УДК. 004.9:621.39

ТЕХНОЛОГИИ IDS/IPS ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ТЕЛЕКОММУНИКАЦИОННУЮ ИНФРАСТРУКТУРУ

Шевченко Тарас Николаевич, *магистрант группы ИТССм-1-16, направления 690300 Инфокоммуникационные технологии и системы связи, ИЭТ КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66. E-mail:taras_taras1@mail.ru*
Зимин Игорь Викторович, *к.т.н., доцент ИЭТ при КГТУ им. И. Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Ч. Айтматова 66. E-mail: igorzimin777@rambler.ru*

В данной статье рассматривается принцип работы технологии IDS/IPS, которая направлена на обнаружения и предотвращения вторжений в телекоммуникационную инфраструктуру.

Ключевые слова: Файервол, IDS, IPS, обнаружения вторжений, блокировка, приложения, пакет, трафик, протокол.

IDS / IPS TECHNOLOGIES FOR THE DETECTION AND PREVENTION OF INTRUSION OF TELECOMMUNICATIONS INFRASTRUCTURE

Shevchenko Taras Nikolaevich*: master of the group ITSSm-1-15, directions 690300 Info communication technologies and communication systems, IET at KSTU named after. I. Razzakov, Kyrgyzstan, 720044, Bishkek city, Aitmatova Ave. 66. E-mail: taras_taras1@mail.ru*

Zimin Igor Viktorovich, *Ph.D., Associate Professor of IET at KSTU. I. Razzakov, Kyrgyzstan, 720044, Bishkek city, Aitmatova Ave. 66. E-mail: igorzimin777@rambler.ru.*

This article discusses the principle of the IDS / IPS technology, which is aimed at detecting and preventing intrusions into the telecommunications infrastructure.

Keywords: firewall, IDS, IPS, intrusion detection, blocking, applications, packet, traffic, protocol.

Введение. В настоящее время защита, обеспечиваемая файерволом и антивирусом, уже не эффективна против сетевых атак и малварей. На первый план выходят решения класса IDS/IPS (рис. 1), которые могут обнаруживать и блокировать как известные, так и еще не известные угрозы. [1]

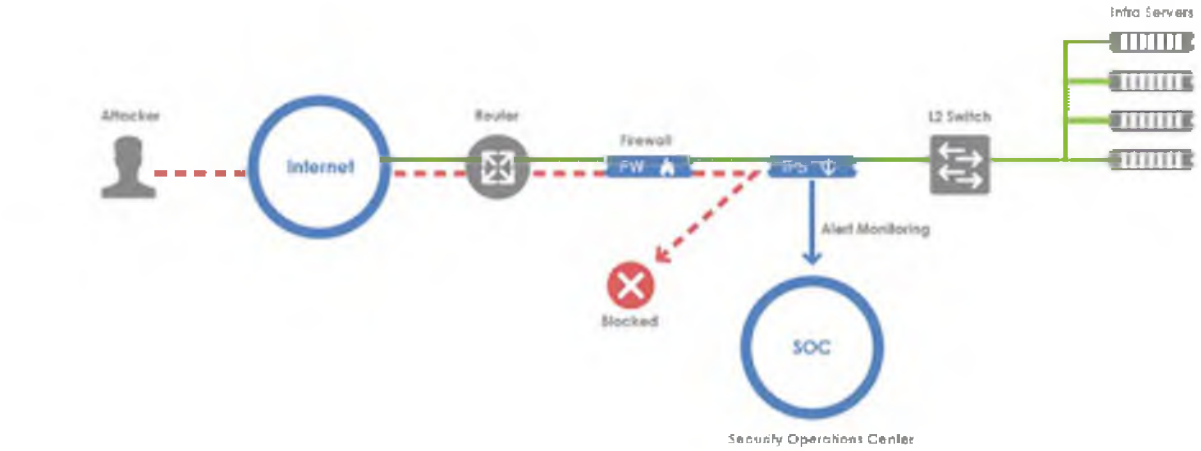

Рисунок 1. Структурная схема сети с использованием IPS

Благодаря технологии IDS/IPS мы можем вывести системы обнаружения вторжений на новый уровень. Чтобы сделать выбор между IDS или IPS, следует понимать их принципы работы и назначение. Система обнаружения вторжений (IDS – Intrusion Detection System) – это решение, обеспечивающее мониторинг событий, происходящих в информационной системе и их анализ на наличие признаков вторжения в систему: нарушения конфиденциальности и целостности информации, и других правил политики информационной безопасности.[2]

