УДК 004.056.57

ПРЕИМУЩЕСТВА ИНТЕГРИРОВАННЫХ IPS

Гержан С.Г., Масальская Е.А.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, 825800@mail.ru

В данной работе рассмотрены интегрированные системы предотвращения вторжений, их принцип действия, а также описаны основные преимущества данных систем в сравнении с остальными существующими системами.

Ключевые слова – IPS, IDS, TCP, защита от вторжений

ВВЕДЕНИЕ

Системы предотвращения вторжений (англ. Intrusion Prevention System) можно рассматривать как расширение Систем обнаружения вторжений (англ. Intrusion Detection System). Они отличаются от IDS тем, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Возможные меры – блокировка потоков трафика в сети, сброс соединений, выдача сигналов о вторжении в сеть оператору. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами. Выполняя проверку TCP/IP пакетов и блокируя нежелательный трафик, IPS являются обязательным компонентом инфраструктуры безопасности практически для любой сети.

ПРЕИМУЩЕСТВА ИНТЕГРИРОВАННЫХ СИСТЕМ

Существует два типа IPS: отдельные (или специальные) и интегрированные.

Отдельные IPS обеспечивают:

- дополнительный уровень сетевой защиты от вторжений;
- возможность установки посредством выделенного специализированного оборудования.

Интегрированные IPS предлагают:

- комплексную систему защиты от вторжений по всей инфраструктуре безопасности;
- возможность интеграции в существующие узлы безопасности, как правило, в межсетевые экраны.

Среди преимуществ интегрированных IPS можно отметить следующие.

Сокращение затрат. Покупка и установка нескольких устройств безопасности обычно является более дорогостоящей, чем установка комплексного решения. Сокращаются как прямые издержки на покупку оборудования, так и косвенные расходы на обучение сотрудников и техническую поддержку, а также производится дополнительная экономия пространства, кабелей и электроэнергии.

Уменьшение задержек. Назначение IPS и межсетевых экранов заключается в защите трафика и информации, поступающей по каналам Интернет, а также между сетями с разным уровнем конфиденциальности. Поскольку межсетевые экраны проверяют весь трафик, проходящий через них, логично, что IPS также инспектируют соответствующий трафик. Качественные интегрированные решения проверяют трафик лишь один раз, выполняя при этом обе функции и сокращая временные задержки, характерные при выборе отдельных устройств IPS.

Связанная политика безопасности.

С увеличением количества отдельных устройств повышается сложность политик и правил, настраиваемых на каждом устройстве, а также возрастает число потенциальных слабых мест в общей инфраструктуре безопасности. Неправильно настроенное устройство повышает вероятность успешной хакерской атаки, либо множественной проверки трафика, а также может привести к проникновению вредоносного ПО в корпоративную сеть. В интегрированных решениях применяется единая связанная политика безопасности, которую проще настраивать и контролировать.

Управление и обучение. Установка нескольких решений различных вендоров повышает сложность технической поддержки и требует комплексной подготовки персонала. Интегрированные решения не только сокращают расходы на поддержку и обучение, но и понижают вероятность ошибок в управлении, поскольку в большинстве случаев межсетевые экраны и системы защиты от вторжений относятся к одной и той же сетевой группе безопасности.

Установка IPS. В силу того, что межсетевые экраны в современных интегрированных сетях устанавливаются во многих местах, добавление к ним функционала IPS сокращает финансовые и организационные проблемы, связанные с покупкой и внедрением дополнительных устройств.

ВЫВОДЫ

Несмотря на тот факт, что в будущем ожидается постепенный переход на интегрированные IPS, все же остаются некоторые ситуации, в которых требуется установка отдельных IPS. Они рекомендуются для тех частей сети, где не устанавливаются межсетевые экраны: если трафик, проходящий между определенными компонентами сети, не защищается межсетевым экраном, то в них желательно установить отдельные устройства IPS. Кроме того, если поддержка функционала IPS и межсетевых экранов относится к разным сетевым группам безопасности, то использование отдельного устройства IPS может быть обосновано в силу практических причин, даже при более уместном интегрированном решении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Система предотвращения вторжений и сетевых атак (Электрон. ресурс) / Способ доступа: URL: http://ithayot.zn.uz/87
2. Система предотвращения вторжений (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/Система_предотвращения_вторжений/
3. Intrusion Prevention Systems: новый шаг в развитии IDS (Электрон. ресурс) / Способ доступа: URL: http://linux.yaroslavl.ru/docs/conf/security/ids/ids.html
4. Обзор систем IPS (Электрон. ресурс) / Способ доступа: URL: http://www.itsec.ru/articles2/techobzor/obzor-sistem-ips-v-chem-raznica
5. Предотвращение сетевых атак: технологии и решения (Электрон. ресурс) / Способ доступа: URL: http://citforum.ru/security/articles/ips/