Juniper Networks **SSG 140**

Juniper Networks Secure Services Gateway 140 (SSG 140) – это специализированная аппаратная платформа, отличающаяся высокой производительностью, широким набором функций защиты и маршрутизации для использования в сетях региональных офисов предприятий среднего масштаба. Весь входящий и исходящий сетевой трафик защищен от червей, Троянов и вредоносного кода с помощью набора UTM – функций, в том числе межсетевого экранирования, IPSec VPN туннелирования, антивирусной фильтрации (защита от шпионского и рекламного программного обеспечения, фишинга) антиспамовой и URL-фильтрации.

Богатый набор UTM-функций позволяет использовать SSG 140 в качестве универсальных платформ сетевой защиты. Благодаря наличию мощных механизмов маршрутизации, SSG 140 могут применяться как обычные маршрутизаторы и как комбинированные устройства, сочетающие в себя одновременно функции сетевой защиты и маршрутизации, что позволит существенно снизить капитальные и текущие IT-расходы.

Отличительные особенности и преимущества SSG 140:

- гибкая модульная архитектура с разнообразным набором интерфейсов для подключения к LAN/WAN-сетям, позволяющая снизить общую стоимость решения;
- широкий набор UTM-функций, реализованных на базе технологий от ведущих мировых производителей и предназначенных для защиты от любых атак;
- расширенные функции безопасности, включая сетевую сегментацию, позволяющие разграничить доступ к сетевым ресурсам со стороны различных групп пользователей;
- специализированные аппаратное и программное обеспечение с высокими показателями производительности для защиты LAN и WAN сетей.

SSG 140 является идеальным решением защиты сетей предприятий среднего масштаба, где предъявляются повышенные требования к обеспечению безопасности и маршрутизации LAN/WAN-трафика.

SSG 140 представляет собой модульную платформу с производительностью 350 Мбит/с в режиме межсетевого экранирования и 100 Мбит/с в режиме IPSec VPN туннелирования.

SSG 140 имеет встроенные порты – восемь 10/100 и два 10/100/1000TX, а также 4 слота для установки интерфейсных модулей T1, E1, ISDN BRI S/T и Serial.

Безопасность

Технологии Stateful firewall и IPSec VPN вместе с UTM-функциями, включая IPS, антивирусное сканирование (в том числе защиту от вредоносного программного обеспечения и фишинга), антиспамовую и web- фильтрации позволяют защитить LAN/WAN трафик от червей, шпионских программ, Троянов и прочих атак.

Интеграция с LAN/WAN сетями

Комбинация LAN/WAN интерфейсных модулей и поддержка большого количества сетевых протоколов позволяет использовать SSG 140 как обычный межсетевой экран или как устройство сетевой безопасности с функциями маршрутизации, снижая общую стоимость владения (TCO).

Сетевая сегментация

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

Технические характеристики шлюзов безопасности SSG серии 140:

SSG 140	
Производительность и пропускная способность (1)	
Поддерживаемая версия ScreenOS	ScreenOS 5.4
Пропускная способность в режиме межсетевого экранирования (пакеты большой длины)	Более 350 Мбит/с
Пропускная способность в режиме межсетевого экранирования (смешанный трафик) (2)	300 Мбит/с
Производительность при обработке пакетов длиной 64 Байт	100 тыс. пакетов/с
Пропускная способность в режиме VPN-туннелирования (3DES)	100 Мбит/с
Максимальное число одновременных сессий	32 тыс.
Максимальная скорость обработки новых сессий	8 тыс. сессий/с
Максимальное число политик	500
Максимальное число пользователей	Неограниченное
Сетевая интеграция	
Встроенные интерфейсы	2 x 10/100, 4 x 10/100/1000
Общее количество слотов для установки интерфейсных модулей PIM	4
Интерфейсные модули WAN	2 x T1, 2 x E1, 1 xISDN BRI S/T, 2 x Serial
Режимы работы	
Layer 2 (прозрачный режим) (3)	да
Layer 3 (маршрутизатор и/или NAT)	да
Трансляция сетевых адресов	
NAT	да
PAT	да
Policy-based NAT/PAT	да
Virtual IP	да
Mapped IP	да
Межсетевое экранирование	
Обнаружение атак на сетевом уровне	да
Защита от DoS и DDoS атак	да
Повторная сборка TCP-сегментов	да
Защита от атак типа “Brute Force”	да
Механизм SYN cookie	да
Защита от IP-спуфинга	да
Возможность защиты от пакетов со структурными изменениями	да
Функции UTM/Защита контента(4)	
IPS (Deep Inspection)	да
Обнаружение аномалий в протоколах	да
Сигнатурный анализ	да
Борьба с технологиями обмана систем IPS/IDS	да
Антивирусный сканер	
Максимальное число сигнатур	Более 100 тыс.
Поддерживаемые протоколы	HTTP, FTP, SMTP, POP3, IMAP
Защита от шпионского ПО	да
Защита от Adware	да
Защита от keylogger	да
Антиспамовый фильтр	да
Встроенная URL-фильтрация	да
Внешняя URL-фильтрация(5)	да
Защита голосового трафика	
H.323 ALG	да
SIP ALG	да
MGCP	да
SCCP	да
NAT для VoIP	да