Так, задача IDS (Intrusion Detection System) состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В зависимости от типа, IDS умеют выявлять различные виды сетевых атак, обнаруживать попытки неавторизованного доступа или повышения привилегий, появление вредоносного ПО, отслеживать открытие нового порта и т. д. В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные. Существует несколько видов систем обнаружения вторжений. Весьма популярны APIDS (Application protocol-based IDS), которые мониторят ограниченный список прикладных протоколов на предмет специфических атак. Типичными представителями этого класса являются PHPIDS, анализирующий запросы к PHP-приложениям, Mod_Security, защищающий веб-сервер (Apache), и GreenSQL-FW, блокирующий опасные SQL-команды (Рис.2) [1](см. статью «Последний рубеж»).

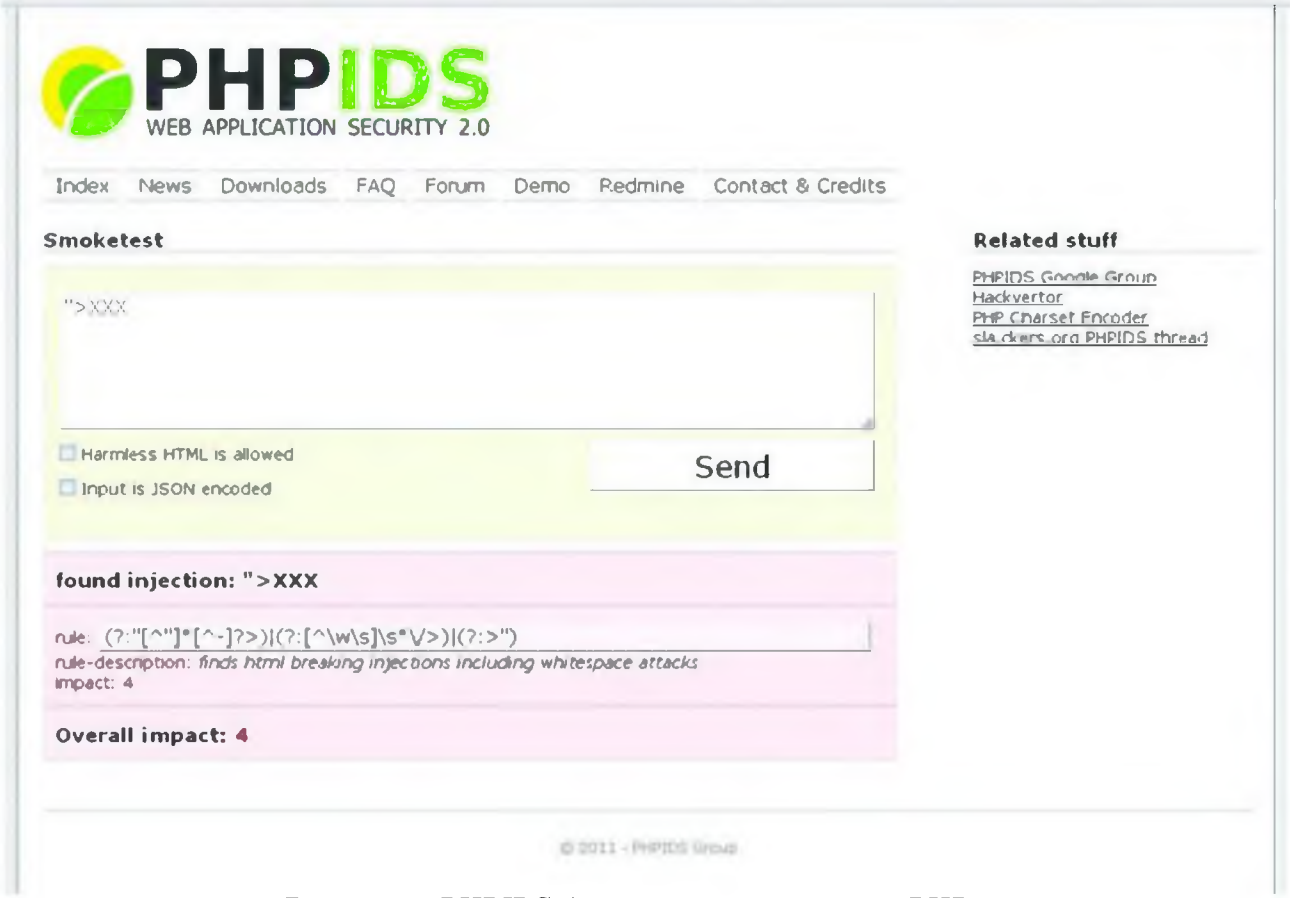

Рисунок 2. *PHPIDS блокирует неправильные PHP-запросы*

Сетевые NIDS (Network Intrusion Detection System) более универсальны, что достигается благодаря технологии DPI (Deep Packet Inspection, глубокое инспектирование пакета). Они контролируют не одно конкретное приложение, а весь проходящий трафик, начиная с канального уровня.

Для некоторых пакетных фильтров также реализована возможность «заглянуть внутрь» и блокировать опасность. В качестве примера можно привести проекты OpenDPI и Fwsnort. Последний представляет собой программу для преобразования базы сигнатур Snort в эквивалентные правила блокировки для iptables. Но изначально файервол заточен под другие задачи, да и технология DPI «накладна» для движка, поэтому функции по обработке дополнительных данных ограничены блокировкой или маркированием строго определенных протоколов. IDS всего лишь помечает (alert) все подозрительные действия. Чтобы заблокировать атакующий хост, администратор самостоятельно перенастраивает брандмауэр во время просмотра статистики. Естественно, ни о каком реагировании в реальном времени здесь речи не идет. Именно поэтому сегодня более интересны IPS (Intrusion Prevention System, система предотвращения атак). Они основаны на IDS и могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, отсылая