secure and separate environment for remote sessions that encrypts all data and controls I/O access (printers, drives).	Ensures that all corporate data is securely deleted from unsecure kiosks after a session.
Coordinated threat control	Enables SA Series SSL VPN Appliances and Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to tie the session identity of the SSL VPN with the threat detection capabilities of the IDP Series, taking automatic action on users launching attacks.	Effectively identifies, stops, and remediates both network and application-level threats within remote access traffic.

Ease of Administration

In addition to enterprise-class security benefits, the SA2500, SA4500, and SA6500 have a wealth of features that make it easy for the administrator to deploy and manage.

Table 2: Ease of Administration Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Bridge CA (Certificate Authority) support	Enables the SA Series to support federated PKI deployments with client certificate authentication. Bridge CA is a PKI extension (as specified in RFC 5280) to cross-certify client certificates that are issued by different trust anchors (Root CAs). Also, enables the customer to configure policy extensions in the SA Series admin UI, to enforce during certificate validation. These policy extensions can be configured as per RFC 5280 guidelines.	Enables customers who use advanced PKI deployments to deploy the SA Series to perform strict standards-compliant certificate validation, before allowing data and applications to be shared between organizations and users.
Based on industry standard protocols and security methods	No installation or deployment of proprietary protocols is required.	SA Series investment can be leveraged across many applications and resources over time.
Extensive directory integration and broad interoperability	Existing directories in customer networks can be leveraged for authentication and authorization, enabling granular secure access without recreating those policies.	Existing directory investments can be leveraged with no infrastructure changes; no APIs for directory integration, as they are all native/built in.
Integration with strong authentication and identity and access management platforms	Ability to support SecurID, Security Assertion Markup Language (SAML), and public key infrastructure (PKI)/ digital certificates.	Leverages existing corporate authentication methods to simplify administration.
Multiple hostname support	Ability to host different virtual extranet websites from a single SA Series SSL VPN Appliance.	Saves the cost of incremental servers, eases management overhead, and provides a transparent user experience with differentiated entry URLs.
Customizable user interface	Creation of completely customized sign-on pages.	Provides an individualized look for specified roles, streamlining the user experience.
Juniper Networks Network and Security Manager (NSM)	Intuitive centralized UI for configuring, updating, and monitoring SA Series appliances within a single device/ cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure and maintain SA Series appliances and other Juniper devices from one central location.
In Case of Emergency (ICE)	Provides licenses for a large number of additional users on an SA Series SSL VPN Appliance for a limited time when a disaster or epidemic occurs.	Enables a company to continue business operations by maintaining productivity, sustaining partnerships, and delivering continued services to customers when the unexpected happens.
Cross-platform support	Ability for any platform to gain access to resources such as Windows, Mac, Linux or various mobile devices including iPhone, WinMobile, Symbian, and Android.	Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.

Rich Access Privilege Management Capabilities

The SA2500, SA4500, and SA6500 provide dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets. When users log into the SA Series SSL VPN Appliance, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security restrictions.

Table 3: Access Privilege Management Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
UAC-SA federation	Seamlessly provision SA Series user sessions into Juniper Networks Unified Access Control upon login – or the alternative (provisioning of UAC sessions into the SA Series). Users need to authenticate only one time to get access in these types of environments.	Provides users – whether remote or local – seamless access with a single login to corporate resources that are protected by access control policies from UAC or the SA Series. Simplifies end user experience.
Certificate authentication to backend servers	Enables customers to enforce client authentication on their secure backend servers and allows the SA to present an admin-configured certificate to these servers for authentication.	Allows customers to mandate strict SSL policies on their backend servers by configuring client authentication.

FEATURE	FEATURE DESCRIPTION	BENEFITS
Client cert auth for ActiveSync	Any mobile device supporting ActiveSync along with client side certificates can now be challenged by the SA Series for a valid client certificate before being allowed access to the ActiveSync server.	Enables the administrator to enforce strict mobile authentication policies for ActiveSync access from mobile devices.
Multiple sessions per user	Allows remote users to launch multiple sessions to the SA Series appliance.	Enables remote users to have multiple authenticated sessions open at the same time.
User-record synchronization	Supports synchronization of user records such as user bookmarks across different non-clustered SA Series appliances.	Ensures ease of experience for users who often travel from one region to another and therefore need to connect to different SA Series appliances.
VDI (Virtual Desktop Infrastructure) support	Allows interoperability with VMware View Manager and Citrix XenDesktop to enable administrators to deploy virtual desktops with the SA Series appliances.	Provides seamless access to remote users to their virtual desktops hosted on VMware or Citrix servers. Provides dynamic delivery of the Citrix ICA client or the VMware View client, including dynamic client fallback options to allow users to easily connect to their virtual desktops.
ActiveSync feature	Provides secure access connectivity from mobile devices (such as Symbian, Windows Mobile, or iPhone) to the Exchange server with no client software installation. Enables up to 5000 simultaneous sessions on the SA6500.	Enables customers to allow a large number of users including employees, contractors and partners to access corporate resources through mobile phones via ActiveSync.
Dynamic role mapping with custom expressions	Combines network, device, and session attributes to determine which types of access are allowed. A dynamic combination of attributes on a per-session basis can be used to make the role mapping decision.	Enables the administrator to provision by purpose for each unique session.
Resource authorization	Provides extremely granular access control to the URL, server, or file level, for different roles of users.	Allows administrators to tailor security policies to specific groups, providing access only to essential data.
Granular auditing and logging	Can be configured to the per-user, per-resource, per-event level for security purposes as well as capacity planning.	Provides fine-grained auditing and logging capabilities in a clear, easy to understand format.

Flexible Single Sign-On (SSO) Capabilities

The SA2500, SA4500, and SA6500 offer comprehensive single sign-on features. These features increase end user productivity, greatly simplify administration of large diverse user resources, and significantly reduce the number of help desk calls.

Table 4: Flexible Single Sign-on Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Kerberos Constrained Delegation	Support for Kerberos Constrained Delegation protocol. When a user logs into the SA Series with a credential that cannot be proxied through to the backend server, the SA Series appliance will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. The ticket will be cached on the SA Series appliance throughout the session. When the user accesses Kerberos-protected applications, the SA Series will use the cached Kerberos credentials to log the user into the application without prompting for a password.	Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Kerberos SSO and NTLMv2 support	SA Series will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	Simplifies user experience by avoiding having users enter credentials multiple times to access different applications.
Password management integration	Standards-based interface for extensive integration with password policies in directory stores (LDAP, Microsoft Active Directory, NT, and others).	Leverage existing servers to authenticate users; users can manage their passwords directly through the SA Series interface.
Web-based Single Sign-On (SSO) basic authentication and NT LAN Manager (NTLM)	Allows users to access other applications or resources that are protected by another access management system without re-entering login credentials.	Alleviates the need for end users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable-based, SAML-based	Ability to pass user name, credentials, and other customer-defined attributes to the authentication forms of other products and as header variables.	Enhances user productivity and provides a customized experience.

The SA2500, SA4500, and SA6500 include three different access methods. These different methods are selected as part of the user's role, so the administrator can enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Table 5: Provisioning Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
IPsec/IKEv2 support for mobile devices	Allows remote users to connect from devices such as PDA's, mobile devices and smartphones which support IKEv2 VPN connectivity. Administrator can also enable strict certificate authentication for access via IPsec/IKEv2.	Extends Juniper's leading mobility and access control features of SA Series to broad range of devices and OS platforms that support IKEv2 VPN connectivity. Enables remote users to securely authenticate to the SA Series appliance from platforms that support IKEv2 VPN connectivity.
Clientless core Web access	Access to web-based applications, including complex JavaScript, XML, or Flash-based apps and Java applets that require a socket connection, as well as standards-based email like Outlook Web Access (OWA), Windows and UNIX file share, telnet/SSH hosted-applications, Terminal Emulation, SharePoint, and others.	Provides the most easily accessible form of application and resource access from a variety of end user machines, including handheld devices; enables extremely granular security control options; completely clientless approach using only a Web browser.
Secure Application Manager (SAM)	A lightweight Java or Windows-based download enabling access to client/server applications.	Enables access to client/server applications using just a Web browser; also provides native access to terminal server applications without the need for a pre-installed client.
Network Connect (NC)	Provides complete network-layer connectivity via an automatically provisioned cross-platform download; Windows Logon/GINA integration for domain SSO; installer services to mitigate need for admin rights. Allows for split tunneling capability.	Users only need a Web browser. Network Connect transparently selects between two possible transport methods to automatically deliver the highest performance possible for every network environment. When used with Juniper Networks Installer Services, no admin rights are needed to install, run, and upgrade Network Connect; optional standalone installation is available as well. Split tunneling capability provides flexibility to specify which subnets or hosts to include or exclude from being tunneled.
Junos Pulse	Single, integrated remote access client that can also provide LAN access control, WAN acceleration and Dynamic VPN features to remote users, in conjunction with Juniper Networks UAC, WXC Series Application Acceleration Platforms and SRX Series Services Gateways devices respectively.	Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities – such as VPN, LAN access control and WAN acceleration. By seamlessly integrating all these functionalities into one single, easy-to-use client, administrators can save on client management and deployment costs to end users.

Product Options

The SA2500, SA4500, and SA6500 appliances include various license options for greater functionality.

User License

With the release of the SA2500, SA4500, and SA6500 appliances, purchasing has been simplified, thanks to a combination of features that were once separate upgrades. Now, there is only one license that is needed to get started: the user licenses. Current customers with the older generation hardware (Juniper Networks SA2000, SA4000, and SA6000) will also benefit from these changes as systems are upgraded to version 6.1 (or higher) software.

User licenses provide the functionality that allows the remote, extranet, and intranet user to access the network. They fully meet the needs of both basic and complex deployments with diverse audiences and use cases, and require little or no client software, server changes, DMZ build-outs, or software agent deployments. And for administrative ease of user license counts, each license only enables as many users as specified in the license and are additive. For example, if a 100 user license was originally purchased and the concurrent user count grows over the next year to exceed that amount, simply adding another 100 user license to the system will now allow for up to 200 concurrent users. Key features enabled by this license include:

- Junos Pulse, SAM and Network Connect provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the SSL transport mode of Junos Pulse and the adaptive dual transport methods of Network Connect. The combination of SAM, Junos Pulse and Network Connect with Core Clientless access provides secure access to virtually any audience, from remote/mobile workers to partners or customers, using a wide range of devices from any network.
- Provision by purpose goes beyond role-based access controls and allows administrators to properly, accurately, and dynamically balance security concerns with access requirements.
- Advanced PKI support includes the ability to import multiple root and intermediate certificate authorities (CAs), Online Certificate Status Protocol (OCSP), and multiple server certificates.
- User self-service provides the ability for users to create their own favorite bookmarks, including accessing their own workstation from a remote location, and even changing their password when it is set to expire.

- Multiple hostname support (for example, https://employees.company.com, https://partners.company.com and https://employees.company.com/engineering) can all be made to look as though users are the only ones using the system, complete with separate logon pages and customized views that uniquely target the needs and desires of that audience.
- User interfaces are customizable for users and delegated administrative roles.
- Advanced endpoint security controls such as Host Checker, Cache Cleaner, and Secure Virtual Workspace work to ensure that users are dynamically provisioned to access systems and resources only to the degree that their remote systems are compliant with the organization's security policy, after which remnant data is scrubbed from the hard drive so that nothing is left behind.
- Provides support of up to 240 VLANs.

Secure Meeting License (Optional)

The Juniper Networks Secure Meeting upgrade license extends the capabilities of the SA Series SSL VPN Appliances by providing secure anytime, anywhere, cost-effective online Web conferencing and remote control PC access. Secure Meeting enables real-time application sharing so that authorized employees and partners can easily schedule online meetings or activate instant meetings through an intuitive Web interface that requires no training or special deployments. Help desk staff or customer service representatives can provide remote assistance to any user or customer by remotely controlling his/her PC without requiring the user to install any software. Best-in-class Authentication, Authorization, and Accounting (AAA) capabilities enable companies to easily integrate Secure Meeting with their existing internal authentication infrastructure and policies. Juniper's market-leading, hardened, and Common Criteria-certified SSL VPN appliance architecture, and SSL/HTTPS transport security for all traffic, means that administrators can rest assured that their Web conferencing and remote control solution adheres to the highest levels of enterprise security requirements.

The Secure Meeting upgrade is available for the SA2500, SA4500, and SA6500.

Instant Virtual System License (Optional)

Juniper Networks Instant Virtual System (IVS) option is designed to enable administrators to provision logically independent SSL VPN gateways within a single appliance/cluster. This allows service providers to offer network-based SSL VPN managed services to multiple customers from a single device or cluster, as well as enabling enterprises to completely segment SSL VPN traffic between multiple groups. IVS enables complete customer separation and provides segregation of traffic between multiple customers using granular role based VLAN (802.1Q) tagging. This enables the secure segregation of end user traffic even if two customers have overlapping IP addresses, and enables provisioning of specific VLANs for different user constituencies such as remote employees and partners of customers.

Domain Name Service (DNS)/Windows Internet Name Service (WINS), AAA, log/accounting servers, and application servers such as Web mail and file shares to name a few, can reside either in the respective customer's intranets or in the service provider network. Service providers can provision an overall concurrent number of users on a per-customer basis with the flexibility to distribute further to different user audiences such as remote employees, contractors, partners, and others. The SA Series extends programmatic support to configure and manage IVS. This enables service providers to integrate IVS management into their own operations support systems (OSS). It also enables enterprises that use Instant Virtual Systems to leverage XML import/export capabilities for management of the individual virtual systems.

The IVS upgrade is available for the SA4500 and SA6500.

High Availability License (Optional)

Juniper Networks has designed a variety of HA clustering options to support the SA Series, ensuring redundancy and seamless failover in the rare case of a system failure. These clustering options also provide performance scalability to handle the most demanding usage scenarios. The SA2500 and SA4500 can be purchased in cluster pairs, and the SA6500 can be purchased in multi-unit clusters or cluster pairs to provide complete redundancy and expansive user scalability. Both multi-unit clusters and cluster pairs feature stateful peering and failover across the LAN and WAN, so in the unlikely event that one unit fails, system configurations (like authentication server, authorization groups, and bookmarks), user profile settings (like user-defined bookmarks and cookies), and user sessions are preserved. Failover is seamless, so there is no interruption to user/enterprise productivity, no need for users to log in again, and no downtime. Multi-unit clusters are automatically deployed in active/active mode, while cluster pairs can be configured in either active/active or active/passive mode.

High availability licenses allow you to share licenses from one SA Series appliance with one or more additional SA Series appliances (depending on the platform in question). These are not additive to the concurrent user licenses. For example, if a customer has a 100 user license for the SA4500 and then purchases another SA4500 with a 100 user cluster license, this will provide a total of 100 users that are shared across both appliances, not per appliance.

The HA option is available for the SA2500, SA4500, and SA6500.

ICE License (Optional)

SSL VPNs can help keep organizations and businesses functioning by connecting people even during the most unpredictable circumstances—hurricanes, terrorist attacks, transportation strikes, pandemics, or virus outbreaks—the result of which could mean the quarantine or isolation of entire regions or groups of people for an extended period of time. With the right balance of risk and cost, the new Juniper Networks SA Series ICE offering delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure business continuity whenever a disastrous event strikes. ICE provides licenses for a large number of additional users on an SA Series SSL VPN Appliance for a limited time. With ICE, businesses can:

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, at any time, and on any device.
- Sustain partnerships with around-the-clock, real-time access to applications and services while knowing resources are secured and protected.
- Continue to deliver exceptional service to customers and partners with online collaboration.
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance.
- Balance risk and scalability with cost and ease of deployment.