SSG 140	
VPN	
Максимальное число VPN-туннелей	125
Максимальное число туннельных интерфейсов	50
Алгоритмы шифрования DES (56-bit), 3DES (168-bit) и AES	да
Алгоритмы аутентификации MD-5 и SHA-1	да
Механизмы обмена ключами Manual Key, IKE, PKI (X.509)	да
Механизмы Perfect forward secrecy (DH - группы)	1, 2, 5
Защита от Replay - атак	да
Remote access VPN	да
L2TP внутри IPSec	да
IPSec NAT Traversal	да
Возможность резервирования VPN–шлюзов	да
Аутентификация в режимах межсетевого экранирования и VPN	
Максимальное число пользователей во внутренней базе	250
Протоколы аутентификации	RADIUS, RSA SecurID, LDAP
XAUTH VPN-аутентификация	да
WEB-аутентификация	да
802.1X	да
Маршрутизация	
Поддержка BGP	да
Поддержка OSPF	да
Поддержка RIPv1/v2	да
Динамическая маршрутизация	да
Статическая маршрутизация	да
Поддержка маршрутизации от источника	да
Поддержка маршрутизации на основе политик	да
Функция ECMP	да
Максимальное число статических маршрутов	2048
Поддержка Multicast - трафика	да
Reverse Forwarding Path (RFP)	да
IGMP (v1, v2)	да
IGMP Proxy	да
PIM SM	да
PIM SSM	да
Поддержка Multicast – трафика внутри VPN IPSec-туннелей	да
Инкапсуляция	
PPP	да
MLPPP	да
Максимальное число физических интерфейсов MLPPP	8
Frame Relay	да
MLFR (FTF 15, FRF 16)	да
Максимальное число физических интерфейсов MLFR	8
HDLC	да
Управление трафиком (QoS)	
Гарантированная полоса пропускания	да
Максимальная полоса пропускания	да, настраивается на физических интерфейсах
Ingress Traffic Policing	+
Распределение полосы пропускания на основе приоритетов	+
Поддержка DiffServ stamp	да, настраивается в политиках
Управление устройством	
Web-интерфейс (HTTP и HTTPS)	да

Интерфейс командной строки (консоль)	да
Интерфейс командной строки (Telnet)	да
Интерфейс командной строки (SSH)	да
Поддержка NetScreen-Security Manager	да
Управление через VPN на любом интерфейсе	да
SNMP Full Custom MIB	да
Функция Rapid deployment	нет

Протоколирование событий и мониторинг

Syslog (несколько внешних серверов)	да
Возможность оповещения администраторов системы по электронной почте (на 2 адреса)	да
Поддержка NetIQ WebTrends	да
Поддержка SNMP (v2)	да
Поддержка Traceroute	да
Мониторинг VPN туннеля	да

Виртуализация

Максимальное число зон безопасности	40
Максимальное число виртуальных маршрутизаторов	3
Максимальное число VLAN	100

Функции высокой доступности

Выделенные HA интерфейсы	нет
Active/Passive	да
Синхронизация конфигурации	да
Синхронизация сессий в режиме VPN и межсетевого экранирования	да
Восстановление сессий в случае изменения маршрута	да
Обнаружение отказа устройства в кластере	да
Обнаружение отказа линии связи	да
Аутентификация устройства в кластере	да
Возможность шифрования трафика в кластере	да

Назначение IP-адресов

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

Поддержка PKI

PKCS 7/ PKCS 10	да
SCEP	да
OCSP	да
Поддерживаемые удостоверяющие центры	Verisign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape), Baltimore, DOD PKI

