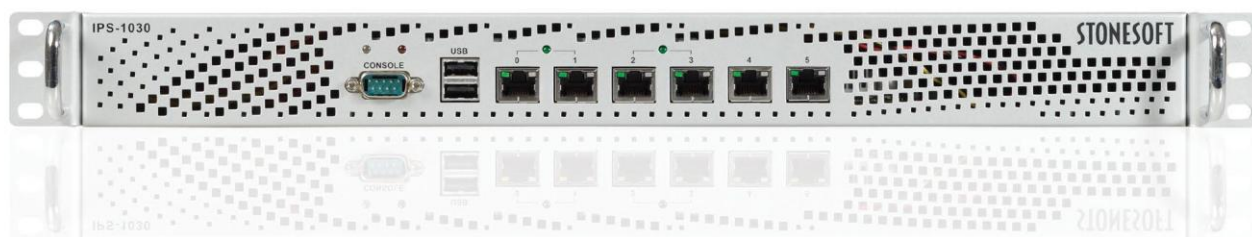


StoneGate™ IPS-1030



Документация Модуля StoneGate™ IPS

Программно- аппаратный комплекс StoneGate™ IPS-1030 Intrusion Prevention System – система проактивной защиты, предназначенная для определения злонамеренных пакетов внутри сетевого трафика и предотвращения вторжений, путем их автоматической блокировки, до того, как они нанесут урон. Новая возможность SSL-инспекции позволяет контролировать зашифрованный web-трафик и предотвращать нарушения бизнес-трафика.

StoneGate IPS-1030 предназначен для небольших организаций, филиалов компании, демилитаризованных зон DMZ, экстранета или внутренних сегментов сети. Модуль обладает функциональностью сенсора и анализатора, дающих гибкую защиту для оборудования, требующего максимальную свободу для действий. Для увеличения возможностей работы StoneGate IPS-1030 может быть настроен в отдельных режимах сенсора или анализатора.

StoneGate IPS-1030 сенсор может защищать свыше двух inline-сегментов сети. В сенсоре имеется двойной bypass-интерфейс для каждого inline-участка и два стандартных Ethernet-порта. Стандартные интерфейсы могут быть использованы как захватывающие интерфейсы для найденного вторжения и один из них нужен для управления устройством.

Совмещенный с StoneGate Firewall и технологией Transparent Access Control, IPS-1030 формирует многоуровневую систему безопасности, где несколько защитных слоев равномерно соединены. Эта испытанная технология обеспечивает целостную защиту всей сети, поднимающую сетевую безопасность на высший уровень.

StoneGate IPS-1030 и остальные StoneGate-решения предлагают всестороннюю сетевую безопасность с объединенным управлением и простым развертыванием.

StoneGate™ IPS-1030 Спецификация



Характеристики

Защита	Приложений, ОС, клиентских/ серверных уязвимостей от сетевых атак
Детектирование	Перегрузки, DoS/DdoS, backdoor (люки), шпионское ПО, черви, трояны, провокации, корреляция событий, Zero-day-атаки, P2P, IM, потоковое медиа
Web-фильтрация	Решение содержит миллионы URL-адресов в 77 категориях, гарантирующее точный мониторинг и контроль просмотра web-сайтов. Опциональная лицензия.
Распознаваемые сигнатуры	3 500 +

Глубокое инспектирование

Протоколы	Полная расшифровка и анализ: Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, SMTP, SSH, NBT, SMB, MSRPC, POP3, SIP, TFTP, HTTPS (SSL/TLS)
Детектирование внутренних угроз	Запись и корреляция событий для более 170 протоколов и приложений
DoS/DDoS защита	Суп-флуд, UDP-флуд, Connection-флуд
Расследование	Обнаружение TCP/UDP/ICMP – сканирования, а также, распределенных во времени

Контроль доступа

Приложения	Контроль сетевых приложений, P2P, IM, Web-браузеров, удаленного доступа и туннелирующих протоколов
IPv4/IPv6	Контекстный контроль и регистрация
Ethernet	Фильтрация пакетов и регистрация для любого Ethernet-трафика (Dix/IEEE)

Особенности

Отказоустойчивость и кластеризация	Inline- кластеризация (active-active/active-passive) IDS- кластеризация (active-active/act-pas)
	Встроенная bypass -технология (bypass/normal)
МСЭ 2-го уровня	МСЭ типа Layer-2, следующее поколение МСЭ
SSL-инспекция	Расшифровка и инспекция входящего HTTPS-трафика Расшифровка и инспекция исходящего HTTPS-трафика
VLAN-инспекция	Максимальное количество проверяемых VLAN (802.1q) составляет 4094
Управление динамическими перегрузками	Приоритет в установлении соединений выше инспектирования и ниже перегрузки IPS-модуля (настраиваемая опция)
Опциональные	Web-фильтрация

Управление и мониторинг

Через StoneGate Management Center	Централизованное управление на уровне предприятия. Отчетность. Больше деталей в документации StoneGate Management Center
SNMP	SNMPv1, SNMPv2c и SNMPv3

Сертификаты

ICSA NIPS Certified	Продолжительное тестирование ICSA Labs.
---------------------	-----------------------------------------

Особенности

Пропускная способность	200 Мбит/с
Задержка	< 150 мкс
Одновременные соединения	> 300 000
Соединений в секунду	> 15 000
SSL-инспекция для клиента/сервера	40 Мбит/с / 40 Мбит/с

Оборудование

Сетевые интерфейсы	
Ethernet	6 x 10/100/1000 Мбит/с
Вурасс-интерфейсы	2
Разъемы	RS-232, 2 x USB

Размеры

Форм-фактор	1U 19" rack unit
Ш x В x Д	425 x 44 x 362 мм / 16.73 x 1.73 x 14.25 дюймов
Вес нетто	5.5 кг / 12.13 фунтов
Вес брутто	8.5 кг / 18.74 фунтов

Классы безопасности

	CE, FCC Class B, LVD, CB, Gost-R, RoHS
--	----------------------------------------

Электропитание

Характеристики	180 Вт, AC Input 100-240 В, 50-60 Гц
Среднее потребление	90 Вт

Разное

Рабочие температуры / влажность	5–35 °C (41–95 °F) / 5%–95%
Температура хранения / влажность	-20–70 °C (-4–158 °F) / 5%–95%
Среднее время до отказа	120 000 часов

Поддержка

Услуга замены аппаратного обеспечения	15 или 39 месяцев для неисправного оборудования
Premium-поддержка	Круглосуточно через web, почту и телефон, реагирование на следующий рабочий день. Обновления ПО. Услуга замены.
Базовая	В рабочее время через web, почту и тел. реагирование на следующий рабочий день. Обновления ПО. Услуга замены.

Код продукта

APP-IPS-1030-C4	StoneGate IPS-1030 модуль
APP-IPS-1030-C1-Z	StoneGate IPS-1030Z analyzer-модуль
FP-IPS-ANZ1	Программный Analyzer для IPS-1030
FP-1Y-WF2-151	Лицензия на web-фильтрацию сроком в 1 год для IPS-1030