The ICE license is available for the SA4500 and the SA6500 and includes the following features:

- Baseline
- Secure Meeting

Antimalware Support with Enhanced Endpoint Security (EES) (Optional)

The amount of newly discovered malicious programs that can harm endpoint devices such as PCs continues to grow. According to the 1985-2008 AV-test.org report, there were over seven million new malware programs discovered in 2008, and just over five million were discovered in 2007. Malware is known to cost enterprises an increasing amount of money every year in terms of efforts involved to quarantine and remediate appropriate endpoints.

In order to prevent endpoints from being infected with malware, Juniper Networks offers the Enhanced Endpoint Security license option. This license is a full-featured, dynamically deployable antimalware module that is an OEM of Webroot's industry-leading Spy Sweeper product. This dynamic antimalware download capability is also available with Unified Access Control. With this new capability, organizations can ensure that unmanaged and managed Microsoft Windows endpoint devices conform to corporate security policies before they are allowed access to the network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before the user enters sensitive information such as their user credentials. The Enhanced Endpoint Security license protects endpoints from infection in real-time and ensures only clean endpoints are granted access to the network. Enhanced Endpoint Security licenses are available as 1-year, 2-year, and 3-year subscription options (see the Ordering Information section for more details).

The Enhanced Endpoint Security option is available for the SA2500, SA4500, and SA6500.

Premier Java RDP Applet (Optional)

Until now, client access software for Microsoft's Terminal Server has been cut-and-dried. Microsoft's Terminal Services client is restricted and can only be used on Windows clients with MS Internet Explorer. With the Premier Java RDP Applet option, users can remotely access centralized Windows applications independently of the client platform (Mac, Linux, Windows, and so on) through Java-based technology.

As a platform-independent solution, the Premier Java RDP Applet lets you use the entire range of Windows applications running on the Windows Terminal Server, regardless of how the client computer is equipped. By centrally installing and managing all the Windows applications, you can significantly reduce your total cost of ownership. The Premier Java RDP Applet is an OEM of the HOBlink JWT (Java Windows Terminal) product created by HOB Inc., a leading European software company specializing in Java programming.

The Premier Java RDP option is available for the SA2500, SA4500, and SA6500.

SA6500

SA2500

SA4500

Specifications

	SA2500	SA4500	SA6500
Dimensions and Power			
Dimensions (W x H x D)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	14.6 lb (6.6 kg) typical (unboxed)	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed)
Rack mountable	Yes, 1U	Yes, 1U	Yes, 2U, 19 inch
A/C power supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 200 W	100-240 VAC, 50-60 Hz, 2.5 A Max, 300 W	100-240 VAC, 50-60 Hz, 2.5 A Max, 400 W
System battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load	80% minimum, at full load
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel	18 gauge (.048 in) cold-rolled steel
MTBF	75,000 hours	72,000 hours	98,000 hours
Fans	Three 40 mm ball bearing fans, one 40 mm ball bearing fan in power supply	Three 40 mm ball bearing fans, one 40 mm ball bearing fan in power supply	Two 80 mm hot swap, one 40 mm ball bearing fan in power supply
Panel Display			
Power LED, HD activity, HW alert	Yes	Yes	Yes
HD activity and fail LED on drive tray	No	No	Yes
Ports			
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)	Four RJ-45 Ethernet – full or half-duplex (auto-negotiation); for link redundancy to internal switches SFP module optional
Management	N/A	N/A	One RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)
Fast Ethernet	IEEE 802.3u compliant	IEEE 802.3u compliant	IEEE 802.3u compliant
Gigabit Ethernet	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant
Console	One RJ-45 serial console port	One RJ-45 serial console port	One RJ-45 serial console port
Environment			
Operating temp	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)
Storage temp	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing
Altitude (operating)	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum
Altitude (storage)	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum
Certifications			
Common Criteria EAL3+ certification	Yes	Yes	Yes
Safety certifications	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001
Emissions certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract	90 days; Can be extended with support contract

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

MODEL NUMBER	DESCRIPTION
SA2500	
Base System	
SA2500	SA2500 Base System
User Licenses	
SA2500-ADD-10U	Add 10 simultaneous users to SA2500
SA2500-ADD-25U	Add 25 simultaneous users to SA2500
SA2500-ADD-50U	Add 50 simultaneous users to SA2500
SA2500-ADD-100U	Add 100 simultaneous users to SA2500
Feature Licenses	
SA2500-MTG	Secure Meeting for SA2500
Clustering Licenses	
SA2500-CL-10U	Clustering: Allow 10 users to be shared from another SA2500
SA2500-CL-25U	Clustering: Allow 25 users to be shared from another SA2500
SA2500-CL-50U	Clustering: Allow 50 users to be shared from another SA2500
SA2500-CL-100U	Clustering: Allow 100 users to be shared from another SA2500
SA4500	
Base System	
SA4500	SA4500 Base System
User Licenses	
SA4500-ADD-50U	Add 50 simultaneous users to SA4500
SA4500-ADD-100U	Add 100 simultaneous users to SA4500
SA4500-ADD-250U	Add 250 simultaneous users to SA4500
SA4500-ADD-500U	Add 500 simultaneous users to SA4500
SA4500-ADD-1,000U	Add 1,000 simultaneous users to SA4500
Feature Licenses	
SA4500-MTG	Secure Meeting for SA4500
SA4500-IVS	Instant Virtual System for SA4500
SA4500-ICE	In Case of Emergency License for SA4500
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500
Clustering Licenses	
SA4500-CL-50U	Clustering: Allow 50 users to be shared from another SA4500
SA4500-CL-100U	Clustering: Allow 100 users to be shared from another SA2500
SA4500-CL-250U	Clustering: Allow 250 users to be shared from another SA4500
SA4500-CL-500U	Clustering: Allow 500 users to be shared from another SA4500

MODEL NUMBER	DESCRIPTION
SA6500	
Base System	
SA6500	SA6500 Base System
User Licenses	
SA6500-ADD-100U	Add 100 simultaneous users to SA6500
SA6500-ADD-250U	Add 250 simultaneous users to SA6500
SA6500-ADD-500U	Add 500 simultaneous users to SA6500
SA6500-ADD-1,000U	Add 1,000 simultaneous users to SA6500
SA6500-ADD-2,500U	Add 2,500 simultaneous users to SA6500
SA6500-ADD-5,000U	Add 5,000 simultaneous users to SA6500
SA6500-ADD-7,500U	Add 7,500 simultaneous users to SA6500
SA6500-ADD-10,000U	Add 10,000 simultaneous users to SA6500
SA6500-ADD-125,00U*	Add 12,500 simultaneous users to SA6500
SA6500-ADD-15,000U*	Add 15,000 simultaneous users to SA6500
SA6500-ADD-20,000U*	Add 20,000 simultaneous users to SA6500
SA6500-ADD-25,000U*	Add 25,000 simultaneous users to SA6500
Feature Licenses	
SA6500-MTG	Secure Meeting for SA6500
SA6500-IVS	Instant Virtual System for SA6500
SA6500-ICE	In Case of Emergency License for SA6500
SA6500-ICE-CL	In Case of Emergency Clustering License for SA6500
Clustering Licenses	
SA6500-CL-100U	Clustering: Allow 100 users to be shared from another SA6500
SA6500-CL-250U	Clustering: Allow 250 users to be shared from another SA6500
SA6500-CL-500U	Clustering: Allow 500 users to be shared from another SA6500
SA6500-CL-1000U	Clustering: Allow 1,000 users to be shared from another SA6500
SA6500-CL-2500U	Clustering: Allow 2,500 users to be shared from another SA6500
SA6500-CL-5000U	Clustering: Allow 5,000 users to be shared from another SA6500
SA6500-CL-7500U	Clustering: Allow 7,500 users to be shared from another SA6500
SA6500-CL-10000U	Clustering: Allow 10,000 users to be shared from another SA6500
SA6500-CL-12500U	Clustering: Allow 12,500 users to be shared from another SA6500
SA6500-CL-15000U	Clustering: Allow 15,000 users to be shared from another SA6500
SA6500-CL-20000U	Clustering: Allow 20,000 users to be shared from another SA6500
SA6500-CL-25000U	Clustering: Allow 25,000 users to be shared from another SA6500

*Multiple SA6500s required

Enhanced Endpoint Security Licenses for SA2500, SA4500, and SA6500

MODEL NUMBER	DESCRIPTION
ACCESS-EES-10U-1YR	Enhanced Endpoint Security subscription, 10 concurrent users, 1-year
ACCESS-EES-25U-1YR	Enhanced Endpoint Security subscription, 25 concurrent users, 1-year
ACCESS-EES-50U-1YR	Enhanced Endpoint Security subscription, 50 concurrent users, 1-year
ACCESS-EES-100U-1YR	Enhanced Endpoint Security subscription, 100 concurrent users, 1-year
ACCESS-EES-250U-1YR	Enhanced Endpoint Security subscription, 250 concurrent users, 1-year
ACCESS-EES-500U-1YR	Enhanced Endpoint Security subscription, 500 concurrent users, 1-year
ACCESS-EES-1000U-1YR	Enhanced Endpoint Security subscription, 1000 concurrent users, 1-year
ACCESS-EES-2500U-1YR	Enhanced Endpoint Security subscription, 2500 concurrent users, 1-year
ACCESS-EES-5000U-1YR	Enhanced Endpoint Security subscription, 5000 concurrent users, 1-year
ACCESS-EES-7500U-1YR	Enhanced Endpoint Security subscription, 7500 concurrent users, 1-year
ACCESS-EES-10U-2YR	Enhanced Endpoint Security subscription, 10 concurrent users, 2-years
ACCESS-EES-25U-2YR	Enhanced Endpoint Security subscription, 25 concurrent users, 2-years
ACCESS-EES-50U-2YR	Enhanced Endpoint Security subscription, 50 concurrent users, 2-years
ACCESS-EES-100U-2YR	Enhanced Endpoint Security subscription, 100 concurrent users, 2-years
ACCESS-EES-250U-2YR	Enhanced Endpoint Security subscription, 250 concurrent users, 2-years
ACCESS-EES-500U-2YR	Enhanced Endpoint Security subscription, 500 concurrent users, 2-years
ACCESS-EES-1000U-2YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 2-years
ACCESS-EES-2500U-2YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 2-years
ACCESS-EES-5000U-2YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 2-years
ACCESS-EES-7500U-2YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 2-years
ACCESS-EES-10U-3YR	Enhanced Endpoint Security subscription, 10 concurrent users, 3-years
ACCESS-EES-25U-3YR	Enhanced Endpoint Security subscription, 25 concurrent users, 3-years
ACCESS-EES-50U-3YR	Enhanced Endpoint Security subscription, 50 concurrent users, 3-years
ACCESS-EES-100U-3YR	Enhanced Endpoint Security subscription, 100 concurrent users, 3-years
ACCESS-EES-250U-3YR	Enhanced Endpoint Security subscription, 250 concurrent users, 3-years
ACCESS-EES-500U-3YR	Enhanced Endpoint Security subscription, 500 concurrent users, 3-years
ACCESS-EES-1000U-3YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 3-years
ACCESS-EES-2500U-3YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 3-years
ACCESS-EES-5000U-3YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 3-years
ACCESS-EES-7500U-3YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 3-years

Premier RDP Applet Licenses for SA2500, SA4500, and SA6500

MODEL NUMBER	DESCRIPTION
ACCESS-RDP-50U-1YR	Java RDP Applet 1-year subscription for 50 simultaneous users
ACCESS-RDP-100U-1YR	Java RDP Applet 1-year subscription for 100 simultaneous users
ACCESS-RDP-250U-1YR	Java RDP Applet 1-year subscription for 250 simultaneous users
ACCESS-RDP-500U-1YR	Java RDP Applet 1-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-1YR	Java RDP Applet 1-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-1YR	Java RDP Applet 1-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-1YR	Java RDP Applet 1-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-1YR	Java RDP Applet 1-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-1YR	Java RDP Applet 1-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-1YR	Java RDP Applet 1-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-2YR	Java RDP Applet 2-year subscription for 50 simultaneous users
ACCESS-RDP-100U-2YR	Java RDP Applet 2-year subscription for 100 simultaneous users
ACCESS-RDP-250U-2YR	Java RDP Applet 2-year subscription for 250 simultaneous users
ACCESS-RDP-500U-2YR	Java RDP Applet 2-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-2YR	Java RDP Applet 2-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-2YR	Java RDP Applet 2-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-2YR	Java RDP Applet 2-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-2YR	Java RDP Applet 2-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-2YR	Java RDP Applet 2-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-2YR	Java RDP Applet 2-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-3YR	Java RDP Applet 3-year subscription for 50 simultaneous users
ACCESS-RDP-100U-3YR	Java RDP Applet 3-year subscription for 100 simultaneous users
ACCESS-RDP-250U-3YR	Java RDP Applet 3-year subscription for 250 simultaneous users
ACCESS-RDP-500U-3YR	Java RDP Applet 3-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-3YR	Java RDP Applet 3-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-3YR	Java RDP Applet 3-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-3YR	Java RDP Applet 3-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-3YR	Java RDP Applet 3-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-3YR	Java RDP Applet 3-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-3YR	Java RDP Applet 3-year subscription for 10,000 simultaneous users

Ordering Information (continued)

MODEL NUMBER	DESCRIPTION
Accessories	
UNIV-CRYPTO	Field upgradeable SSL acceleration module for SA4500
UNIV-PS-400W-AC	Field upgradeable secondary 400 W power supply for SA6500
UNIV-80G-HDD	Field replaceable 80 GB hard disk for SA6500
UNIV-MR2U-FAN	Field replaceable fan for SA6500
UNIV-MR1U-RAILKIT	Rack mount kit for SA2500 and SA4500
UNIV-MR2U-RAILKIT	Rack mount kit for SA6500
UNIV-SFP-FSX	Mini-GBIC transceiver - fiber SX for SA6500
UNIV-SFP-FLX	Mini-GBIC transceiver - fiber LX for SA6500
UNIV-SFP-COP	Mini-GBIC transceiver - copper for SA6500
SA6500-IOC	GBIC I/O card

About Juniper Networks

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

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

1000220-009-EN June 2010

Printed on recycled paper

Product Data Sheet

RSA® Authentication Manager

Enterprise-class security engine for RSA SecurID® authentication

At a Glance

- Enterprise-class two-factor security engine powers the authentication of more than 25 million RSA SecurID® users worldwide
- Scales to meet the needs of small to large enterprises
- Interoperable with more than 350 products from more than 200 vendors at no additional charge
- Enables a flexible array of centrally managed credential methods

Identity Assurance

Identity assurance is the set of capabilities and methodologies that minimize business risk associated with identity impersonation and inappropriate account use. Identity assurance brings confidence to organizations by allowing trusted identities to freely and securely interact with systems and access information, opening the door for new ways to generate revenue, satisfy customers and control costs.

