

StoneGate™ IPS-1205



Документация Модуля StoneGate IPS

Программно- аппаратный комплекс StoneGate™ IPS-1205 Система Предотвращения Вторжений осуществляет оперативное управление и защиту от угроз для современных корпоративных сетей. Модуль StoneGate™ IPS-1205 предоставляет организациям полную прозрачность и контроль поверх трафика сетевых приложений. Это помогает обеспечить компетентной информацией внешних аудиторов и выполнить условия стандарта PCI (Payment Card Industry).

Обладая производительностью в 2 Гбит/с, StoneGate™ IPS-1205 обеспечивает высочайший уровень защиты без ущерба для скорости трафика через сеть. Комплекс прост в развертывании на любом сегменте сети и оборудован двумя парами соединений, которые можно одновременно настроить, как инспектирующие каналы. В то же время, стоимость восстановления незащищенных компьютеров в сети, а также, время простоя, могут оказаться непоправимыми для любой организации.

StoneGate™ IPS-1205 обеспечит надежную и экономичную защиту для дата-центров, а также, предотвращение атак, распределенных во времени, существенно сберегая активы организации, сохраняя и гарантируя непрерывность бизнеса во все времена.

StoneGate™ IPS-1205 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
Расознаваемые 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	Сун-флуд, UDP-флуд, Connection-флуд
Расследование	Обнаружение TCP/UDP/ICMP –сканирований, 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) Настраиваемый bypass
MCЭ 2-го уровня	MCЭ типа Layer-2, следующее поколение MCЭ
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)

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
---------------------	--

Производительность

Пропускная способность	2 Гбит/с
Одновременные соединения	1 300 000
Соединений в секунду	50 000
SSL-инспекция клиент/сервер	350 / 350 Мбит/с
MCЭ типа Layer-2	+
Web-фильтрация	опционально
Задержка	< 150 мкс

Оборудование

Сетевые интерфейсы

Ethernet	2 x 10/100/1000 Мбит/с 4 x 10/100/1000 Ethernet bypass (2 пары)
Разъемы	Console RJ45, 2 x USB

Размеры

Форм-фактор	1U 19" rack unit
Ш x В x Д	426 x 44 x 400 мм / 16.77 x 1.73 x 15.7 дюймов
Вес нетто	6.25кг / 13.8 фунта

Классы безопасности

	CE, FCC, CB, Gost-R, RoHS
--	---------------------------

Электропитание

Характеристики	AC input: 100-240 В, 50-60 Гц, 250Вт DC input: -72 - -36В, 200Вт
Среднее потребление	85-150 Вт

Разное

Рабочие температуры/ относительная влажность	+5–35 °C (41–95 ° F) 10%–90%
Температура хранения/ относительная влажность	-20–75 °C (-4–167 ° F) 10%–95%
Среднее время до отказа	120 000 часов

Поддержка

Услуга замены аппаратного обеспечения	15 или 39 месяцев для неисправного оборудования
Премиум –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-1205-C1	StoneGate IPS Модуль, AC Блок питания
APP-IPS-1205-C2	StoneGate IPS Модуль, DC Блок питания
FP-IPS-ANZ5	Analyzer Модуль для IPS-1205
FP-1Y-WF2-196	Web фильтрация для IPS-1205 в течение года
APP-RACK-1205	Серверная стойка