

Шлюзы безопасности Juniper Networks **SSG 500**



Платформы Juniper Networks серии SSG 500 (Secure Services Gateway) – это новый класс специализированных устройств, обладающих высокой производительностью, широким набором функций сетевой безопасности, а также богатыми возможностями интеграции в сети LAN/WAN. Исчерпывающий набор функций, включая Stateful Firewall, IPS, Антивирус (в том числе, Anti-Spyware, Anti-Adware, Anti-Phishing) Anti-Spam и Web-Filtering, позволяет использовать устройства серии SSG для борьбы с вирусными атаками, шпионским и прочим вредоносным ПО. Устройства серии SSG500 можно применять в качестве традиционных маршрутизаторов доступа региональных офисов или комбинированных экономических решений, совмещающих функции межсетевого экрана и маршрутизатора.

Основными достоинствами SSG 500 являются:

- высокая производительность и надежные механизмы защиты LAN/WAN сетей, достигаемые за счет аппаратной реализации и наличия специализированной операционной системы
- сегментация на зоны безопасности, виртуальные маршрутизаторы и VLAN с возможностью изоляции подозрительных групп пользователей, хостов и подсетей
- гибкая модульная архитектура с разнообразным набором интерфейсов для подключения к LAN/WAN-сетям, позволяющая снизить общую стоимость решения
- наличие богатого функционала для борьбы с вирусами, шпионским программным и прочим вредоносным программным обеспечением

Экономичные модульные устройства SSG550 и SSG520 идеально подходят для защиты сетей филиалов и региональных офисов крупных компаний, предприятий среднего масштаба и провайдеров услуг.

SSG 550:

Устройства SSG 550 обладают пропускной способностью 1 Гбит/с в режиме межсетевого экранирования, 500 Мбит/с – при IPSec VPN – туннелировании и 500 Мбит/с – в режиме IPS (Deep Inspection). Устройства SSG550 имеют резервные блоки питания и удовлетворяют стандартам NEBS.

SSG 520:

Устройства SSG 520 обладают пропускной способностью 600 Мбит/с в режиме межсетевого экранирования, 300 Мбит/с – при IPSec VPN – туннелировании и 300 Мбит/с – в режиме IPS (Deep Inspection).

Безопасность и производительность

Шлюзы безопасности SSG550 имеют лучшие в своем классе характеристики и способны обеспечить надежную защиту вычислительных сетей на 3-7 уровнях. На прикладном уровне защита обеспечивается за счет встроенных антивирусного, антифишингового, антишпионского и антиспамового фильтров.

Модульность

Устройства серии SSG500 имеют четыре встроенных порта 10/100/1000 и 6 слотов для установки LAN/WAN - интерфейсных модулей, в том числе, поддерживающих стандарты T1/E1, DS3, Serial, 10/100/1000, SPF и FE. Благодаря широкому спектру интерфейсных модулей и сетевых протоколов, SSG500 способен удовлетворить как существующие, так и перспективные требования заказчиков.

Сетевая сегментация

Наличие зон безопасности, виртуальных маршрутизаторов и поддержка VLAN позволяет сетевым администраторам назначать собственные политики безопасности для различных групп пользователей, хостов и подсетей.

Технические характеристики шлюзов безопасности SSG серии 500:

	SSG 550	SSG 520
Производительность и пропускная способность (1)		
Версия ScreenOS	ScreenOS 5.4	ScreenOS 5.4
Пропускная способность в режиме сетевого экранирования (пакеты большой длины)	Более 1 Гбит/с	SSG520: Более 650 Мбит/с
Пропускная способность в режиме сетевого экранирования (смешанный трафик) (2)	1 Гбит/с	600 Мбит/с
Пропускная способность в режиме VPN-туннелирования (3DES+ SHA 1)	500 Мбит/с	300 Мбит/с
Производительность при обработке пакетов размером 64 Байт	600 тыс. пакетов/с	300 тыс. пакетов/с
Пропускная способность в режиме IPS (Deep Inspection (3))	500 Мбит/с	300 Мбит/с
Максимальное количество одновременных сессий	128 тыс.	64 тыс.
Максимальная скорость обработки новых сессий	15 тыс. сессий/с	10 тыс. сессий/с
Максимальное количество политик	4 тыс.	1 тыс.
Максимальное число пользователей	Неограниченное	Неограниченное
Сетевые интерфейсы		
Встроенные интерфейсы	4 x 10/100/1000	4 x 10/100/1000
Общее количество слотов для установки интерфейсных модулей PIM	6	6
Количество быстродействующих PIM - слотов	4	2
Интерфейсные модули WAN	Serial, T1, E1, DS3	
Интерфейсные модули LAN	SFP, FE, 10/100/1000	
Режимы работы		
Layer 2 (прозрачный режим) (4)	+	+
Layer 3 (маршрутизатор и/или NAT)	+	+
Возможности по трансляции сетевых адресов		
NAT	+	+
PAT	+	+
Policy-based NAT/PAT	+	+
Virtual IP	64	32
Mapped IP	6 тыс.	1,5 тыс.
Межсетевое экранирование		
Обнаружение атак на сетевом уровне	+	+
Защита от DoS и DDoS атак	+	+
Повторная сборка TCP-сегментов	+	+
Защита от пакетов со структурными изменениями	+	+
Защита на прикладном уровне		
IPS (Deep Inspection FW)	+	+
Обнаружение аномалий в протоколах	+	+
Сигнатурный анализ	+	+
Антивирусный сканер (5)	+	+
База сигнатур	более 100 тыс.	
Поддерживаемые протоколы	POP3, SMTP, HTTP, IMAP, FTP	
Борьба с фишингом	+	+
Борьба со шпионским ПО	+	+
Anti-Adware	+	+
Anti-Keylogger	+	+
Антиспамовый фильтр (6)	+	+
Встроенный URL фильтр (7)	+	+
Внешняя URL фильтрация (8)	+	+
Защита голосового трафика		
H.323 ALG	+	+
SIP ALG	+	+
SCCP ALG:	+	+
MGCP ALG	+	+
NAT для H.323/SIP	+	+
VPN		
Максимальное количество VPN-туннелей	1 тыс.	500
Максимальное количество туннельных интерфейсов	300	100
Поддержка алгоритмов шифрования DES (56-bit), 3DES (168-bit) и AES	+	+
Поддержка алгоритмов аутентификации MD-5 и SHA-1	+	+
Поддержка механизмов обмена ключами Manual Key, IKE, PKI (X.509)	+	+
Поддержка механизма Perfect forward secrecy (DH Groups)	+	+
Защита от атак типа Replay	+	+
Поддержка VPN-туннелей типа Remote access	+	+
Поддержка L2TP-over-IPSec	+	+
Поддержка IPSec NAT Traversal	+	+
Резервирование VPN-шлюзов	+	+

Аутентификация в режимах межсетевого экранирования и VPN

Максимальное количество пользователей во внутренней базе	1,5 тыс.	1,5 тыс.
Протоколы аутентификации	RADIUS, RSA SecurID, LDAP 802.1x	
XAUTH VPN-аутентификация	+	+
WEB-аутентификация	+	+

Маршрутизация

Поддержка BGP	До 15 таблиц	До 9 таблиц
Поддержка OSPF	До 8 таблиц	До 3 таблиц
Поддержка RIPv1/v2	До 256 таблиц	До 128 таблиц
Динамическая маршрутизация	+	+
Статическая маршрутизация	+	+
Маршрутизация от источника	+	+
Маршрутизация на основе политик (Policy-Based Routing)	+	+
Функция Equal cost multi-path routing	+	+
Максимальное количество статических маршрутов	20 тыс.	10 тыс.

Инкапсуляция

PPP	+	+
MLPPP	+	+
Максимальное количество физических интерфейсов MLPPP	12	12
Frame Relay	+	+
MLFR (FTF 15, FRF 16)	+	+
Максимальное количество физических интерфейсов MLFR	12	12
HDLC	+	+

Управление полосой пропускания (QoS)

Гарантированная полоса пропускания	+	+
Максимальная полоса пропускания	+ настраивается на физических интерфейсах	+ настраивается на физических интерфейсах
Распределение полосы пропускания на основе приоритетов	+	+
Поддержка DiffServ stamp	+ (Настраивается в политиках)	+ (Настраивается в политиках)

Управление устройством

Web-интерфейс (HTTP и HTTPS)	+	+
Интерфейс командной строки CLI (консоль)	+	+
Интерфейс командной строки CLI (Telnet)	+	+
Интерфейс командной строки CLI (SSH)	+ (версия 1.5 и 2.0)	+ (версия 1.5 и 2.0)
Поддержка NetScreen-Security Manager	+	+
Управление через VPN	+	+
SNMP Full Custom MIB	+	+
Функция Rapid deployment	+	+

Протоколирование событий и мониторинг

Поддержка Syslog	До 4 внешних серверов	
Оповещение администраторов системы по электронной почте	(2 адреса)	(2 адреса)
Поддержка NetQ WebTrends	+	+
Поддержка SNMP (v2)	+	+
Traceroute	+	+
VPN tunnel monitor	+	+

Виртуализация

Максимальное количество зон безопасности	60	60
Максимальное количество виртуальных маршрутизаторов	8	5
Максимальное количество VLAN	150	125