TCP RST. В зависимости от принципа работы, IPS может устанавливаться «в разрыв» или использовать зеркалирование трафика (SPAN), получаемого с нескольких сенсоров. Например, в разрыв устанавливается Hogwash Light BR, которая работает на втором уровне OSI. Такая система может не иметь IP-адреса, а значит, остается невидимой для взломщика.

В обычной жизни дверь не только запирают на замок, но и дополнительно защищают, оставляя возле нее охранника, ведь только в этом случае можно быть уверенным в безопасности. В IT в качестве такого секьюрити выступают хостовые IPS[1] (см. «Новый оборонительный рубеж»), защищающие локальную систему от вирусов, руткитов (набор

программных средств)[4] и взлома. Их часто путают с антивирусами, имеющими модуль про активной защиты. Но HIPS, как правило, не используют сигнатуры, а значит, не требуют постоянного обновления баз. Они контролируют гораздо больше системных параметров: процессы, целостность системных файлов и реестра, записи в журналах и многое другое.

Чтобы полностью владеть ситуацией, необходимо контролировать и сопоставлять события как на сетевом уровне, так и на уровне хоста. Для этой цели были созданы гибридные IDS, которые коллектят данные из разных источников (подобные системы часто относят к SIM — Security Information Management). Среди OpenSource-проектов в свободном доступе интересен Prelude Hybrid IDS, собирающий данные практически со всех OpenSource IDS/IPS и понимающий формат журналов разных приложений (поддержка этой системы приостановлена несколько лет назад, но собранные пакеты еще можно найти в репозиториях Linux (специальные хранилища))[3].

В разнообразии предлагаемых решений может запутаться даже профи. Сегодня мы познакомимся с наиболее яркими представителями IDS/IPS-систем.

Система предотвращения вторжений (IPS – Intrusion prevention system) – решение, обеспечивающее блокировку выявленных вторжений.

В целом IPS по классификации и свои функциям аналогичны IDS. Главное их отличие состоит в том, что IPS может в автоматическом режиме блокировать сетевые атаки. Каждая IPS включает в себя модуль IDS.