RSA Authentication Manager

RSA Authentication Manager is the de facto standard in identity assurance. The system comprehensively addresses the four capabilities required for identity assurance: credential management and policy, authentication, authorization and intelligence. The RSA Identity Assurance portfolio extends user authentication from a single security measure to a continual trust model that is the basis of how an identity is used and what it can do. Trusted identities managed by RSA bring confidence to everyday transactions and support new business models by providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience.

RSA® Authentication Manager software is the management component of the RSA SecurID® solution. It is used to verify authentication requests and centrally administer user authentication policies for access to enterprise networks. Working in conjunction with RSA SecurID authenticators and RSA® Authentication Agent software, the solution provides two-factor user authentication that protects access to more VPNs, wireless networks, web applications, business applications and operating environments, including the Microsoft® Windows® operating system, than any other system available today.

High Performance and Scalability

RSA Authentication Manager software is designed to fit the needs of organizations of all sizes. Built upon an enterprise-class multi-processor architecture, it is capable of handling tens of thousands of users, as well as hundreds of simultaneous authentications per second. It is deployed in banking, government, manufacturing, retail, high tech and healthcare worldwide, including many small to medium-sized businesses. It is available in two versions: Base Edition and Enterprise Edition.

Database Replication

The database replication feature of the RSA Authentication Manager enables flexible network configuration and load balancing for improved performance that ultimately lowers management costs.

RSA®
The Security Division of EMC

The Base Edition provides one primary server and one replica server. User administration is handled by the primary server and all information is duplicated to the replica. Both servers are capable of handling authentication requests; RSA Authentication Agents balance the work load between servers by detecting response times and directing the request accordingly, to ensure optimum performance.

The Enterprise Edition offers one primary and multiple replicas (up to 5 on the RSA SecurID Appliance; 10 or more on the software release), along with the ability to have up to six separate realms. This provides administrators with the ability to track user authentication to their network anytime in the world in real time, update security policy simultaneously across the worldwide network and develop a global network topology that increases network performance.

Manageability and Control

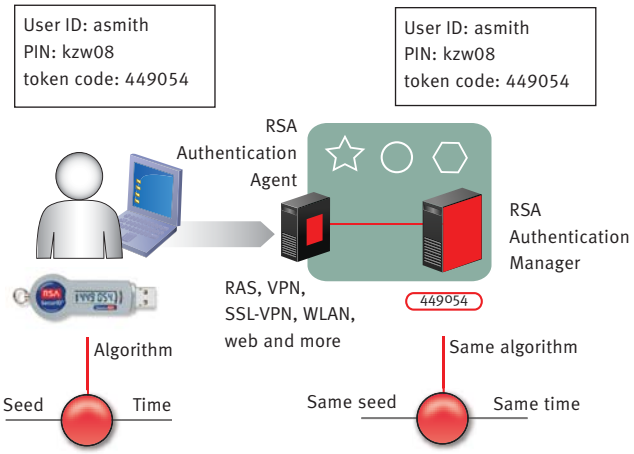
RSA Authentication Manager software offers a high level of management flexibility and control. There is no desktop admin software to install; a built-in web server allows for access to the management console from any web browser. The included Juniper® Steel Belted RADIUS server is similarly managed from completely within the intuitive, easy-to-navigate administration console.

Native LDAP integration enables RSA Authentication Manager to point to a single authoritative data store in real time for user and group information. Supported identity sources include Microsoft Active Directory® or Sun One™, and no schema changes are required to the underlying database infrastructure. A Microsoft Management Console snap-in supports manipulation of user records directly from an MMC interface.

Both the Base and Enterprise Editions include RSA® Credential Manager, a completely integrated software module that enables user self service (Base and Enterprise) and workflow provisioning (Enterprise only) to dramatically speed the on-boarding of users to their credentials.

Auditing and Reporting

Because RSA Authentication Manager logs all transactions and user activity, administrators can utilize it as an auditing, accounting and compliance tool. It includes report templates that can be easily tailored to administration needs, including activity, exception, incident and usage summaries. In addition to the reporting capabilities the product supports a live activity monitor that shows all or administrator-selected activity across a global deployment.



RSA SecurID Time-synchronous Two-factor Authentication

Array of Credentialing Methods

RSA Authentication Manager supports authenticators in a variety of form factors from the traditional hardware tokens to software-based tokens that install on PCs and smart phones, to the On-demand Authenticator that delivers one-time token codes using Short Message Service (SMS) or e-mail. All of these credentials are centrally managed from a common interface.

Turnkey Interoperability

RSA Authentication Manager is interoperable with many of the major network infrastructure and operating system products on the market - including more than 350 products from over 200 vendors – providing an organization with maximum flexibility and investment protection. Leading vendors of remote access products, VPNs, firewalls, wireless network devices, web servers and business applications have built in support for RSA Authentication Manager.

RSA®
The Security Division of EMC

www.rsa.com

SIDAM_DS_0710

Product Data Sheet

RSA SecurID® 700 Authenticator

Convenient, reliable and secure choice for two-factor authentication

At a Glance

- Convenient keyfob form factor is easy for users to carry and use
- High-quality solution combined with a lifetime warranty creates a reliable choice
- Advanced time-based algorithm and tamper-evident body ensures secure authentication

The RSA SecurID 700 authenticator is the most popular form factor in the SecurID authenticator portfolio offered by RSA, the Security Division of EMC, due to its convenience, reliability and security. Thousands of organizations worldwide rely upon the SecurID 700 to protect valuable network and customer resources. Used in conjunction with RSA® Authentication Manager, the SecurID 700 adds an additional layer of security by requiring users to identify themselves with two unique factors – something they know, a PIN, and something they have, a unique one-time password (OTP) that changes every 60-seconds – before they are granted access to the secured application.

Convenient Form Factor

With its robust key ring, small size and easy-to-read LCD display, the SecurID 700 is a convenient form factor for employees, partners and customers. Loss of the authenticator is minimized as it easily fits on a ring of keys or in a pocket or purse. Users can easily read the OTP displayed on the authenticator and know when the number is going to change by watching the countdown indicator. The SecurID 700 is convenient for IT managers too, as it comes pre-seeded and is ready-to-use out-of-the-box. It is integrated with over 350 certified third-party applications, helping to lower deployment costs by providing the assurance that important applications are "RSA SecurID Ready." The SecurID 700 can also be customized with company artwork to reinforce the issuer's brand.

Reliable Authentication Solution

The SecurID 700 authenticator is designed to withstand the worst imaginable conditions, offering industry-leading reliability. From temperature cycling to mechanical shocks to being immersed in water, the SecurID 700 is subjected to rigorous tests to ensure that customers do not face hidden costs due to token failures. The combination of this high-level of quality with a lifetime warranty allows organizations to reduce the overhead costs of distributing replacement tokens and drive down the overall cost of security while providing a consistent and easy-to-use authentication experience for end-users.

Strong Security

The SecurID 700 offers a time-based OTP solution that ensures a strong level of security. It has a unique symmetric key that is combined with a proven algorithm to generate a new one-time password every 60 seconds. RSA technology synchronizes each authenticator with the security server, ensuring a high level of security. The one-time password, something you have, is coupled with a secret personal identification number (PIN), something you know, to create a combination that is nearly impossible for a hacker to guess. The SecurID 700 is also tamper evident, meaning that if someone opened the token for nefarious purposes, it would be evident to the user of the device.

The RSA SecurID 700 authenticator is a smart choice for companies that are looking for a convenient, reliable and secure authentication solution. Its use by millions of users world-wide for secure access to enterprise and consumer applications demonstrates that the SecurID 700 is a proven solution that can be counted on to protect your organization's resources.

RSA®

The Security Division of EMC

Environmentally friendly

In an effort to help preserve the environment, RSA reuses almost 100% of all returned authenticators. Customers can send the authenticator back to RSA and RSA will recycle the token at no additional charge.

Technical Specifications

Height: 20mm; 27mm at highest point

Width: 68mm

Thickness: 9mm

Weight: 15 grams

Materials: Plastic – ABS

Power: 3v Lithium (Coin cell)

Display: Liquid Crystal (LCD)

Server support: RSA Authentication Manager 5.1 or higher; RSA SecurID Authentication Engine

Operating temperature: -15°C to 60°C

Lifetime: Purchased in increments of 24, 36, 48, or 60 months

Warranty: Lifetime warranty

Tamper evidence: Conforms to ISO 13491-1; ISO DIS 13491-2:2005

Product safety standards: RoHS, WEEE, CE, cRoHS,

Regulatory standards: FCC Part 15 Class A and Class B, EN55022 Class A and Class B

RSA
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

SID700 DS 0709

ANEXO 3: Hojas Técnicas de los productos que participaron en el proceso de selección

Se presenta en este anexo las hojas técnicas de los productos, equipos y software, que participaron del proceso de selección de componentes para la solución de seguridad propuesta.

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

CHECK POINT
SECURITY APPLIANCES

More. Better. Simpler Security℠

Table of Contents

Introduction

Check Point appliances deliver a powerful turnkey solution for deploying Check Point award-winning software solutions to address virtually any security need. Based on the new Check Point Software Blade architecture, Check Point appliances provide the highest level of flexibility, scalability, and extensibility in the industry. All Check Point appliances are built around a unified security architecture, enabling organizations to perform all aspects of security management via a single, unified console. With Check Point appliances, organizations of all sizes can tailor their network security infrastructure to meet their functional and performance needs—with centralized management, simple deployment, and full extensibility.

CHECK POINT APPLIANCE OPTIONS

Check Point offers the following appliance options to effectively deliver comprehensive security applications:

- **Dedicated Appliances**—Check Point dedicated hardware platforms devoted to a single security application such as intrusion prevention (IPS) and data loss prevention (DLP). Dedicated appliances provide hardware resources for a single application, delivering higher performance.

- **Integrated Appliances**—Check Point integrated appliances take an all-in-one approach, combining multiple security applications on a single enterprise-class platform. Because applications are consolidated within a unified security architecture, organizations can reduce TCO and simplify security configuration.

- **Bladed Hardware**—Check Point bladed hardware platforms include a chassis with multiple hardware blades that run independent security applications. Each blade is equivalent to an independent server or appliance, and contains dedicated resources for each security application. Bladed hardware platforms deliver built-in failover and load-balancing utilities, as well as an increase in system performance.

UTM-1 Appliances

All inclusive. All secured.

OVERVIEW

UTM-1™ appliances offer the ideal combination of proven security technologies and easy-to-use deployment and management features. With a full line of hardware-based solutions, Check Point UTM-1 appliances consolidate key security applications such as firewall, VPN, intrusion prevention, and antivirus and more into a single, easy-to-manage solution. UTM-1 Appliances are based on the Check Point Software Blade architecture that enables flexible and fast deployment of additional security capabilities, such as VoIP protections, without the addition of new hardware.

UTM-1 appliances deliver a comprehensive set of security features including firewall, intrusion prevention, antivirus, anti-spyware, anti-spam, Web filtering, Web application security—as well as secure site-to-site and remote access connectivity. **UTM-1 Edge**™ family of appliances deliver integrated firewall, intrusion prevention, VPN, and antivirus for branch offices of up to 100 users, ensuring small offices stay as secure as the corporate office.

BENEFITS

- Industry-leading application- and network-layer firewall
- Site-to-site and remote-access VPNs
- Gateway antivirus and anti-spyware
- Intrusion prevention with type-based protections and security updates
- Web security with URL filtering and integrated security for Web applications
- Email security and anti-spam, including the Check Point six dimensions of comprehensive messaging security
- Software Blade architecture for fast and flexible deployment of new security services

UTM-1 appliances come in six models and **UTM-1 Edge** family of appliances consists of X-Series and N-Series models. UTM-1 Edge X-Series appliances come in four models and UTM-1 Edge N-Series appliances come in two models that let organizations choose the right solution to meet price and performance requirements.

UTM-1 Edge N-Series

UTM-1 130

UTM-1 3070

For more information: www.checkpoint.com/products/utm

Series 80 Appliance

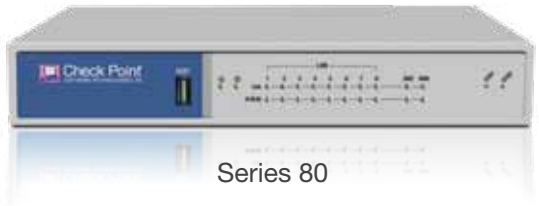
Enterprise-grade branch office security

OVERVIEW

The **Series 80 Appliance** sraises the bar on remote and branch office security by extending Software Blades to the edge of the network—delivering enterprise-grade security in a high-performance desktop form factor. The Series 80 appliance delivers IPsec/SSL VPN and the same industry-proven firewall technology that secures the Global 100—all right out-of-the box. Based on the Check Point Software Blade architecture, the Series 80 appliance enables flexible, single-click upgrades of additional security capabilities, including IPS, antivirus and anti-malware, anti-spam and email security, and URL filtering. And, the Series 80 can be easily configured, deployed and managed without the need for corporate IT staff.

BENEFITS

- Delivers flexible and manageable enterprise-grade security for branch offices
- Includes Best-in-Class Integrated Firewall and IPsec/SSL VPN
- Provides the best price/performance in its class with proven throughput of 1.5 Gbps for firewall, 220 Mbps for VPN and 720 Mbps for IPS
- Protects against emerging threats with optional Software Blades such as IPS, antivirus, email security, and more
- High port density provides enhanced performance and minimizes the overhead of switches and routers in remote environments
- New intuitive and fast start-up wizard allows hassle-free configuration, deployment and management
- Centrally managed by SmartCenter and Provider-1



Series 80

Series 80

Power-1 Appliances

Security for high-performance environments

OVERVIEW

Check Point Power-1™ appliances enable organizations to maximize security in high-performance environments such as large campuses or data centers. They combine integrated firewall, IPsec VPN, and intrusion prevention with advanced acceleration and networking technologies, delivering a high-performance security platform for multi-Gbps environments. The Check Point Software Blade architecture enables flexible and fast deployment of additional security capabilities, such as VoIP protections and UTM functionality, on Power-1 appliances.

BENEFITS

- Streamlines deployment of enterprise security for large offices and data centers
- Ensures availability of business-critical applications with up to 30 Gbps firewall throughput and up to 15 Gbps intrusion prevention throughput
- Provides comprehensive security including Firewall, IPS, IPsec VPN, Advanced Networking, and Acceleration & Clustering Software Blades
- Protects against emerging threats with optional Software Blades such as VoIP, Web Security, Antivirus, and more
- Simplifies administration with a single management console for all sites
- Power-1 11000 series adds performance extensibility via field upgradeability and enables customers to boost performance by 100% from lowest to highest model

Power-1 appliances, which include **Power-1 5075**, **Power-1 9075**, and the **Power-1 11000** series, let organizations choose the proper levels of performance and port density for their environments.

Power-1 5075

Power-1 9075

Power-1 11000 series

For more information: www.checkpoint.com/products/power-1

IP Appliances

Flexible networking and performance options

OVERVIEW

Proven for years in complex networking and performance-demanding environments, **Check Point IP** appliances offer customers integrated turnkey security functionality such as firewall, VPN, and intrusion prevention across a wide range of models. Optimized for Check Point Security Gateway software, the IP appliances offer unsurpassed scalability, high performance, manageability, and high port densities that reduces operational costs in complex, mission-critical security environments. IP appliances enable customers to extend a unified security architecture from the network core out to branch and remote offices.

