

StoneGate™ IPS-3205



Документация Модуля StoneGate IPS

Программно- аппаратный комплекс StoneGate™ IPS-3205 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.

Серия StoneGate™ 3200 включает в себя устройства, обеспечивающие высокую гибкость развертывания, и масштабируемость, путем использования Экспресс-Модулей (Express Modules) и SFP – трансиверов.

StoneGate™ IPS-3205 –это наращиваемое модульное устройство, предназначенное для защиты от атак реального времени и контроля приложений. Модуль соответствует высочайшим требованиям к защите и надежности для высокоскоростных дата –центров, провайдеров управляемых услуг (MSP) и операторов сетевого оборудования.

StoneGate™ IPS-3205 предоставляет непревзойденную защиту, совмещенную с максимальной прозрачностью и контролем поверх трафика сетевых приложений. Со скоростью глубокой проверки в 13 Гбит/с, и поддержкой до 15 миллионов одновременных соединений, StoneGate™ IPS-3205 обеспечивает высочайший уровень безопасности без ограничения скорости трафика через сеть.

Совмещенная с межсетевым экраном StoneGate Firewall, система предотвращения вторжений StoneGate IPS-3205, формирует многоуровневую систему безопасности в которой защитные слои, включая контроль доступа, предотвращение вторжений и идентификация приложений органично соединены. Эта испытанная технология обеспечивает целостную защиту всей сети.

Модуль StoneGate™ IPS-3205 и остальные StoneGate™ - решения предлагают всестороннюю сетевую безопасность с объединенным управлением и простым конфигурированием. Это оптимизирует данное решение при развертывании на любых географически распределенных подразделениях.

StoneGate™ IPS-3205 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	Syn-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)
Настраиваемый bypass	Сетевые интерфейсы с Экспресс-Модулями
МСЭ 2-го уровня	МСЭ типа Layer-2, следующее поколение МСЭ
SSL инспекция	Расшифровка и инспекция входящего/ 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
---------------------	--

Особенности

Пропускная способность	13 Гбит/с
Одновременные соединения	15 000 000
Соединений в секунду	750 000

SSL-инспекция для клиента/ сервера	+ / +
МСЭ типа Layer-2	+
Web-фильтрация	опционально, при дополнительной лицензии
Задержка	< 150 мкс

Оборудование

Сетевые интерфейсы	
Фиксированные	2 x 10/100/1000 Мбит/с
Слоты	3 (Доступные платы в разделе «код продукта»)

Разъемы	4 x USB, 1 serial, VGA, IPMI ethernet
---------	---------------------------------------

Размеры	
Форм-фактор	2U 19" rack unit
Ш x В x Д	437 x 89 x 450 мм / 17.2" x 3.5" x 17.7"
Вес нетто	16 кг / 35 фунта

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

Электропитание	
Характеристики	1+1 резервный 700Вт + 700Вт

Разное	
Рабочие температуры/ относительная влажность	+10—+35° C (+50... +95° F) 8%-90%
Температура хранения/ относительная влажность	-40—+70° C (-40...158° F) 5%-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-3205-C1	StoneGate IPS модуль, AC Блок питания

Экспресс модули	
MOD-EM1-GE-4-B	модуль на 4 порта Gigabit Ethernet
MOD-EM1-GE-SX-2-B	модуль на 2 порта Gigabit Ethernet SX
MOD-EM1-10G-SR-2-B	модуль на 2 порта 10 Gigabit Ethernet SR
MOD-EM1-10G-LR-2-B	модуль на 2 порта 10 Gigabit Ethernet LR

Код дополнений	
FP-1Y-WF2-194	Web-фильтрация сроком в 1 год для IPS-3205
APP-RACK1-3200	Монтажная стойка (2 полки)
APP-RACK2-3200	Монтажн. стойка (500 - 680 мм/ 19,7" - 26,8")
APP-RACK3-3200	Монтажн. стойка (680 - 920 мм/ 26,8" - 36,2")
MOD-PSU-DC-3200	DC Блок питания для серии 3200