Администрирование

Максимальное число локальных администраторов	20
Внешние системы администрирования	RADIUS, LDAP, SecurID
Максимальное число административных подсетей	6
Уровни администрирования Root Admin, Admin, and Read Only	да
Обновление программного обеспечения	да
Откат к предыдущей рабочей конфигурации	да

Внешняя Flash - память

Дополнительное хранилище событий (logs)	USB 1.1
Запись и хранение событий (logs и alarms)	да
Запись и хранение файлов конфигураций	да
Запись и хранение образа операционной системы	да

Физические параметры

Габаритные размеры (высота/ширина/глубина)	4.3 см /44 см /37.5 см
Вес	4,6 кг
Возможность установки в стандартную стойку	да (1U)
Источник питания напряжения постоянного тока	Входное напряжение 90-240 В, 50-60 Гц, 2А
Тепловыделение	580 BTU/час (170 Вт)

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	От 0°C до +50 °C
Температура хранения	От -20°C до + 70 °C
Допустимая влажность	10% – 90%
MTBF (Bellcore model)	16 лет

[1] Указанные значения производительности, пропускной способности и других характеристик получены при тестировании устройств с установленной операционной системой ScreenOS версии 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, на 33,33% из пакетов размером 570 Байт и на 8,33% из пакетов 1518 Байт.

[3] В режиме Transparent не поддерживаются функции NAT, PAT, policy based NAT, VIP, MIP, виртуальные системы, виртуальные маршрутизаторы, VLAN, OSPF, BGP, RIPv, кластеры Active/Active, возможность назначения IP-адресов.

[4] Функции UTM (IPS/Deep Inspection, антивирусный сканер, антиспамовый и Web фильтры) становятся доступными после приобретения ежегодной подписки от Juniper Networks. Ежегодная подписка предоставляет возможность обновления сигнатур и обеспечивает соответствующую техническую поддержку. Для реализации функций UTM необходим максимальный объем оперативной памяти.

[5] Функция внешней WEB-фильтрации предусматривает использование серверов SurfControl или WebSense, которые приобретаются отдельно.

Пакеты Stateful-сигнатур подсистемы Deep Inspection

Поставляемые пакеты сигнатур подсистемы Deep Inspection оптимизированы для решения специфических задач и в зависимости от вариантов развертывания устройств

Наименование пакета	Варианты развертывания	Назначение	Типы атак
Base	Региональные офисы Небольшие и средние предприятия	Защита клиент-серверных приложения и защита от вирусов	Все атаки уровня «Critical»
Client	Удаленные офисы	Защита периметра, защита хостов	Все атаки в направлении от сервера к клиенту
Server	Удаленные офисы	Защита периметра, защита серверов	Все атаки в направлении от клиента к серверу
Worm Mitigation	Удаленные/региональные офисы крупных предприятий	Защита от вирусов	Вирусные атаки (черви, Трояны)

Информация для заказа

Продукт	Номер для заказа
SSG 140	
SSG 140 с 256 Мбайт ОЗУ, без модулей PIM, блок питания напряжения постоянного тока	SSG- 140-SB
SSG 140 с 512 Мбайт ОЗУ, без модулей PIM, блок питания напряжения постоянного тока	SSG- 140-SH
Интерфейсные модули	
2 x T1 PIM	JX-2T1-RJ48-S
2 x E1 PIM	JX-2E1-RJ48-S
2 x Serial PIM	JX-2Serial-S
1 ISDN BRI S/T PIM	JX-1BRI-ST-S
Наборы для Upgrade	
Upgrade ОЗУдо 512MB	SSG-100-MEM-512
Пакеты подписки - UTM функции/защита контента	
Антивирусное сканирование (защита от шпионского ПО, антифишиг)	NS-K-AVS-SSG 140
Deep Inspection	NS-DI-SSG 140
WEB-фильтрация	NS-WF-SSG 140
Антиспамовая фильтрация	NS-SPAM-SSG 140
Комплект подписки для удаленных офисов (Антивирусное сканирование, Deep Inspection, WEB-фильтрация)	NS-RBO-CS-SSG 140
Комплект подписки для головных офисов офисов (Антивирусное сканирование, Deep Inspection, WEB-фильтрация, Антиспамовая фильтрация)	NS-SMB-CS-SSG 140

Landata
ТОЧКА ОПОРЫ

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

Juniper NETWORKS

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