IP295

IP695

IP2455

BENEFITS

- Integrated security appliances based on Check Point Software Blade architecture for fast, flexible deployment of security functionality
- Scalable, modular, and configurable security architecture with multiple acceleration (ADP service modules), security, and interface options insures investment protection
- Achieve high performance across a broad spectrum of traffic types
- Enterprise-class high availability, scalability, and fault tolerance to insure network resiliency and business continuity
- Carrier-grade serviceability and redundancy
- Streamlined IT efficiency with advanced management tools for installation, configuration, and maintenance

IP appliances come in six models that deliver security solutions ideal for large enterprises, carrier-grade networks and remote and branch offices.

Accelerated Data Path (ADP) for IP Appliances

For more information: www.checkpoint.com/products/ip-appliances

VSX-1 Appliances

Virtualized security

OVERVIEW

The **VSX-1**™ appliances are virtualized security gateways that enable the creation of hundreds of security systems on a single hardware platform, delivering deep cost savings and infrastructure consolidation. Based on the proven security of VPN-1® Power™, VSX provides best-in-class firewall, VPN, URL filtering, and intrusion-prevention technology to multiple networks, securely connecting them to each other and shared resources such as the Internet and DMZs. All security systems, virtual and real, are centrally managed through Check Point SmartCenter™ or Provider-1® management consoles.

Ideal for MSPs, VSX-1 becomes the ideal platform for new subscription revenue opportunities by delivering new security services easily and efficiently.

BENEFITS

- Unique and comprehensive virtualized security solution with firewall, VPN, IPS, and URL filtering
- Consolidates from five to hundreds of security gateways on a single device, increasing device utilization and reducing power, space, and cooling
- Linear scalability with performance up to 27 Gbps
- Flexible deployment options including software and a full line of turnkey appliances
- Single proven security management architecture

VSX-1 appliances come in three models that allow organizations to choose the right solution for their performance and scalability needs.

VSX-1 3070

VSX-1 9070

VSX-1 9090

For more information: www.checkpoint.com/products/vpn-1_power_vsx

DLP-1 Appliances

Check Point makes DLP work

OVERVIEW

Check Point DLP-1™ solves the longstanding problem with data loss prevention technology—enabling organizations to effectively protect sensitive company and customer data, without placing an additional burden on your scarce IT resources. Check Point DLP combines state-of-the-art prevention and enforcement with end user remediation capabilities, for the ideal blend of security and usability.

UserCheck™, Check Point's unique user remediation function, educates users on self-incident handling and corporate data policies, while empowering them to remediate events in real-time. Files that are sent or uploaded to the web are processed by Check Point MultiSpect™, a multi-data classification engine that inspects traffic flow for all data-in-motion, and provides high accuracy in correlating users, data types, and processes.

BENEFITS

- Easily defines data policies while assuring consistent enforcement across the entire network
- Prevents data loss by inspecting traffic in real-time, and proactively blocking the transmission of sensitive information
- Includes more than 250 pre-defined best-practices policies and rules for easy administration
- High performance from 700Mbps to over 2.5Gbps
- Centralized Check Point management for unprecedented visibility and control
- Open scripting language to create customized data types for easily extensible and granular prevention

DLP-1 2571

DLP-1 9571

For more information: www.checkpoint.com/products/dlp

Smart-1 Appliances

Extensible security management

OVERVIEW

Smart-1 appliances deliver Check Point's market leading security management software blades on a dedicated hardware platform specifically designed for mid-size and large enterprise security networks. Based on Check Point's software blade architecture, the line of four Smart-1 appliances are first to deliver a unified management solution for network, IPS and endpoint security with unsurpassed extensibility.

BENEFITS

- Provides a comprehensive set of security management Software Blades in four turnkey security management appliances
- Maximize efficiency with a single unified management console for network and endpoint security
- Reduce costs and conserve resources with up to 12 TB of integrated storage capabilities
- Ensure operational continuity for the most demanding environments
- Simplify large scale security policy provisioning with multi-domain management (Provider-1)

Smart-1 150: Security management for large service providers with more than 150 gateways and including up to 12 TB of integrated log storage

Smart-1 50: Security management for enterprises and service providers with 50 to 150 gateways, including up to 4 TB of integrated log storage

Smart-1 25: Security management for enterprises with 25 to 50 gateways, including up to 2 TB of integrated log storage

Smart-1 5: Security management for businesses with 5 to 25 gateways including up to 500 GB of integrated log storage

Smart-1 5

Smart-1 50

Smart-1 150

For more information: www.checkpoint.com/products/smart-1

Smart-1 SmartEvent Appliances

Unified security event management

OVERVIEW

Smart-1 SmartEvent appliances deliver Check Point's SmartEvent Software Blade event management software blades on a dedicated hardware platform. Smart-1 SmartEvent appliances are specifically designed for mid-size and large enterprise security networks, providing comprehensive security event analysis in a turnkey, plug-and-play appliance. Based on Check Point's software blade architecture, Smart-1 SmartEvent appliances are first to deliver a unified event management solution for network, IPS and endpoint security with unsurpassed extensibility.

BENEFITS

- Provides a comprehensive set of security management Software Blades in three turnkey security management appliances
- Maximize efficiency with a single unified management console for network and endpoint security event management
- Reduce costs and conserve resources with up to 4 TB of built-in storage capabilities
- Ensure operational continuity for the most demanding environments

Smart-1 SmartEvent 50: Security Management for enterprises that need maximum flexibility, high performance and up to 2 years of log storage

Smart-1 SmartEvent 25: Security Management for enterprises that want maximum flexibility and up to 1 year of log storage

Smart-1 SmartEvent 5: Security Management for businesses that want an affordable solution that can scale as their business grows

Smart-1 SmartEvent 5

Smart-1 SmartEvent 25

Smart-1 SmartEvent 50

For more information: www.checkpoint.com/products/smartevent

Check Point Integrated Appliance Solutions

Integrated hardware and software from Check Point and IBM

OVERVIEW

Check Point Integrated Appliance Solutions (IAS) provide organizations with the ultimate choice in appliances—integrated software and hardware bundles customized to their exact specifications. These customized platforms enable them to provision security services based on exact corporate needs.

Organizations can choose from Check Point Software Blades such as firewall, IPSec VPN, and intrusion prevention, and additional blades including UTM functionality. They can also chose to deploy Check Point's virtualized security gateway, VPN-1 Power VSX™, as well as Provider-1 for management of large deployments with separate security domains.

Check Point integrates the selected software onto an IBM System x™ server or IBM BladeCenter® to provide a comprehensive solution that includes direct technical support from Check Point

BENEFITS

- Provides a software/hardware combination trusted by the largest organizations in the world
- Reduces complexity by ensuring compatibility of the latest certified components and servers
- Increases flexibility for security services provisioning by allowing customers to choose from multiple Check Point solutions
- Delivers scalable performance and port density based on customer needs
- Protects against emerging threats with service-based Check Point Software Blades including IPS, Antivirus, Anti-Malware, and URL Filtering

M series Integrated Appliance Solutions are predefined models that can be customized to meet specific needs. The **M2** model delivers UTM functionality. The **M6** and **M8** models both provide maximum security for high-performance environments with integrated firewall, VPN, and intrusion prevention.

Check Point® SOFTWARE TECHNOLOGIES LTD.

IBM

IAS M8

For more information: www.checkpoint.com/products/ias

Integrated Appliance Solution Bladed Hardware

Customized security with superior network performance

OVERVIEW

Check Point Integrated Appliance Solution (IAS) Bladed Hardware provides a customized, integrated security solution on a single, high-performance chassis. By integrating essential Check Point Security Gateway Software Blades with Crossbeam's X-Series carrier-grade chassis, IAS Bladed Hardware can effectively serve the needs of the most demanding, highest performance environments. Alternatively, the VPN-1 Power VSX provides a dedicated gateway for multi-layer, multi-domain virtualized security. Leveraging the Check Point Software Blade Architecture, IAS Bladed Hardware provides customized security solutions to meet specific customer needs—including unified management of physical and virtual environments.

BENEFITS

- Provides a customized, integrated security solution on a single, high-performance chassis
- Integrates best-in-class award-winning security software blades with carrier-grade chassis for a comprehensive security solution
- Enables true performance scalability, with up to 40Gbps firewall throughput
- Increases flexibility for security services provisioning by allowing customers to choose from multiple Check Point solutions
- Provides a single point of contact for hardware, software, and support

With Check Point **IAS Bladed Hardware**, customers can choose among two hardware chassis and two security software bundles for a customized solution that best fits their individual needs. The Crossbeam X80 hardware chassis provides scalability and performance, while the X45 chassis provides performance in a space-saving design. The Check Point Security Gateway SG805 software bundle is designed for physical environments, while the VPN-1 Power VSX provides a virtualized security solution.

Crossbeam X80

For more information: www.checkpoint.com/products/ias-bladed-hardware

Check Point Integrated Appliance Solutions

Integrated hardware and software from Check Point and HP ES

OVERVIEW

Check Point Integrated Appliance Solutions (IAS) D-Series Appliances provide organizations to create customized security solution—integrated software and hardware—built on a baseline set of standardized platforms for delivery of security services. This choice allows organizations to combine the proven security of Check Point on high performance-oriented platforms with a single point of contact for fulfillment and support of all issues.

Organizations can customize their security solution using Check Point Software Blades such as firewall, IPSec VPN, and intrusion prevention, advanced networking and more. Organizations can also chose to deploy Check Point's virtualized security gateway, VPN-1 Power VSX™, Provider-1 for management of large deployment with separate security domains, End Point Suite POINTSEC.

BENEFITS

- Provides a customized security software and hardware bundle on high performance-oriented platforms
- Allows customers to extend security by simple software blades upgrade
- Delivers high firewall performance of up to 20 Gbps based on customer needs
- Increases flexibility for security services provisioning by allowing customers to choose from multiple Check Point solutions
- Provides a single point of contact for hardware, software and support

D-Series Integrated Appliance Solutions are predefined models that can be customized to meet specific needs. There are eleven (11) models to choose from to meet your security needs. The VSX and VSLS provides virtualized security solution and the UTM models deliver UTM functionality.

D8

Appliance Specifications

UTM-1 Series

	UTM-1 Edge	UTM-1 Edge N-Series	UTM-1 130	UTM-1 270	UTM-1 570	UTM-1 1070	UTM-1 2070	UTM-1 3070
Models	UTM-1 Edge X, UTM-1 Edge W, UTM-1 Edge X ADSL, UTM-1 Edge W ADSL	UTM-1 Edge N UTM-1 Edge NW	UTM-1 132 UTM-1 136	UTM-1 272 UTM-1 276	UTM-1 572 UTM-1 576	UTM-1 1073 UTM-1 1076	UTM-1 2073 UTM-1 2076	UTM-1 3073 UTM-1 3076
Software Edition	Embedded NGX	Embedded NGX	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71
10/100 Ports	6	-	1	-	-	-	-	-
10/100/1000 Ports	-	6	4	4	6	6	8	10
Firewall Throughput	190 Mbps	1.0 Gbps	1.5 Gbps	1.5 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps	4.5 Gbps
VPN Throughput	35 Mbps	200 Mbps	120 Mbps	120 Mbps	300 Mbps	350 Mbps	450 Mbps	1.1 Gbps
Concurrent Sessions	8,000	60,000	600,000	600,000	650,000	1.1 million	1.1 million	1.1 million
IPS Throughput	5 Mbps	30 Mbps	1.0 Gbps	1.0 Gbps	1.7 Gbps	2.2 Gbps	2.7 Gbps	4 Gbps
Licensed Users	8/16	32/Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
VLANs	32	64	1,024[1]	1,024[1]	1,024[1]	1,024[1]	1,024[1]	1,024[1]
UTM Out of the Box	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Security Acceleration	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Multisite Management	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Storage	-	-	80 GB	160 GB	160 GB	160 GB	160 GB	160 GB
Form Factor	Desktop	Desktop	Desktop/1U	1U	1U	1U	1U	1U
Dimensions (standard)	8 x 1.2 x 4.8 in.	8 x 1.2 x 4.8 in.	10.6 x 5.7 x 1.6 in.	16.8 x 10 x 1.73 in.	16.8 x 10 x 1.73 in.	16.8 x 10 x 1.73 in.	17.4 x 15 x 1.73 in.	17.4 x 15 x 1.73 in.
Dimensions (metric)	203.2 x 30.5 x 122mm	203.2 x 30.5 x 122mm	270 x 145 x 40mm	429 x 255 x 44mm	429 x 255 x 44mm	429 x 255 x 44mm	443 x 381 x 44mm	443 x 381 x 44mm
Weight	0.7kg (1.6 lbs.)	0.7kg (1.6 lbs.)	1.6kg (3.52 lbs.)	3.7kg (8.1lbs.)	3.7kg (8.1 lbs.)	3.7kg (8.1 lbs.)	6.5kg (14.3 lbs.)	6.5kg (14.3 lbs.)
Operating Environment	Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m[2]							
Power Input	100/240V, 50/60Hz							
Power Supply Spec (Max)	18W	18W	60W	65W	65W	65W	250W	250W
Power Consumption (Max)	-	-	46.9W	26.2W	41.1W	40.1W	63.1W	77.5W
Compliance	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3; AS/NZS 3548:1995; CNS 13438 Class A (test passed; country approval pending); KN22, KN61000-4 Series, TTA; IC-950; ROHS							

[1] Maximum of 256 VLANs per interface
[2] UTM-1 Edge operating environment: Temperature: 0° to 40° C, Humidity: 10%–90% non-condensing, Altitude: 4500m (15,000ft)

Appliance Specifications

Series 80

	Series 80
Software Edition	R71
10/100/1000 Ports	10
Firewall Throughput	1.5 Gbps
VPN Throughput	220 Mbps
Concurrent Sessions	150,000
IPS Throughput	720 Mbps
Licensed Users	Unlimited
VLANs	1024
AV Throughput	100 Mbps
Disk or Flash Based	Flash
Enclosure	Desktop
Dimensions (standard)	8.75 x 1.75 x 6 in.
Dimensions (metric)	220 x 44 x 152.4mm
Weight	3.6kg (8 lbs.)
Operating Environment	Temperature: 0° to 40° C; Humidity: 5% to 95% non-condensing
Power Input	100/240V, 50/60Hz, 240W
Power Supply Spec (max)	12V/2A DC 24W
Power Consumption (max)	16.68W
Compliance	EMC: EN55022+24_2007-ITE; FCC: FCCP15B+ICES-003-ITE; Safety: UL/c-UL 60950-1_2nd_2007(US+CA); IEC 60950_1_2nd_2005-CB