На современном этапе развития информационных систем существует достаточно большое число способов, позволяющих злоумышленникам атаковать компьютерные сети. Результатом атак, как правило, является похищение или порча информации, а также сбои в работе информационной инфраструктуры предприятия.

Чтобы обезопасить свою сеть от подобных угроз, многие компании сегодня задумываются над вопросом своевременного обнаружения атак, защиты корпоративной сети, что является первым шагом к успешному противодействию им.

Именно с этой целью на базе продуктов компаний «Cisco Systems», «Check Point Software Technologies», «Stonesoft» и «Symantec» были разработаны решения по обнаружению и предотвращению вторжений для сетевых корпоративных ресурсов. Данные решения, наблюдая за сетевой активностью, позволяют выявить аномальные или опасные события в информационной системе предприятия.

Использование средств IDS/ IPS позволяет достичь следующих целей:

- ✓ обнаружить сетевую атаку (система обнаружения атак);
- ✓ спрогнозировать возможные будущие атаки для предотвращения их дальнейшего развития, путём обнаружения предварительных зондирующих акций;
- ✓ выполнить документирование обнаруженных атак;
- ✓ обеспечить контроль качества администрирования сетей с точки зрения безопасности;
- ✓ определить расположение источника атаки по отношению к атакуемой сети или узлу.

Средства IDS/IPS способны обнаружить многие типы сетевых вторжений и вести ответные действия на нарушения, оперативно отражая атаки.

Варианты внедрения. Обычно при упоминании систем IPS в голову приходят выделенные устройства, которые могут быть установлены на периметре корпоративной сети и, в ряде случаев, внутри нее. Внедрение в качестве систем защиты таких аппаратных устройств (security appliance) - наиболее распространенный вариант, но далеко не единственный. Такие шлюзы безопасности, несмотря на хорошую краткосрочную и среднесрочную перспективу, в дальнейшем постепенно уйдут в тень, и их место займут решения, интегрированные в инфраструктуру, что гораздо эффективнее со многих точек зрения.

Во-первых, стоимость интегрированного решения ниже стоимости автономного (stand-alone) устройства. Во-вторых, ниже и стоимость внедрения (финансовая и временная) такого решения - можно не менять топологию сети. В-третьих, надежность выше, так как в цепочке прохождения трафика отсутствует дополнительное звено, подверженное отказам. Наконец, в-четвертых, интегрированные решения предоставляют более высокий уровень защиты за счет более тесного взаимодействия с защищаемыми ресурсами.

Сама интеграция может быть выполнена различными путями. Самым распространенным способом в настоящий момент является использование маршрутизатора (router). В этом случае система IPS становится составной частью данного устройства и получает доступ к анализируемому трафику сразу после поступления его на определенный интерфейс. Интегрированная в сетевое оборудование система IPS может быть реализована в виде отдельного модуля, вставляемого в шасси маршрутизатора, или в виде неотъемлемой части операционной системы маршрутизатора. Первой в данном направлении развития систем IPS стала компания Cisco Systems, имеющая как отдельные модули для своих маршрутизаторов, так и подсистему Cisco IOS IPS, входящую в состав операционной системы Cisco IOS. Примеру Cisco последовали и другие сетевые производители: Extreme, 3Com и т. д.

Но система IPS, интегрированная в маршрутизатор, умеет отражать атаки только на периметре сети, оставляя внутренние ресурсы без защиты. Поэтому второй точкой интеграции являются коммутаторы локальной сети (switch), в которые с успехом могут быть внедрены механизмы предотвращения атак, причем как в виде части ОС, так и в виде отдельного аппаратного модуля. Первое слово в данной области сказала компания ODS Networks, предложившая коммутаторы с встроенной системой IPS. Позже ODS была куплена компанией SAIC, а технология интеграции IPS в коммутаторы на время забыта, пока ее не возродила Cisco Systems в своем семействе Cisco Catalyst.

