УДК: 004.72.056.52:004.492.2

Межсетевой экран на примере ССПТ-2-06

Тимохина Н.Ю., ФГБОУ ВПО «Госуниверситет — УНПК»,
11-ИБ

Межсетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей межсетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также межсетевые экраны часто называют фильтрами, так как их основная задача— не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые межсетевые экраны также позволяют осуществлять трансляцию адресов— динамическую замену внутрисетевых адресов или портов на внешние, используемые за пределами ЛВС (локально вычислительная сеть).

Межсетевой экран ССПТ-2-06 (специализированный сетевой процессор для телематических сетей) разработки ЗАО НПО РТК. Как утверждают сами представители компании-разработчика, ССПТ-2 представляет собой персональный компьютер специального исполнения с установленной операционной системой FreeBSD. Уникальностью продукта называется его возможность работы в прозрачном режиме.

FNP типа ССПТ-2-06 является сертифицированным ФСТЭК И ФСБ межсетевым экраном нового поколения (патент РФ 2214623, патент US 7281129), реализующим функции межсетевого экрана, но при этом остающимся «невидимым» для любых протоколов и тестовых воздействий, что достигается за счет отсутствия физических и логических адресов на его фильтрующих интерфейсах.

Скрытность функционирования межсетевого экрана повышает надежность системы защиты в целом и существенно упрощает процедуру установки ССПТ-2-

06 в существующие компьютерные сети и функционирующие на их основе информационные и телематические системы.

Назначение и область применения:

На базе ССПТ-2-06 реализуются высокоэффективные масштабируемые решения по защите информации в компьютерных сетях на базе технологии Ethernet. Устройство FNP используется как:

1.Основное средство защиты для реализации различных политик информационной безопасности с помощью:

-фильтрации пакетов на канальном, сетевом, транспортном и прикладном уровнях;

-управления транспортными соединениями между отдельными узлами ЛВС или виртуальной ЛВС (VLAN);

-контроля контента данных на прикладном уровне с учетом направления, времени и типа протоколов передачи трафика.

2.Дополнительное устройство защиты для:

-обеспечения безопасности функционирования ранее установленных в компьютерной сети средств защиты и устройств маршрутизации;

-мониторинга трафика с возможностью анализа данных регистрации пакетов по различным критериям и интеграции с IDS;

-обеспечения функционирования сетевых распределенных телематических приложений и GRID ресурсов.

Характеристики:

-количество фильтрующих интерфейсов - 2

-тип интерфейса - Ethernet 10BASE-T/100BASE-TX/1000BASE-TX

-скорость, мбит/сек - 1000

-количество управляющих интерфейсов - 2

-тип интерфейса - Ethernet 10BASE-T/100BASE-TX/1000BASE-TX

-тип корпуса - стоечное исполнение 1U

-габаритные размеры - 460x430x44 мм

Функциональные характеристики:

-Многоуровневая скрытная фильтрация пакетов по совокупности критериев.

-Контроль транспортных соединений (до 40000 TCP сессий) на основе проверки соответствия каждого пакета контексту выбранной TCP сессии.

-Трансляция сетевых адресов (режим NAT) в режиме «стелс» для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны».

-Блокировка компьютерных flood-атак на основе фильтрации аномальной активности сетевых потоков данных.

-Регистрация системных событий и полных заголовков обработанных пакетов на всех уровнях межсетевого взаимодействия.

-Ведение журналов регистрации пакетов и их выгрузкапо запросам администратора сети с использованием протоколов FTP и SYSlog.

-Защита каналов управления с использованием алгоритмов шифрования, реализованных в OpenSSL.

-Аутентификация и авторизация администратора с помощью протокола RADIUS.

-Контроль доступа к интерфейсу управления на основе списка доверенных сетевых адресов.

-Синхронизация системного времени по протоколу NTP.

Режим скрытной фильтрации для систем защиты информации:

Применение системы защиты, состоящей из межсетевых экранов, функционирующих в режиме скрытной фильтрации или в режиме «стелс» позволяет не только гарантировать безопасность сетевых приложений в соответствии с РД ФСТЭК и ФСБ, но и повышает надежность работы системы защиты в целом.

Устройства защиты типа FNP в режиме «стелс» невозможно обнаружить никакими известными средствами удаленного мониторинга сети.

Межсетевые экраны типа ССПТ отвечают требованиям современных стандартов безопасности для устройств 3-го класса защиты и имеют сертификат ФСБ РФ N СФ/525-1093.

Список литературы:

1. Межсетевой экран-специализированный сетевой процессор для телематических сетей ССПТ-2-06 [Электронный ресуср]:(с изм. и доп.)-Режим доступа: http://linuxcenter.ru/shop/sertified_fstek/firewall_fstek/sspt_firewall/setevoy_proceccor_sspt_2_06 (дата обращения 13.11.2012)

2. Сертифицированные межсетевые экраны,информационный портал по безопасности [Электронный ресурс]:(с изм. и доп.)- Режим доступа : http://securitylab.ru/blog/personal/zlonov/25278 (дата обращения 13.11.2012)

3.Межсетевой экран-специализированный сетевой процессор для телематических сетей ССПТ-2-06 [Электронный ресуср]:(с изм. и доп.)- Режим доступа: http://dlp-expert.ru/blog/2466/18448 (дата обращения 13.11.2012)