Appliance Specifications

Power-1 Series

	Power-1 5075	Power-1 9075	Power-1 11000 Series		
			11065	11075	11085
Software Edition	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71
10/100/1000 Ports	10/14	14/18	14/18	14/18	14/18
10Gb Ports	2 Optional	4 Optional	4 Optional	4 Optional	4 Optional
Firewall Throughput[1]	9 Gbps	16 Gbps	15 Gbps	20 Gbps	30 Gbps
VPN Throughput[1]	2.4 Gbps	3.7 Gbps	3.7 Gbps	4 Gbps	4.5 Gbps
Concurrent Sessions	1.2 million	1.2 million	1.2 million	1.2 million	1.2 million
IPS Throughput[1]	7.5 Gbps[2]	10 Gbps[2]	10 Gbps[2]	12 Gbps[2]	15 Gbps[2]
Licensed Users	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
VLANs	1,024[3]	1,024[3]	1,024[3]	1,024[3]	1,024[3]
UTM Out of the Box	Optional	Optional	Optional	Optional	Optional
Security Acceleration	Yes	Yes	Yes	Yes	Yes
Integrated Multigateway Management	-	-	-	-	-
Storage	160 GB	2 x 160 GB	2 x 250 GB	2 x 250 GB	2 x 250 GB
Enclosure	2U	2U	2U	2U	2U
Dimensions (standard)	17 x 20 x 3.46 in.	17 x 20 x 3.46 in.	17 x 22.8 x 3.46 in.	17 x 22.8 x 3.46 in.	17 x 22.8 x 3.46 in.
Dimensions (metric)	431 x 509.5 x 88mm	431 x 509.5 x 88mm	431 x 580 x 88mm	431 x 580 x 88mm	431 x 580 x 88mm
Weight	14.5kg (31.9 lbs.)	16.5kg (36.3 lbs.)	23.4kg (51.6 lbs.)	23.4kg (51.6 lbs.)	23.4kg (51.6 lbs.)
Operating Environment	Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m				
Power Input	100/240V, 50/60Hz[4]				
Power Supply Spec (max	250W	400W	500W	500W	500W
Power Consumption (max)	164.1W	200.7W	253.2W	253.2W	253.2W
Compliance	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Class A (test passed; country approval pending); KN22KN61000-4 Series, TTA; IC-950; ROHS				

[1] Performance data represents the maximum capabilities of the systems as measured under optimal testing conditions. Deployment and policy considerations may impact performance results.
[2] Test based on real-world traffic blend using the default profile
[3] Maximum of 256 VLANs per interface
[4] Redundant power supply

Appliance Specifications

IP Series

	IP282	IP295	IP395	IP565	IP695	IP1285	IP2455
Software Edition	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71	R65, R70, R71
10/100/1000 Ports	6	6/8	4/8	4/12	4/16	4/28	4/32
10 GbE Ports	-	-	-	-	6[1]	10[1]	10[1]
Firewall Throughput	1.5Gbps	1.5 Gbps	3.0 Gbps	7 Gbps	7.2/11.7 Gbps[2]	10.3/17.5 Gbps[2]	11/30 Gbps[2]
VPN Throughput	1.0 Gbps	1.0 Gbps	677 Mbps	1.7 Gbps	1.9/ 3.3 Gbps[2]	1.9/8.3 Gbps[2]	1.9/8.3 Gbps[2]
Concurrent Sessions	900,000	900,000	1 million	1 million	1 million	1 million	1 million
IPS Throughput	1.4 Gbps	1.4 Gbps[3]	2.9 Gbps[3]	2.9 Gbps[3]	4 Gbps[3]	7 Gbps[3]	9 Gbps[3]
VLANs	1024[4]	1024[4]	1024[4]	1024[4]	1024[4]	1024[4]	1024[4]
ADP Module	-	-	-	-	Optional	Optional	Optional
VPN Acceleration	Optional	Optional	Included	Included	Included	Included	Included
Storage	40GB	40 GB	80 GB	80 GB	80 GB	80 GB	80 GB
Disk-Based or Flash	Disk	Disk or Flash	Disk or Flash	Disk or Flash	Disk or Flash	Disk or Flash	Disk or Flash
Enclosure	1U/half rack	1U/half rack	1U	1U	1U	2U	2U
Dimensions (standard)	8.52 x 18 x 1.71 in	8.52 x 18 x 1.71 in.	17 x 16 x 1.71 in.	17.23 x 22 x 1.71 in.	17.23 x 24 x 1.71 in.	17.23 x 24.11 x 3.46 in.	17.23 x 24.11 x 3.46 in.
Dimensions (metric)	216 x 457 x 44 mm	216 x 457 x 44mm	432 x 406 x 44mm	438 x 559 x 44mm	438 x 610 x 44mm	438 x 613 x 88mm	438 x 613 x 88mm
Weight	5.1kg (11.25 lbs)	5.1kg (11.25 lbs)	7.71kg (17.0 lbs)	11.84kg (26.1 lbs)	12.38kg (27.3 lbs)	19.6kg (43.2 lbs)	20.57kg (45.35 lbs)
Operating Environment	Temperature: 5° to 40° C[5]; Humidity: 10% to 85% non-condensing; Altitude: 2,500m						
Power Input	100/240V, 50/60Hz						
Power Supply Spec (max)	133W	133W	150W	225W	250W	700W	700W
Power Consumption (max)	-	-	100W	165W	-	-	-
DC Power Supply	-	-	-	-	-	Optional	Optional
Compliance	Safety: UL60950-1, First Edition: 2003, CAN/CSAC22.2, No 60950:2000, IEC60950-1: 2001, EN60950-1:2001+A11 with Japanese National Deviations; Emission Compliance: FCC Part 15, Subpart B, Class A, EN50024,EN55022A: 1998, CISPR 22 Class A: 1985, EN61000-3-2, EN61000-3-3; Immunity: EN55024: 1998						

[1] Optional
[2] Performance without ADP/with ADP
[3] Preliminary results
[4] Maximum of 256 VLANs per interface
[5] IP395 can go to 50° C

Appliance Specifications

VSX-1 Series

	VSX-1 3070	VSX-1 9070	VSX-1 9090
Software Edition (VSX Version)	R65	R65	R65
10/100/1000 Ports	10	14/18	28/36
Firewall Throughput	4.5 Gbps	13.5 Gpbs	27 Gpbs
VPN Throughput	1.1 Gbps	3.5 Gbps	7 Gpbs
Concurrent Sessions	1 million	1.1 million	1.8 million
Licensed Users	Unlimited	Unlimited	Unlimited
VLANs	4096	4096	4096
Virtual Systems (included/capacity)	5/10	10/150	10/150
UTM Out of the Box	Optional	Optional	Optional
Security Acceleration	Yes	Yes	Yes
Multisite Management	Optional[1]	Optional[1]	Optional[1]
Storage	160 GB	2 x 160 GB	4 x 160 GB
Enclosure	1U	2U	4U
Dimensions (standard)	17.4 x 15 x 1.73 in.	17 x 20 x 3.46 in.	17 x 20 x 7 in.
Dimensions (metric)	443 x 381 x 44mm	431 x 509.5 x 88mm	431 x 509.5 x 176mm
Weight	6.5kg (14.3 lbs.)	16.5kg (36.3 lbs.)	33kg (72.6 lbs.)
Operating Environment	Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m		
Power Input	100/240V, 50/60Hz		
Power Supply Spec (max)	250W	400W	800W
Power Consumption (max)	77.5W	200.7W	400.5W

[1] Management server resides on separate server

Appliance Specifications

DLP-1 Series

	DLP-1 2571	DLP-1 9571
Software Edition	R71	R71
Number of Users	1000	5000
Messages/Hour	70,000	350,000
Throughput	700 Mbps	2.5 Gbps
Built-in Interfaces	6 Copper 1 GbE	10 Copper 1 GbE
Optional Interfaces	Built-in 4-Port Copper Bypass Card	LOM, 2x4 1 GbE Fiber, 2x4 1GbE Copper, 2x2 10 GbE, Modular 4-Port Copper Bypass Card
Storage Size	500GB	2x2TB (Mirrored – RAID 1)
Enclosure	1U	2U
Dimensions (standard)	17.4 x 15 x 1.73 in.	17 x 20 x 3.46 in.
Dimensions (metric)	443 x 381 x 44mm	431 x 509.5 x 88mm
Weight	6.5kg (14.3 lbs.)	16.5kg (36.3 lbs.)
Dual, Hot-Swappable Power Supplies	No	Yes
Power Input	100/240V, 50/60Hz	
Power Supply Spec (max)	250W	400W
Power Consumption (max)	77.5W	200.7W
Operating Environment	Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m	
Compliance	UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3AS/NZS 3548:1995; CNS 13438 Class A (test passed; country approval pending); KN22KN61000-4 Series, TTA; IC-950; ROHS	

Appliance Specifications

Smart-1 Series

	Smart-1 5	Smart-1 25	Smart-1 50	Smart-1 150
Software Edition	R65, R70	R65, R70	R65, R70	R65, R70
Managed Gateways	5 up to 25	25 up to 50	50 up to 150	150 up to unlimited
Managed Domains	-	-	1 up to 3/5/10	3 up to 5/10/50
Management HA	Included	Included	Included	Included
Logs/sec	7,500	14,000	30,000	30,000
Built-in Interfaces	5 Copper GbE	5 Copper GbE	4 Copper GbE	4 Copper GbE
LCD Display	Yes	-	Yes	Yes
Storage	1 x 0.5 TB	4 x 0.5 TB	4 x 1 TB	4 x 1 TB, up to 12 TB
Storage Type	-	RAID 10	RAID 10	RAID 10
Fiber Channel SAN Card	-	-	Optional	Optional
Out-of-Band Management	-	Integrated	Integrated	Integrated
Enclosure	1U	1U	2U	3U
Dimensions (standard)	17 x 10.9 x 1.75 in.	17 x 21.7 x 1.75 in.	22.8 x 17.4 x 3.5 in.	24.9 x 17.4 x 5.2 in.
Dimensions (metric)	431 x 277 x 44mm	431 x 551 x 44mm	580 x 442 x 88mm	632 x 442 x 131mm
Weight	6kg (13.2 lbs.)	13kg (28.7 lbs.)	23.5kg (51.8 lbs.)	29.5kg (65 lbs.)
Power Supply	1	2	2	3
Power Input	100/240V, 50/60Hz	100/240V, 50/60Hz	90/264V, 47/63Hz	90/264V, 47/63Hz
DC Option	-	-	Yes	-
Power Supply Spec (max)	150W	2 x 250W	2 x 600W	3 x 930W
Power Consumption (max)	70.5W	135.8W	505.3W	399.6W
Operating Environment	Temperature: Ambient operating 0° to 40° C; Humidity: 5% to 95% non-condensing (RH)			
Compliance	CE, FCC Class A, RoHS			

Appliance Specifications

Smart-1 SmartEvent Series

	Smart-1 SmartEvent 5	Smart-1 SmartEvent 25	Smart-1 SmartEvent 50
Software Edition	R70.2	R70.2	R70.2
Managed Gateways	5 up to 25	25 up to 50	50 up to 150
Managed Domains	1	1	1 up to 3/5/10
Management HA	Included	Included	Included
Logging Capacity (Recommended)	2GB per day	10GB per day	25GB per day
Storage	1 x 0.5 TB	4 x 0.5 TB	4 x 1 TB
Storage Type	-	RAID 10	RAID 10
Built-in Interfaces	5 Copper GbE	5 Copper GbE	4 Copper GbE
Fibre Channel SAN card	-	-	optional
Out-of-band management	-	Integrated	Integrated
LCD Display	Yes	-	Yes
Enclosure	1U	1U	2U
Dimensions (standard)	17 x 10.9 x 1.75 in.	17 x 21.7 x 1.75 in.	22.8 x 17.4 x 3.5 in.
Dimensions (metric)	431 x 277 x 44mm	431 x 551 x 44mm	580 x 442 x 88mm
Weight	6kg (13.2 lbs.)	13kg (28.7 lbs.)	23.5kg (51.8 lbs.)
Power Supply	1	2	2
Power Input	100/240V, 50/60Hz	100/240V, 50/60Hz	90/264V, 47/63Hz
DC Option	-	-	Yes
Power Supply Spec (max)	150W	2 x 250W	2 x 600W
Power Consumption (avg)	61.7W	122W	350.8W
Operating Environment	Temperature: Ambient operating 0° to 40° C; Humidity: 5% to 95% non-condensing (RH)		
Compliance	CE, FCC, Class A, RoHS		

Appliance Specifications

Check Point Integrated Appliance Solutions

	IAS[1] M2	IAS[1] M6	IAS[1] M8
Software Edition	R65, R70	R65, R70	R65, R70
10/100/1000 Ports	4/10	10/10	14/18
Firewall Throughput[2]	7 Gbps	16 Gbps	20 Gbps
VPN Throughput[2]	2.4 Gbps	3 Gbps	4 Gbps
Concurrent Sessions	1.2 million	1.2 million	1.2 million
IPS Throughput[2]	4 Gbps[3]	7.1 Gbps[3]	8.6 Gbps[3]
Licensed Users	Unlimited	Unlimited	Unlimited
VLANs	256	256	256
UTM Out of the Box	Optional	Optional	Optional
Security Acceleration	Yes	Yes	Yes
Integrated Multigateway Management	Optional	Optional	Optional
Storage	2 x 73 GB	2 x 73 GB	2 x 73 GB
Enclosure	1U	1U	2U
Dimensions (standard)	17.3 x 27.5 x 1.75 in.	17.3 x 27.5 x 1.75 in.	17.5 x 27.5 x 3.36 in.
Dimensions (metric)	440 x 698 x 44mm	443 x 698 x 44mm	444 x 698 x 84.8mm
Weight	16.1kg (35.5 lbs.)	16.1kg (35.5 lbs.)	26.1kg (57.5 lbs.)
Operating Environment	Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m		
Power Input	100/240V, 50/60Hz[4]		
Power Supply Spec (max)	650W	650W	1300W
Power Consumption (max)	180W	212W	342W

[1] IAS = Integrated Appliance Solutions
[2] Performance data represents the maximum capabilities of the systems as measured under optimal testing conditions. Deployment and policy considerations may impact performance results.
[3] Test based on real-world traffic blend using the default profile
[4] Redundant power supply

Appliance Specifications

Integrated Appliance Solution Bladed Hardware Series

	Crossbeam X45	Crossbeam X80
Throughput	Up to 8 Gbps per APM Up to 20 Gbps per chassis	Up to 8 Gbps per APM Up to 40 Gbps per chassis
Form Factor/Size	13.5 x 17.5 x 19 in. - 19 in. rack mountable	30 x 17.5 x 17.5 in.
Interfaces/Connectivity	Data: 2 x 10 Gigabit Ethernet- SR/LR via XFP and 10 x 1 Gigabit Ethernet- SX/LX via SFP	Per Network Processor Module (NPM); 2x10 GbBase-SR/LR via XFP 10x1 GbBase-SX/LX via SFP
Processor	Single or dual dual, or Quad-core CPU	Single, dual dual-core, or Quad Core CPU
System Memory	Up to 16 GB per APM	Up to 16 GB per APM
Disk Size	120 GB HDD per APM	120 GB HDD per APM
Power	1-2 PS, 1,200W or 2,700W 120-240 VAC, 2,400W rated max 200-240 VAC, 2,700W rated max	1-4 PS, 1,200W or 2,700W 120-240 VAC, 3,600W rated max 200-240 VAC, 5,000W rated max X80-DC: -48 volt DC, 100A
Module Support	Up to 2 NPM, up to 5 APM, up to 2 CPM Supports up to 7 modules total	Up to 4 NPM, up to 10 APM, up to 2 CPM Supports up to 14 modules total
Management	Command Line Interface (SSH, telnet, console), Greenlight Element Manager (GEM) EMS (https), SNMP V1,2,3 support, Standard Syslog	
Certification	Common Criteria EAL4 with Check Point Software Technologies VPN-1 R65	
Status Indicators	Power Supply and Module Active/Failed Status LED, Port link (NPM, CPM), Minor/Major/Critical Alarm LEDs	
Regulatory Compliance for Chassis	RoHS; UL 60950, IEC 950, FCC 47 CFR Part 15 Class A, EN 55022 : EN 55024, VCCI V-3 : AS/NZS 3548 : 1995 : CNS 13438 Class A	
Green IT Compliancy	High efficiency power system up to 91 percent, Member of The Green Grid; WEEE Directive, ISO 14001, RoHS	
Other	Single or Dual System High Availability GUI- or CLI-based management, scales to 2 Network Processing Modules (NPM), 3 Application Processing Modules (APM) and 2 Control Processing Modules (CPM)	Single or Dual System High Availability GUI- or CLI-based management, scales to 4 Network Processing Modules (NPM), 8 Application Processing Modules (APM) and 2 Control Processing Modules (CPM)
Check Point Software	VPN-1 NGX R65, Security Gateway R70 & R71, VPN-1 Power VSX R65 & R67	VPN-1 NGX R65, Security Gateway R70 & R71, VPN-1 Power VSX R65 & R67
Operating System	XOS 7.2.1, 7.3.0.3, 8.0.1, 8.1.0, 8.5.0, and 9.0	XOS 7.2.1, 7.3.0.3, 8.0.1, 8.1.0, 8.5.0, and 9.0
Operating Environment	Temperature: 0° to 40° C (32° to 104° F); Humidity: 10% to 90% non-condensing; Altitude: 3,048m (10,000 ft.)	