Третий тип устройств, через которые может проходить трафик, нуждающийся в анализе, представлен точками беспроводного доступа (wireless access point). Сегодня это направление активно развивается, что связано со всплеском интереса к беспроводным технологиям (Wi-Fi, WiMAX, RFID). По пути интеграции пошли такие производители, как Cisco Systems и Aruba, оснастившие свое оборудование необходимыми функциями. Такого рода системы, помимо обнаружения и предотвращения различных атак, умеют определять местонахождение несанкционированно установленных беспроводных точек доступа и клиентов. Другие производители (например, Trapeze Networks) не имеют собственных решений, поэтому интегрируются с производителями самостоятельных систем предотвращения атак в беспроводных сетях - AirDefense, AirMagnet, AirTight, Network Chemistry и Newbury Networks.

Последним рубежом обороны, где может быть установлена система IPS, является рабочая станция или сервер. В этом случае IPS реализуется несколькими путями. Во-первых, как программное обеспечение, интегрированное в операционную систему. Пока таких решений немного и все они ограничиваются системами семейства UNIX, поскольку их ядро можно скомпилировать вместе с подсистемой отражения атак. Во-вторых, система IPS на рабочей станции или сервере может представлять собой прикладное ПО, устанавливаемое "поверх" операционной системы. Выпускается большим числом производителей: Cisco Systems, ISS, McAfee, Star Force и другими. Эти системы называются Host IPS (HIPS). Кроме отражения сетевых атак, они обладают еще большим количеством полезных функций: контроль доступа к USB, создание замкнутой программной среды, контроль утечки информации, контроль загрузки с посторонних носителей и т. д. В-третьих, система IPS может представлять собой отдельную подсистему отражения атак, реализованную в сетевой карте. Некоторые производители (в частности, D-Link) выпускают такого рода устройства, однако их распространенность оставляет желать лучшего. Ситуация может измениться только в том случае, когда такой функционал будет базовым для любой сетевой карты.

Если же вернуться к выделенным средствам предотвращения атак, то основными игроками этого рынка являются компании Cisco Systems, ISS, Juniper; из малоизвестных в России - 3Com, McAfee, Sourcefire, Top Layer, NFR и другие. И уж совсем неизвестны такие производители, как V-Secure, StillSecure, DeepNines, NitroSecurity и Reflex Security.

Особняком стоит технология обнаружения и блокирования аномалий в сетевом трафике, которую поддерживают Arbor Networks, Cisco Systems, Lancope, Mazu Networks и Q1 Labs. Однако данные решения отличаются от классических систем IPS. Прежде всего, они работают не в режиме online, они имеют дело не с самим трафиком, а, например, с Netflow. Кроме того, продукты данного класса не автономны, а тесно связаны с другими решениями (как правило, с сетевым оборудованием). Наконец, системы обнаружения и блокирования аномалий не предотвращают атаки, а действуют реактивно - изменяют списки контроля доступа (ACL, Access Control Lists) уже после обнаружения атаки. [6]

Выводы: Современный интернет несет огромное количество угроз, поэтому узкоспециализированные системы уже не актуальны. Необходимо использовать комплексное многофункциональное решение, включающее все компоненты защиты: файервол, IDS/IPS, антивирус, прокси-сервер, контентный фильтр и антиспам-фильтр. Такие устройства получили название UTM (Unified Threat Management, объединенный контроль угроз). В качестве примеров UTM можно привести Trend Micro Deep Security,Kerio Control, Sonicwall Network Security, FortiGate Network Security Platforms and Appliances или специализированные дистрибутивы Linux, такие как Untangle Gateway, IPCop Firewall.

Система обнаружения и предотвращения вторжений – основа защиты корпоративной сети от несанкционированного доступа.

Сама по себе технология IPS не является панацеей, и ее эффективность зависит от грамотного применения имеющихся инструментов и их интеграции с другими защитными и сетевыми технологиями. Только в случае построения комплексной инфраструктуры защиты системы IPS будут надежным кирпичиком в неприступной стене, опоясывающей вашу организацию.

Список литературы

1. http://xakep.ru
2. http://compuway.ru/ips-2/
3. http://help.ubuntu.ru/wiki/репозитории
4. https://ru.wikipedia.org/wiki/руткит
5. https://ru.wikipedia.org/wiki/ Вредоносная_программа
6. http://citforum.ru/security/articles/ips/

(*Алексей Лукацкий, менеджер по развитию бизнеса Cisco Systems*)