Возможности по резервированию

Active/Active	+	-
Active/Passive	+	+
Резервирование физических портов	+	+
Синхронизация конфигурации	+	+
Синхронизация сессий (в режиме VPN и межсетевого экранирования)	+	+
Восстановление сессий при изменении маршрута	+	+
Обнаружение отказа устройства в кластере	+	+
Обнаружение отказа линии связи	+	+
Аутентификация устройства в кластере	+	+
Шифрование трафика в кластере	+	+

Назначение адресов

Статическое	+	+
DHCP, клиент PPPoE	+	+
Внутренний DHCP-сервер	+	+
DHCP-relay	+	+

Поддержка PKI		
PKCS 7/ PKCS 10	+	+
SCEP	+	+
OCSF	+	+
Поддерживаемые удостоверяющие центры	Verisign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape), Baltimore, DOD PKI	
Администрирование		
Максимальное количество локальных администраторов	20	20
Внешние системы администрирования	RADIUS, LDAP, SecureID	
Максимальное количество административных подсетей	6	6
Уровни администрирования Root Admin, Admin, and Read Only	+	+
Обновление программного обеспечения	TFTP, Web, NSM	
Откат к предыдущей рабочей конфигурации	+	+
Внешняя Flash-память		
Дополнительное хранилище событий (logs)	USB (в перспективе)	
Запись и хранение событий	+	+
Запись и хранение файлов конфигураций	+	+
Возможность записи и хранения образа операционной системы	+	+
Физические параметры		
Габаритные размеры (высота/ширина/глубина)	9 см / 44 см / 54 см	9 см / 44 см / 54 см
Вес	12,5 кг (без интерфейсных модулей, с одним блоком питания) 15,4 кг (шесть интерфейсных модулей, два блока питания)	11,5 кг (без интерфейсных модулей) 12,7 кг (шесть интерфейсных модулей)
Установка в стандартную стойку	+ (2U)	+ (2U)
Источник питания напряжения постоянного тока	90-264 В, 420 Ватт	90-264 В, 350Вт
Источник питания напряжения переменного тока	-48 - -60 В, 420Вт	-48 - -60 В, 420Вт
Резервный блок питания	+	-
Сертификаты		
Сертификаты на соответствие требованиям по технике безопасности	UL, CUL, CSA, CB	
Сертификаты по обеспечению требований электромагнитной совместимости (ЭМС)	FCC class A, CE class A, C-Tick, VCCI class A	
Условия эксплуатации		
Температура работы	0°C - 50°C	0°C - 50°C
Температура хранения	-4°C - 70°C	-4°C - 70°C
Допустимая влажность	10% - 90%	10% - 90%
MTBF (Bellcore model)	12 лет	12 лет
Другие	NEBS Level 3	NEBS Level 3

- ⁽¹⁾ Указанные значения производительности, пропускной способности и других характеристик получены при тестировании устройств с установленной операционной системой ScreenOS 5.4 в идеальных условиях. В реальных условиях и, в случае использования других версий операционной системы, ScreenOS значения параметров могут отличаться от указанных.
- ⁽²⁾ Приведенные значения производительности получены при обработке UDP-трафика, состоящего на 58,33 % из пакетов размером 64 байт, 33,33% из пакетов размером 570 Байт и на 8,33% из пакетов 1518 Байт.
- ⁽³⁾ Пропускная способность при обработке HTTP пакетов длиной 100 кБайт (60% текста, 20 % графики и 20 файлов).
- ⁽⁴⁾ Приведенные значения производительности получены при обработке UDP-трафика, состоящего на 58,33 % из пакетов размером 64 байт, на 33,33% из пакетов размером 570 Байт и на 8,33% из пакетов 1518 Байт.
- ⁽⁵⁾ Антивирусный сканер «Лаборатории Касперского»
- ⁽⁶⁾ Технология Symantec Brightmail
- ⁽⁷⁾ Технология SurfControl
- ⁽⁸⁾ Технологии SurfControl и WebSense



CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA
 Juniper Networks, Inc.
 1194 North Mathilda Avenue
 Sunnyvale, CA 94089 USA
 Phone: 888-JUNIPER (888-586-4737)
 or 408-745-2000
 Fax: 408-745-2100
www.juniper.net

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
 Juniper Networks (UK) Limited Juniper House
 Guildford Road
 Leatherhead
 Surrey, KT22 9JH, U. K.
 Phone: 44(0)-1372-385500
 Fax: 44(0)-1372-385501



ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР В РОССИИ
 ЗАО НТЦ «Ландата»
 121471, г. Москва,
 2-й пер. Петра Алексеева, д.2, стр.1
 тел: +7 (495) 925-7620
 факс : +7 (495) 925-7621
 e-mail: info@landata.ru
 web: www.landata.ru