Appliance Specifications

Check Point Integrated Appliance Solutions

	D1 Gateway	D1 Gateway Pair	D2 Gateway	D6 Gateway	D8 Gateway
Software Edition	R70 4003	R70 4003	NGX R70 PWR	NGX R70 PWR	NGX R70 PWR
Virtual Firewalls	-				
10/100/1000 Ports	6/6	6/6	6/10	6/10	8/18
10 Gb Ports	-				
Firewall Throughput	2 Gbps	2 Gbps	7 Gbps	16 Gbps	20 Gbps
VPN Throughput	1.2 Gbps	1.2 Gbps	2.4 Gbps	3 Gbps	4 Gbps
Concurrent Sessions	1.2 million	1.2 million	1.2 million	1.2 million	1.2 million
IPS Throughput	-				
VLANs	254	254	256	256	256
Lights Out Management	Included	Included	Included	Included	Included
Storage	160 GB	160 GB	2 x 73 GB (8 Max)	2 x 73 GB (8 Max)	2 x 73 GB (12 Max)
Memory	1 GB	1 GB	2 GB	4 GB	8 GB
Dimensions (standard)	1.69 x 17.64 x 27.56 in.	1.69 x 17.64 x 27.56 in.	1.70 x 16.78 x 27.25 in.	1.70 x 16.78 x 27.25 in.	3.38 x 17.54 x 29.25 in.
Dimensions (metric)	432 x 448.1 x 700mm	432 x 448.1 x 700mm	432 x 426.2 x 692.2mm	432 x 426.2 x 692.2mm	859 x 445.5 x 743mm
Weight	14.3 kg (31.49 lbs.)	14.3 kg (31.49 lbs.)	17.92 kg (39.5 lbs.)	17.92 kg (39.5 lbs.)	-
Power Input	90/132V, 180/264V, 47/63Hz	90/132V, 180/264V, 47/63Hz	100/240V, 50-60Hz	100/240V, 50/60Hz	100/240V, 50/60Hz
Power Supply Spec (max)	430W	430W	460W	460W	460W
Power Consumption (max)	75W	75W	170W	181W	290W
Operating Environment	Temperature: 10° to 35° C (50° to 95° F); Humidity: 10% to 90% non-condensing; Attitude: 3,050m (10,000 ft.)				
Compliance	CISPR 22; EN55022; EN55024; FCC CFR 47, Pt 15; ICES-003; CNS13438; GB9254; EN 61000-3-2; EN 61000-3-3; EN 60950-1; IEC 60950-1		CISPR 22; EN55022; EN55024; FCC CFR 47, Pt 15; ICES-003; CNS13438; GB9254; K22; K24; EN 61000-3-2; EN 61000-3-3; EN 60950-1; IEC 60950-1		

continues on next page

Appliance Specifications

Check Point Integrated Appliance Solutions

continued from previous page

	VSX 50 Virtual Firewall D8	VSLS 50 Virtual Firewall D8	VSX 100 Virtual Firewall D8	VSLS 100 Virtual Firewall D8	UTM Appliance & UTM Appliance Pair
Software Edition	NGX R67 VSX	NGX R67 VSX	NGX R67 VSX	NGX R67 VSX	R70.1
Virtual Firewalls	50/250	100/250	100/250	100/250	-
10/100/1000 Ports	4/4	4/4	4/4	4/4	4 x RJ-45 Base-T
10 Gb Ports	4/8	4/8	4/8	4/8	-
Firewall Throughput	20 Gbps (System Aggregate)	20 Gbps (System Aggregate)	20 Gbps (System Aggregate)	20 Gbps (System Aggregate)	600 Mbps
VPN Throughput	4 Gbps (System Aggregate)	4 Gbps (System Aggregate)	4 Gbps (System Aggregate)	4 Gbps (System Aggregate)	100 Mbps
Concurrent Sessions	1.2 million (System Aggregate)	1.2 million (System Aggregate)	1.2 million (System Aggregate)	1.2 million (System Aggregate)	600,000
IPS Throughput	-	-	-	-	380 Mbps
VLANs	256 per Firewall	256 per Firewall	256 per Firewall	256 per Firewall	1,024
Lights Out Management	Included	Included	Included	Included	-
Storage	2 x 73 GB (12 Max)	2 x 73 GB (12 Max)	2 x 73 GB (12 Max)	2 x 73 GB (12 Max)	46 GB
Memory	1 6GB	16 GB	16 GB	16 GB	1 GB
Dimensions (standard)	3.38 x 17.54 x 29.25 in.	3.38 x 17.54 x 29.25 in.	3.38 x 17.54 x 29.25 in.	3.38 x 17.54 x 29.25 in.	16.8 x 10 x 1.73 in.
Dimensions (metric)	859 x 445.5 x 743mm	859 x 445.5 x 743mm	859 x 445.5 x 743mm	859 x 445.5 x 743mm	429 x 255 x 44mm
Weight	-	-	-	-	3.7kg (8.1 lbs.)
Power Input	100/240V, 50/60Hz	100/240V, 50/60Hz	100/240V, 50/60Hz	100/240VAC, 50/60Hz	100/240V, 50/60Hz
Power Supply Spec (max)	430W	430W	460W	460W	65W
Power Consumption (max)	75W	75W	170W	181W	41.1W
Operating Environment	Temperature: 10° to 35° C (50° to 95° F); Humidity: 10% to 90% non-condensing; Attitude: 3,050m (10,000 ft.)			Temperature: 5° to 40° C; Humidity: 10% to 85% non-condensing; Altitude: 2,500m	
Compliance	CISPR 22; EN55022; EN55024; FCC CFR 47, Pt 15; ICES-003; CNS13438; GB9254; K22; K24; EN 61000-3-2; EN 61000-3-3; EN 60950-1; IEC 60950-1			UL 60950; FCC Part 15, Subpart B, Class A; EN 55024; EN 55022; VCCI V-3; AS/NZS 3548:1995; CNS 13438 Class A (test passed; country approval pending); KN22, KN61000-4 Series, TTA; IC-950; ROHS	

More. Better. Simpler Security℠

Contact Check Point now

www.checkpoint.com/contactus

By phone in the US: 1-800-429-4391 option 5 or 1-650-628-2000

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

Easy and secure application access from anywhere

Citrix Access Gateway™ is a secure access solution that provides administrators granular application-level policy and action controls to secure access to virtual desktops, applications and data while allowing users to work from anywhere. It offers flexible deployment options with both physical and virtual appliances, a single point of management, and tools to help ensure compliance and the highest levels of information security across and outside the enterprise. At the same time, it empowers users with a single point of access—optimized for roles, devices and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

Citrix Access Gateway is the leading secure access solution for applications and desktops

- HDX SmartAccess – Delivers simple and seamless secure access anywhere
- Data security through adaptive application-level control
- Broad client support
- Flexible deployment options with virtual and physical appliances
- World-class scalability and performance
- Accelerated virtual desktops and applications

Features

All Access Gateway appliances include secure access to Citrix® XenDesktop® and Citrix® XenApp™ deployments at no additional cost, making it the most integrated and cost-effective solution for these environments. Expanded capabilities are also available with Universal Licenses that enable Access Gateway to secure all types of applications and data, and enforce strong data security through adaptive policies. Universal Licenses can be purchased separately and are included with Platinum Editions of XenApp, XenDesktop and Citrix® NetScaler®.

Feature		Included appliance features	Requires Universal License
Easy desktop and application access Provides secure access to all applications and data from any device with a single point of access that simplifies the user experience.	**Secure access to XenApp and XenDesktop** Provides secure access to XenDesktop and XenApp sessions without requiring a VPN connection.	•	
	Secure network access Full VPN support enables network-level access to any server within the protected network.		•
	Secure browser-only access Provides secure access to web applications, e-mail, and file shares using only a browser (no additional client components required).		•
	Single point of access Provides a robust landing page for users to easily access all their applications, files, e-mail, and other IT resources.		•
	User localization Localizes user interfaces in English, Spanish, French, German, and Japanese.	•	
	Broad client support Supports major platforms including Windows® 32 and 64-bit operating systems (including Windows 7) and Mac® Os X.	•	
Endpoint analysis Ensures that devices are safe to connect to the network and users have a method to easily update their devices to meet established policies.	**Integrated endpoint scanning** Continually scans client devices to determine if client security products (anti-virus, personal firewall, or other mandatory corporate programs) are active.		•
	Enhanced machine identity scans Determines machine identity by scanning for known corporate images on client devices.		•
	Quarantine groups / remediation Provides clients that fail endpoint analysis scanning with limited access to remediation sites to bring client devices into compliance with the organization's security policies.		•[1]
	Extensible endpoint analysis Extends endpoint analysis capabilities using industry-standard development tools.		•[2]

1. Requires MPX 5500 or NetScaler
2. Requires Advanced Access Controller server

Feature		Included appliance features	Requires Universal License
Scenario-based policy control (SmartAccess) Provides control to configure the most secure access to data and applications by dynamically adjusting access based on device configuration, location, and identity	**Adaptive access control** Provides access control on resources based on endpoint analysis results.		•
	Adaptive access control for virtual hosted applications and desktops Provides adaptive access control to applications and desktops controlled by XenDesktop and XenApp.		•
	Adaptive application and action control Controls the behavior of XenDesktop and XenApp sessions by preventing operations that may compromise data to unsecure devices.		•
Application and data security Protects and keeps private all data transmitted between the client and gateway.	**Standards-based security** Ensures that all communications are secure with SSL/TLS encryption.	•	
	Extensive authentication support Provides strong authentication with 2-factor methods and authenticates users against LDAP and RADIUS servers to leverage existing directories within the organization.	•	
	Client certificate support Validates certificates prior to granting access to protected resources in order to verify managed client devices.		•
	Basic split tunneling control Disables access to all network resources not hosted on the protected network.		•
	Enhanced split tunneling control Can disable split tunneling on clients to shut down direct Internet access but still permit access to resources on the client's local subnet.		•[1]
	Browser cache cleanup Removes objects and data stored on the local browser during the SSL VPN session.		•[1]
Accelerated secure access Ensures that users have a secure and optimized access experience to avoid common networking performance issues.	**Branch Repeater integration** When used together with the Citrix® Branch Repeater™ and Citrix Acceleration plug-in, Citrix Access Gateway can optimize connections to XenDesktop, XenApp, and other traffic within a VPN connection to ensure the best performance over a WAN and overcome common usability problem that exist as a result of network issues.		•

1. Requires MPX 5500 or NetScaler

Feature		Included appliance features	Requires Universal License
Fault tolerance Creates secure access deployments that guarantee a high-level of availability and reliability.	**Basic high availability configuration** Links appliances to create an active-passive pair, ensuring sessions remain active if the master fails.	•	
	Optional global server load balancing (GSLB) Routes client connections to the best VPN site based on availability, health, proximity, and responsiveness.	•[2]	
Simplified administration Maximizes the efficiency of the IT organization by simplifying common installation and management tasks.	**Centralized administration** Configures and manages Access Gateway appliances from a single management console.	•	
	Wizard-driven configuration Provides an intuitive series of click-through screens and simple instructions to guide administrators through installation and configuration.	•	
	Multiple virtual VPN servers A single appliance can emulate multiple SSL VPNs by hosting one or more virtual servers each with a unique IP, FQDN, and certificate.	•[1]	
	Historical charting Provides administrators with a graphical view of system and user activities.	•[1]	
	Administrative auditing Monitors all configuration changes made by administrators to ensure accountability and easy roll-back of configuration errors.		•[1]
	Auto-downloading / Auto-updating client plug-in Automatically downloads the Citrix Secure Access plug-in when the user connects to Access Gateway and ensures that they always receive the latest version of the client software.	•	
	Support for automated distribution of Access Gateway plug-in Simplifies client installation by allowing deployment of the Access Gateway plug-in through systems and client management solutions.		•

1. Requires MPX 5500 or NetScaler
2. Requires NetScaler

Platform specifications

	Access Gateway VPX virtual appliance on XenServer and VMWare® ESX™	Access Gateway 2010	Access Gateway MPX 5500	Access Gateway 9010 FIPS
Maximum VPN users	500	500	5,000	5,000
Chassis dimensions	NA	HH: 1.72” (4.36 cm) (1U rackmount) W: 17.22” (43.73 cm) D: 18.4” (46.72 cm)	H: 1.72” (4.36 cm) (1U rackmount) W: 17.22” (43.73 cm) D: 21.75” (55.2 cm)	H: 3.5” (8.9 cm) (2U rackmount) W: 17” (43.2 cm) D: 16” (40.6 cm)
Weight		12.57 lbs (5.7 kg)	22 lbs (9.97 kg)	34 lbs (15.4 kg)
Power	NA	100-240VAC Full Range 50-60 Hz 250W	100-264VAC Full Range 47-63 Hz	90-264VAC Full Range 47-63 Hz 335W
Interface ports	NA	1 Serial Port 1 USB Port 2 x 10/100/1000 BASE-T	8x10/100/1000 BASE-T	4 x 10/100/1000 BASE-T 1 x 10/100/1000 BASE-T
Warranty, software and firmware updates	12 months included, (software updates only)	12 months included, additional plan available	12 months included, additional plan available	12 months included, additional plan available

CITRIX®

www.citrix.com

About Citrix
Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2009 was $1.61 billion.

FirePass SSL VPN

DATASHEET

What's Inside:

Increase Productivity with Flexible, Secure Remote Access

As more mobile and remote workers use an increasing number of different devices to access corporate applications and data from many locations, your business benefits from more flexible and productive users. But securing applications, data, the network, and client devices from unauthorized access and attacks can quickly add management complexity and cost.

The FirePass® SSL VPN appliance and Virtual Edition (VE) provide secure remote access to enterprise applications and data for users over any device or network. FirePass ensures easy access to applications by delivering outstanding performance, scalability, availability, policy management, and endpoint security. The result is unified security enforcement and access control that increases the agility and productivity of your workforce.

Key Benefits:

Increase worker productivity
Provide fast and secure, always connected remote access from any location, from any device.

Gain ultimate flexibility
Quickly and easily deploy a virtual appliance to add remote access functionality to your existing virtual infrastructure.

Decrease costs
Reduce deployment and support costs with easy management, simple deployment, and secure application access.

Increase security
Deliver granular access control to intranet resources on a group basis, enhancing security.

Reduce risk with endpoint security
Verify the user quickly and easily with endpoint security to validate compliance with corporate policy.

ICSA labs CERTIFIED SSL VPN

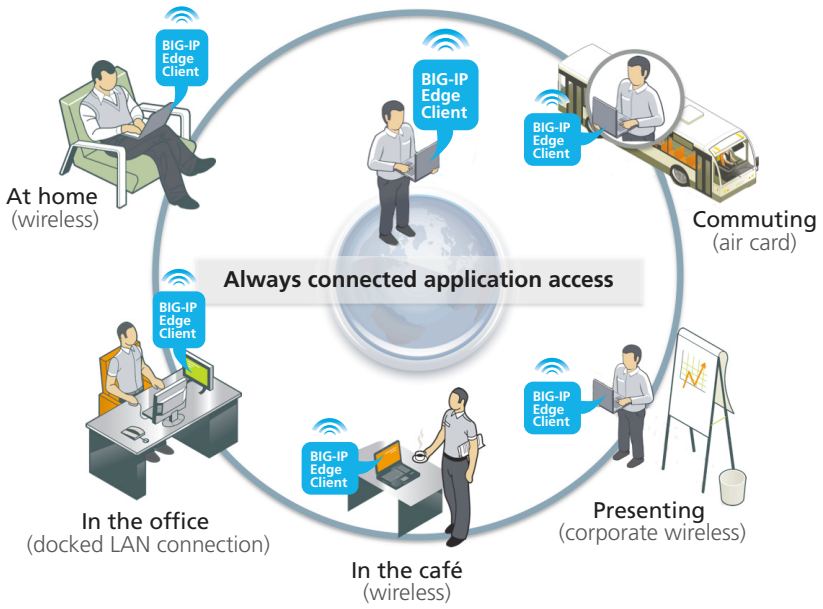
Improved User Experience

FirePass helps ensure user productivity by minimizing the time and effort required to gain access to authorized files and applications.

"Always connected" remote access

Some access clients need constant reconnection throughout the day as users move locations or restart applications. The BIG-IP® Edge Client™ solution is a state-of-the-art, integrated client that provides location awareness and zone determination to deliver a remote access solution unlike any other. Cutting-edge roaming, domain detection, and automatic connection create a seamless transition as users move between locations. BIG-IP Edge Client helps ensure continued user productivity whether the user is at home on a wireless network, using an air card in transit, giving a presentation from corporate wireless, in a café on guest wireless, or docked on a LAN connection. BIG-IP Edge Client is supported in FirePass 6.1 and 7.0.

BIG-IP Edge Client uses cutting edge roaming, domain detection, and automatic connection to deliver a seamless transition between locations.



Seamless VPN access

When the user first enters credentials as part of the Windows logon process, BIG-IP Edge Client caches them and then automatically tries them in the first attempt to log onto the VPN. This streamlines the user experience to help improve productivity.

Network Access

FirePass provides LAN-type network access connectivity for all applications by supporting existing network infrastructure, identity management systems, and client-server operating systems.

FirePass Network Access for Microsoft Windows (Windows 7, Vista, XP), Mac, and Linux Systems

- Eliminates the need for special administrative privileges for FirePass client component updates with Windows Installer Service, lowering management costs.
- Provides secure remote access to the entire network for all IP-based (TCP, UDP) applications.
- Includes standard features across all desktop and laptop platforms, as well as split tunneling, compression, activity-based timeouts, and automatic application launching.
- Provides remote access—unlike IPSec VPNs—without requiring preinstalled client software and configuration of the remote device. Client- or server-side application changes are not required.
- Enables administrators to restrict and protect resources accessible through the connector by instituting rules that limit access to a specific network or port.
- Uses the standard HTTPS protocol with SSL as the transport, so the device works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that don't support IPSec VPNs.
- Utilizes GZIP compression to compress traffic before it is encrypted, reducing the amount of traffic that is sent across the Internet and improving performance.
- Supports the latest OSs and Browsers—FirePass 7.0 supports 32-bit versions of: Windows 7, Vista, and XP; Mac OS X Leopard and Snow Leopard; Internet Explorer 6, 7, and 8; Firefox 3.x; and Safari 4. It supports 64-bit versions of: Windows 7, Vista, and XP; Linux (contact F5 or Reseller for list), Internet Explorer 7 (except Win 7) and 8; and Firefox 3.0. Talk to an F5 sales representative or reseller to review compatibility for your environment.

Client Security

- Safe Split Tunneling—To protect against back-door attacks when accessing the network with split tunneling, FirePass provides a dynamic firewall that protects Windows, Mac, and Linux users when using the full network access feature. This prevents hackers from routing through the client to the corporate network or users from inadvertently sending traffic to the public network.
- Endpoint Client Checking—FirePass increases security by detecting the presence of required processes (for example, virus scans, anti-malware, personal firewalls, OS patch levels, registry settings, and more) and the absence of other processes (for example, key logger) on the Mac, Linux or Windows client before enabling full network access.
- Hardware Endpoint Inspectors—FirePass inspects client machine features such MAC address, CPU ID, and HDD ID to identify remote devices. FirePass authorizes machines without the complexity of deploying machine certificates.

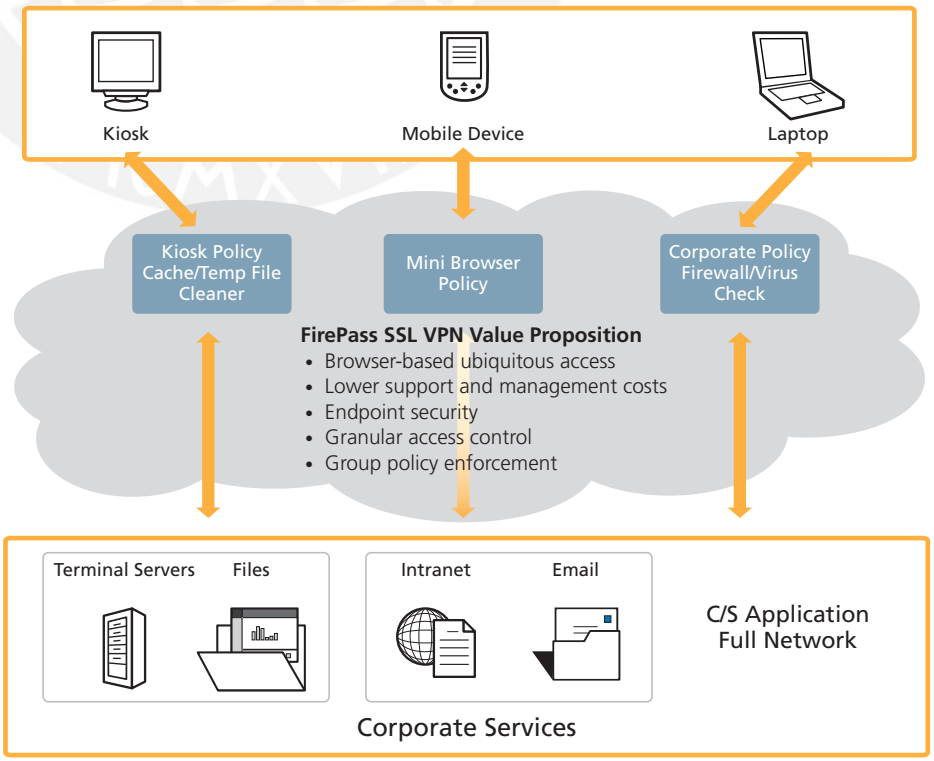
Windows Network Access Features

- Standalone Windows Client—FirePass establishes a network connection after entering user credentials. Software can be automatically distributed to the client using Microsoft's MSI installer technology.
- Windows Logon/GINA Integration—Enables implied, transparent user logon to the corporate network by integrating with the GINA ("Ctrl + Alt + Del" prompt) logon process.
- Standalone VPN Client CLI—Command-line interface support offers single sign-on support through integration with third-party applications (such as remote dialer software).
- Windows VPN Dialer—Provides a simplified user experience for those more comfortable with the dialup interface.
- Automatic Drive Mapping—Network drives can be automatically mapped to a user's Windows PC.
- Static IP Support—Assigns a static IP based on the user when the user establishes a network access VPN connection, lowering administrative support costs.
- Transparent Network Access—Eliminates network access browser window pop-ups and prevents users from accidentally terminating the connection.

Mobile Device Support

- Enables secure application access from Windows Mobile and smartphones.
- Provides access to both client/server- and web-based applications.

FirePass policies enable secure application access to a full set of corporate services, including kiosks, mobile devices, or laptops.



Application Access—Secure Access to Specific Applications

FirePass enables administrators to grant certain users—for example, business partners using equipment not maintained by the company—access to specific extranet applications and sites. FirePass protects network resources by only permitting access to applications that are cleared by the system administrator.

Specific Client/Server Application Access

- Enables a native client-side application to communicate back to certain corporate application servers via a secure connection between the browser and the FirePass device.
- Requires no pre-installation or configuring of any software.
- Involves no additional network-side software to access the application servers.
- Accesses applications via standard protocols: HTTP and SSL/TLS. It works with all HTTP proxies, access points, and private LANs, and over networks and ISPs that do not support traditional IPSec VPNs.
- Includes supported applications such as Outlook to Exchange Clusters, Passive FTP, Citrix Nfuse, and network drive mapping.
- Supports custom CRM applications as well as applications that use static TCP ports.
- Supports auto-login to AppTunnels, Citrix, and WTS applications to simplify the user experience.
- Integrates with Citrix SmartAccess to deliver endpoint inspection results to Citrix applications and send SmartAccess filters to XenApp based on the results of endpoint scans.
- Supports the auto-launch of client-side applications to simplify user experience and lower support costs.
- Enables lock-down Java-based application tunnels for non-Windows and Windows systems to prevent the execution of ActiveX controls.
- Offers complete DHCP support for clients using network access, automating IP address assignment and dynamic DNS registration of addresses. DHCP support provides easier multi-unit deployments while remote-access IP address range can overlap with internal LAN.
- Delivers support for Microsoft Communicator via Portal Access, enhancing VoIP communications.
- Offers unique support for the compression of client/server application traffic over the WAN, enhancing performance.

Terminal Server Access

- Provides secure web-based access to Microsoft Terminal Servers, Citrix MetaFrame applications, Windows XP Remote Desktops, and VNC servers.
- Provides Terminal Services for VMware View web client to enable user access from virtual desktops.
- Supports group access options, user authentication, and automatic log-on capabilities for authorized users.
- Supports automatic downloading and installation of the correct Terminal Services or Citrix remote platform client component, if not currently installed on the remote device, saving time.

- Supports remote access to XP desktops for remote troubleshooting using RDP and non-XP desktops with the built-in VNC feature.
- Provides Java-based Terminal Services support for Citrix and Microsoft.

Dynamic App Tunnels

- Provides maximum support for accessing a wide variety of client/server- and web-based applications.
- Offers a better alternative to reverse proxies for accessing applications from Windows client devices.
- Eliminates the need for web application content interoperability testing.
- Requires only "power user" privileges for installation and no special privileges for execution.
- Provides added support for auto-launching web application tunnels, simplifying the user experience.

Host Access

- Enables secure web-based access to legacy VT100, VT320, Telnet, X-Term, and IBM 3270/5250 applications.
- Requires no modifications to the applications or application servers.
- Eliminates the need for third-party host access software, reducing total cost of ownership (TCO).

Portal Access—Proxy-Based Access to Web Applications, Files, and Email

FirePass Portal Access capability works on any client OS with a browser: Windows, Linux, Mac, smartphones, PDAs, and more.

Web Applications

- Provides access to internal web servers, including Microsoft Outlook Web Access, Lotus iNotes, and Microsoft SharePoint Server as easily as from inside the corporate LAN.
- Delivers granular access control to intranet resources on a group policy basis. For example, employees can gain access to all intranet sites; partners can be restricted to a specific web host.
- Dynamically maps internal URLs to external URLs, so the internal network structure does not reveal them.
- Manages user cookies at the FirePass device level to avoid exposing sensitive information.
- Passes user credentials to web hosts to support automatic login and other user-specific access to applications. FirePass also integrates with existing identity management servers (for example, CA Netegrity) to enable single sign-on to applications.
- Proxies login requests from web hosts to avoid having users cache their passwords on client browsers.
- Enables or restricts access to specific parts of an application with granular access control list (ACL) for increased security and reduced business risks.

- Provides split-tunneling support for web applications, resulting in faster user performance when accessing public websites.
- Validates back-end certificate with rapid reverse-proxy to quickly authenticate the server's certificate.
- Offers dynamic server-side and DNS caching for increased web application (reverse proxy) performance and faster page download times.
- Delivers out-of-the-box reverse proxy support for rewriting a wide variety of JavaScript content in web pages, saving time.
- Provides Java patch ACL support to limit client-initiated connections through FirePass using Portal Access.
- Enables NTLMv2 support for access to web applications.
- Delivers DNS relay proxy service, enabling client-side name resolution without requiring any special runtime rights (for example, modification of hosts). Also enables redirection of ports to more fully support applications such as Outlook and Windows drive mapping.

File Server Access

- Enables users to browse, upload, download, copy, move, or delete files on shared directories.
- Supports: SMB Shares; Windows Workgroups; NT 4.0 and Win2000 domains; Novell 5.1/6.0 with Native File System pack; and NFS servers.

Email Access

- Provides secure web-based access to POP/IMAP/SMTP email servers from standard and mobile device browsers.
- Enables users to send and receive messages, download attachments, and attach network files to emails.

Mobile Device Support

- Provides secure access from Apple iPhone, Windows Mobile, PDAs, smartphones, cell phones, WAP, and iMode phones to email and other web-based applications.
- Dynamically formats email from POP/IMAP/SMTP email servers to fit the smaller screens of mobile phones and PDAs.
- Supports the sending of network files as email attachments and the viewing of text and Word documents.
- Supports ActiveSync applications, enabling PDA synchronization of email and calendar on Exchange Server from a PDA device, without requiring the pre-installed VPN client component.

Portal Access—Comprehensive Security

FirePass delivers multiple layers of control for securing information access from public systems.

Client Security

- Protected Workspace—Users of the 32-bit version of Windows XP/Vista/7 or the 64-bit version of Windows Vista/7 can be automatically switched to a protected workspace for their remote access session. In a protected workspace mode, the user cannot write files to locations outside the protected workspace; the temporary folders and all of their contents are deleted at the end of the session.
- Cache Cleanup—The cache cleanup control removes—and empties from the recycle bin—the following data from the client PC: cookies, browser history, auto-complete information, browser cache, temp files, and all ActiveX controls installed during the remote access session.
- Secure Virtual Keyboard—For additional password security, FirePass offers the patent-pending Secure Virtual Keyboard which enables secure password entry from the mouse instead of the keyboard.
- Download Blocking—For systems unable to install a "cleanup" control, FirePass can be configured to block all file downloads to avoid the issue of inadvertently leaving behind temporary files, yet still enable access to applications.
- Automatic File Virtualization—In protected workspace mode, temporary files and registry settings are written to a virtual file system rather than to the local machine.
- Encrypted Saved Content—All temporary content saved on the remote system is encrypted in the event that the protected workspace doesn't exit normally, such as in a power failure, rendering the content unreadable.
- Portal Support for Popular Mobile Clients—FirePass supports portal access with iPhone, BlackBerry, and Opera Mini browsers.

Content Inspection and Web Application Security

For users accessing web applications on the corporate network, FirePass enhances application security and prevents application-layer attacks (for example, cross-site scripting, invalid characters, SQL injection, buffer overflow) by scanning web application access for application layer attacks—then blocking user access when an attack is detected.

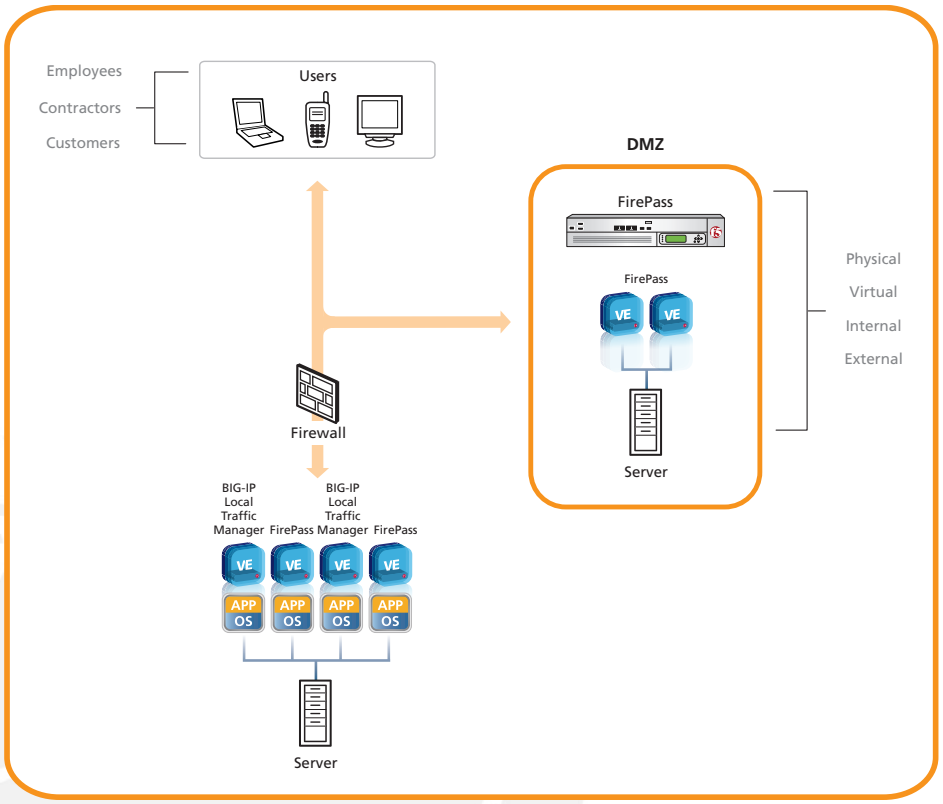
Integrated Virus Protection

FirePass can scan web and file uploads using either an integrated scanner or external scanner via ICAP API. Infected files are blocked at the gateway and not allowed onto email or file servers on the network, for increased protection.

Flexible Remote Access

FirePass Virtual Edition (VE) makes it easy to quickly deploy a virtual appliance to add SSL VPN functionality to an existing virtual infrastructure. This offers greater flexibility in disaster recovery scenarios or during a surge in remote access demand. Virtual editions of FirePass and BIG-IP Local Traffic Manager can be combined to provide industry-leading application delivery and remote access in the same environment.

FirePass VE is an easy way to add flexible remote access to your current virtual environment.



Dynamic Policy Engine—Total Administrative Control

The FirePass policy engine enables administrators to easily manage user authentication and authorization privileges.

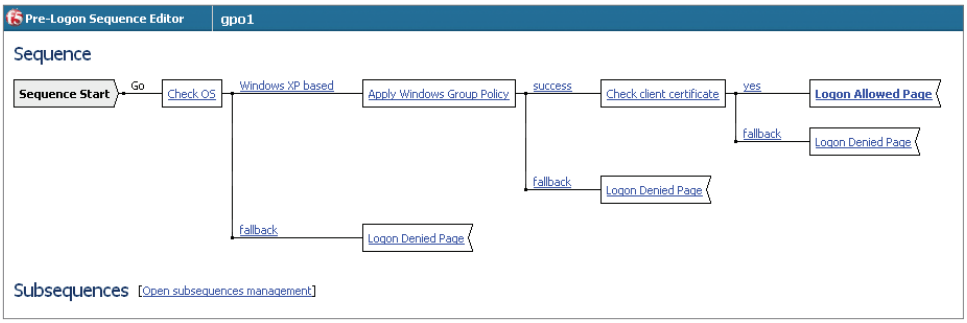
Dynamic Policy-Based Access

Administrators have quick and granular control over their network resources. Through policy management support, they can authorize access to applications based on the user and device. Administrators can easily implement existing policies with import and export of pre-logon policies.

Visual Policy Editor

The Visual Policy Editor creates a flow-chart style graphical view of your access policies, giving you point-and-click ease in profiling and managing groups, users, devices, or any combination of the three. This simplifies the definition and management of endpoint policies, lowers administrative costs, and increases the ability to quickly ensure the protection of company resources.

The Visual Policy Editor makes it easy to create access policies.



User Authentication

Users can be authenticated against an internal FirePass database, using passwords. FirePass can also be easily configured to work with RADIUS, Active Directory, RSA 2-Factor, LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (for example, Netegrity), and Windows domain servers. With Active Directory, users can change current or expired passwords and receive warnings when passwords are set to expire. Support for nested Active Directory configurations enables the use of a more complex, hierarchical directory structure.

Two-Factor Authentication

Many organizations use "two-factor" authentication (such as tokens or SmartCards) that require more than just a user ID and password. FirePass supports two-factor authentication including RSA SecurID® Native ACE authentication.

Challenge Response Test

Administrators can implement CAPTCHA, an easy challenge response test for humans that protects the organization from DoS and script-based brute force attacks.

CAPTCHA protects against DoS and script-based brute force attacks.

Client-side and Machine Certificates/PKI Support

FirePass integrates seamlessly with the existing PKI infrastructure and enables the administrator to restrict or permit access based on the device being used to access FirePass. FirePass can check for the presence of a client-side digital certificate or Windows machine certificate during user login. Based on the presence of a valid certificate, FirePass can support access to a broader range of applications. FirePass can also use client-side or machine certificates as a form of two-factor authentication and prohibit all network access for users without a valid certificate.

Group Management

Access privileges can be granted to individuals or to groups of users (for example: sales, partners, or IT). This enables FirePass to restrict individuals and groups to particular resources.

Group Policy Enforcement

Group policy provides an exclusive mechanism to apply and enforce policies on client systems not part of the network domain. You can use the Visual Policy Editor to design group policies, in the form of templates, that restrict user authority and access while enforcing compliance with PCI, HIPAA, and GLBA. (Note: Group Policy Objects are only available on Active Directory.)

Dynamic Group Mapping

FirePass dynamically maps users to FirePass groups using various dynamic group mapping mechanisms such as Active Directory, RADIUS, LDAP, client certificates, landing URI, and virtual host name as well as pre-logon session variables.

Single Sign-On (SSO) Support

SSO configuration uses authentication session variables to extract SSO information from certificates and authentication information from username and password settings. Advanced session variables help system administrators extend and customize FirePass, enabling them to manipulate and create new session variables for custom deployments. They also can collect and capture RADIUS attributes plus LDAP, Active Directory, and certificate field values.

Session Timeouts and Limits

Administrators can configure inactivity and session timeouts to protect against a hacker attempting to take over a session from a user who forgets to logoff at a kiosk.

Role-Based Administration

Organizations have the flexibility to provide some administrative functions (enrolling new users, terminating sessions, re-setting passwords) to some administrator-users, without exposing all functions to them (for example, shutting down the server or deleting a certificate).

Logging and Reporting

FirePass delivers built-in logging support for logging user, administrator, session, application, and system events. Additionally, FirePass provides logs in silo format for integration with an external syslog server. The administration console offers a wide range of audit reports to help comply with security audits. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, websites accessed, session duration, session termination type, and other information for a user-specified time interval. A single URL is used to retrieve summary/group reports in either HTML or spreadsheet format.

Customization

FirePass provides advanced customization features, enabling the administrator to design a unique GUI or existing corporate website portal to best reflect corporate and user requirements.

Localized User GUI

FirePass enables all fields on the user web page to be localized, including the names of the feature (for example, web applications). This helps companies localize the user's GUI, not just user favorites—increasing business value and lowering TCO.

Complete Login and Webtop Customization

With FirePass, administrators can completely customize an entire login and webtop web page to best suit their existing corporate website portals. Administrators can use WebDAV capabilities to upload custom pages, for an enhanced user experience.

iControl SSL VPN Client API for Secure Application Access

As the only SSL VPN product with an open client API and SDK, FirePass enables automated, secure access from the Win32 client OS (XP, Vista, 7) by providing secure system-to-system or application-to-application communication. Applications can automatically start and stop network connections transparently without requiring users to log into the VPN. This enables faster, easier connections for users while reducing client application installation costs.

FirePass Product Details

The range of FirePass appliances and Virtual Edition address the concurrent user access needs of small to large enterprises.

FirePass 1200

The FirePass 1200 device is designed for small to medium enterprises and branch offices, and supports from 10 to 100 concurrent users.

FirePass 4100

The FirePass 4100 controller is designed for medium-size enterprises and, from a price/performance standpoint, is recommended for up to 500 concurrent users.

FirePass 4300

The FirePass 4300 appliance is designed for medium to large enterprises and service providers and supports up to 2000 concurrent users.

FirePass Virtual Edition

FirePass Virtual Edition runs in a VMware ESX 4.0 virtual environment and is designed for medium to large enterprises and service providers supporting up to 2000 concurrent users.

Clustering

The FirePass 4100 and 4300 appliances and Virtual Edition have built-in clustering support. They can be combined with F5 BIG-IP® Global Traffic Manager™ and BIG-IP® Local Traffic Manager™ to provide industry-leading scalability, performance, and availability.

Failover

FirePass appliances and Virtual Edition can also be configured for stateful failover between pairs of servers (an active server and a standby server) to avoid having to re-logon to another FirePass device or Virtual Edition in the unlikely event of a primary unit failure.

SSL Accelerator Hardware Option

FirePass 4100 offers a unique Hardware SSL Acceleration option to offload the SSL key exchange as well as the encryption and decryption of SSL traffic. This enables significant performance gains in large enterprise environments for processor-intensive ciphers such as 3DES and AES.

FIPS SSL Accelerator Hardware Option

FirePass is FIPS compliant* to meet the strong security needs of government, finance, healthcare, and other security-conscious organizations. FirePass 4100 and 4300 devices offer support for FIPS 140 Level-2 enabled tamper-proof storage of SSL keys, as well as FIPS-certified cipher support for encrypting and decrypting SSL traffic in hardware. FIPS SSL Accelerator is available as a factory install option to the base 4100 and 4300 platform.

* FIPS 140-2 meets the security criteria of CESG (UK's National Technical Authority For Information Assurance) for use in private data traffic.

FirePass Specifications

The FirePass appliance is available in three models and as a Virtual Edition to address the concurrent user access needs of small to large enterprises.

FirePass Virtual Edition

Virtual Specifications

Recommended Conc. Users:	Up to 2000*
Clustering Support:	Yes – up to 10 virtual appliances

*Note: Actual performance varies depending on hardware platform, resources available, and configuration. Customer is responsible for performance testing and scaling of FirePass Virtual Edition.

Host System Requirements	It is highly recommended that the host system contain CPUs based on AMD-V or Intel-VT technology.
Hypervisor:	VMware ESX 4.0 or ESXi 4.0 VMware vSphere Client VMware virtual hardware version 7
Processor:	1 CPU (4 CPUs or more are recommended for more than 500 concurrent users.)
Memory:	2 GB RAM (8 GB or more are recommended for more than 500 concurrent users.)
Network Adapters:	3 network interfaces
Disk Space:	30 GB hard drive of thin provisioning

4300 and 4100 Series

1200 Series

Physical Specifications	4300	4100	1200
Recommended Conc. Users:	2000	500	100
Max. Conc. Users per Appliance :	2000	2000	100
Interfaces:	4 (10/100/1000) LAN ports	4 (10/100/1000) LAN ports	2 (10/100) LAN ports
Dimensions:	3.5" H x 17.5" W x 23.5" D 2U industry standard rack mount chassis	3.5" H x 17.5" W x 23.5" D 2U industry standard rack mount chassis	1.7"H x 16.7" W x 11" D 1U industry standard rack mount chassis
Weight:	43 lbs	40 lbs	10 lbs
Processors:	Two Opteron 2.2 GHz - dual core	Two Opteron 2.0 GHz - single core	Intel Celeron 2.0GHz - single core
Power Supply:	Dual 475 W 90/240 +/- 10% VAC auto switching	425 W 90/240 +/- 10% VAC auto switching Optional redundant power supply	Single full-range 250 W
Typical Power Consumption:	275 W	275 W	180 W
Maximum Heat Output:	939 BTU/hr	939 BTU/hr	785 BTU/hr
Device Redundancy:	Watchdog timer, failsafe cable (primary and secondary)	Watchdog timer, failsafe cable (primary and secondary)	Watchdog timer, failsafe cable (primary and secondary)
Clustering support:	Yes – up to 10 appliances	Yes – up to 10 appliances	No
FIPS SSL Accelerator Card Option:	Yes – factory only	Yes – factory only	No
Hard Drive Capacity:	160 GB	160 GB	40 GB
RAM:	8 GB standard	4 GB standard on 4110, 4120, 4130 – factory upgradable to 8 GB (4140 and 4150 8 GB standard)	512 MB
Temperature (operating):	41° F to 104° F (5° C to 40° C)	41° F to 104° F (5° C to 40° C)	41° F to 104° F (5° C to 40° C)
Non-Operating Ambient Temperature Range:	-40° F to 149° F (-40° C to 65° C) Relative humidity 10% to 95% at 40° C non-condensing	-40° F to 149° F (-40° C to 65° C) Relative humidity 10% to 95% at 40° C non-condensing	-40° F to 149° F (-40° C to 65° C) Relative humidity 5% to 85% at 40° C non-condensing
Humidity (relative):	20% to 90% at 40° C	20% to 90% at 40° C	20% to 90% at 40° C
Safety Agency Approval:	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950 CB test certification to IEC 950, EN 60950	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950	UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950
Electromagnetic Emissions Certifications:	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A	EN55022 1998 Class A EN55022 1998 Class A FCC Part 15B Class A VCCI Class A

More Information

Visit these resources on F5.com to learn more about FirePass.

White papers

F5 FirePass Endpoint Security

Get to Know GPO

Podcast

Secure Remote Access for Disaster Recovery

Case study

City of Diamond Bar Deploys FirePass

Deployment guides

F5 FirePass controller with BIG-IP LTM and GTM (FirePass v6.x, LTM, and GTM 9.4.2), Deployment Guide

FirePass and VMware View Deployment Guide

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com