Решения для систем предотвращения вторжений

В статье рассказывается о том, как высокопроизводительная масштабируемая платформа ADLINK CSA-7400 помогла компании NSFOCUS создать системы обнаружения и предотвращения вторжений (IDS и IPS) нового поколения 100G+, обеспечивающего более безопасные, надёжные и стабильные решения для передачи данных.

По мере перехода от эпохи Интернета к эпохе Интернета вещей проблемы сетевой безопасности становятся всё более серьёзными. Увеличивается не только количество организованных, преднамеренных атак в сети, но и сама форма кибератак становится всё более и более сложной и продвинутой. В этот новый век сетевой безопасности системы обнаружения (IDS – Intrusion Detection System) и системы предотвращения вторжений (IPS – Intrusion Prevention System) приобретают всё большее значение.

Новые требования для IDS/IPS

Традиционным брандмауэрам становится всё труднее справляться с новыми типами кибервторжений, поэтому сегодняшняя сетевая защита требует всё более сложных и разнообразных возможностей.

В результате системы IDS/IPS постепенно стали незаменимыми компонентами для построения эффективной инфраструктуры сетевой безопасности. IDS контролирует безопасность сетевых операций, собирая и анализируя информацию в сети. Впоследствии эта информация используется для корректировки правил безопасности. IPS блокирует вторжения, реализуя на основе глубокого анализа сетевых данных эти правила безопасности в реальном времени.

Традиционные технологии обнаружения

Чтобы повысить вероятность обнаружения вторжений и минимизировать количество ошибок, как IDS, так и IPS пользуются комплексными технологиями обнаружения, включающими сопоставление функций, анализ протоколов и обнаружение аномалий. Сопоставление функций применяется наиболее часто благодаря высокой точности и скорости. Максимальная эффективность сопоставления функций зависит от качества построения библиотеки функций и от возможностей оборудования по их сопоставлению. Чтобы обнаружить атаки переполнения и отказа в обслуживании (Denial of Service – DoS), анализатор протокола ищет подозрительное поведение в сети, учитывая принципы работы протокола (обычно основанные на Интернет-стандартах RFC). Эффективное использование этой технологии обеспечивает высокую достоверность обнаружения с почти нулевым уровнем ошибок. Контроль аномалий трафика обнаруживает неожиданный аномальный трафик путём анализа и настройки критериев нормального трафика для конкретной сетевой среды. Когда фактическая статистика для данного критерия трафика превышает пороговое значение, отправляется сигнал обнаружения аномалии.

Несмотря на преимущества, каждая технология имеет свои недостатки. Например, сопоставление функций во избежание пропусков требует регулярного обновления библиотеки функций. Из-за значительных различий в реализации каждого протокола и недоступности полных сведений о проприетарных протоколах анализ протокола обычно может быть реализован только для открытых протоколов, таких как HTTP, FTP и SMTP. Если пороговые значения трафика установлены неправильно, функциональность обнаружения аномалий может привести к ложным срабатываниям. Поскольку количество веб-сетей и постоянных угроз повышенной сложности (Advanced Persistent Threats – APT) продолжает расти, IDS/IPS, основанные на этих традиционных технологиях, будут работать неадекватно.

Проблемы защиты веб-сетей

HTTP – безусловно, самый распространённый источник сетевого трафика. Согласно анализу статистики трафика по портам TCP Национальной технической группы по реагированию на чрезвычайные ситуации в компьютерных сетях / Координационного центра Китая (CNCERT), трафик в порту 80 намного выше, чем по другим портам (рис. 1). При таких условиях всё большее количество вирусов, троянов и ботнетов, естественно, использует атаки через HTTP. Веб-угрозы и кибератаки нового поколения становятся всё бо-

Рис. 1. Трафик по портам TCP согласно статистике CNCERT

лее скрытными. Поскольку они скрыты в легитимном трафике в Интернете, зависимые от Интернета в повседневной операционной деятельности предприятия часто подвергаются атакам, представляющим огромную угрозу информационным активам и бизнесу в целом. Следовательно, для эффективного предотвращения угроз безопасности в корпоративной интрасети, а также утечки конфиденциальных данных и других инцидентов информационной безопасности нужен встроенный механизм веб-репутации, позволяющий IDS и IPS отправлять своевременные предупреждения (IDS) или блокировать атаки (IPS), когда пользователи посещают веб-страницу, на которую был внедрён троянец.

Применение технологии глубокого анализа пакетов

Основное различие между IPS и традиционным межсетевым экраном заключается в том, что IPS может выполнять глубокую проверку содержимого пакетов (Deep Packet Inspection – DPI). Если хакер запускает атаки через уязвимость на сетевых уровнях 2–7, IPS может обнаруживать и затем блокировать такие атаки в потоке данных. Напротив, традиционный брандмауэр может находить только сочетание пятёрки данных в пакете (исходный IP-адрес, исходный порт, целевой IP-адрес, целевой порт и протокол на уровне передачи), не обнаруживая содержимого на уровне приложения или отдельных байтов и таким образом игнорируя многие атаки. Поскольку система IPS проверяет каждый байт трафика данных, она определяет большинство основных протоколов приложений на основе своей логики их распознавания. Затем с помощью тонкого управления идентифицированной информацией она может обнаруживать уязвимости в этих приложениях и предпринимать меры по предотвращению веб-атак. Для идентификации приложений с использованием DPI обычно требуется оборудование с возможностью ресурсоёмких параллельных вычислений для фильтрации и обнаружения десятков тысяч пакетов в секунду, также способное выполнять дефрагментацию IP, агрегацию потоков TCP и отслеживание состояния потока данных.

Поведенческий анализ пользователей

В последние годы мобильная сеть стала для предприятий важной инфраструктурой, в результате чего наблюдается рост числа инцидентов проникновения в интрасети через беспроводные сети. При развёртывании беспроводной сети становятся всё более популярными открытые точки доступа Wi-Fi для посетителей, обеспечивающие неаутентифицированный доступ к корпоративной сети. Кроме того, сотрудники, работающие вне офиса, могут получить доступ к сети компании из дома, аэропорта или из офиса клиента. Несмотря на свою эффективность, эти беспроводные сети часто не обладают достаточной защищённостью, что позволяет хакерам легко обходить брандмауэры компании, используя беспроводные сети в качестве входных ворот во внутреннюю сеть компании. В качестве второго шлюза безопасности после межсетевого экрана IDS/IPS предлагает идентификацию и контроль доступа пользователей, что эффективно решает проблемы с нарушением контроля доступа (Broken Access Control – BAC), вызванные перемещением неаутентифицированного оборудования и сотрудников. Благодаря статистическому анализу посещений сети сотрудниками компании с учётом таких характеристик, как идентификация пользователя, данные геолокации, операционное время, содержание и частота посещений, может быть построен шаблон посещения веб-сайтов. Система может точно обнаруживать ненормальное поведение, отклоняющееся от типичного шаблона посещения, и отправлять сигналы тревоги (IDS) или блокировать активность (IPS).

Продвинутые постоянные угрозы

Часто целью APT является кража основных данных. Веб-атаки на корпоративных пользователей и вторжения часто осуществляются в течение длительного периода времени и очень скрытно. APT-атаки, как команды спецназа, оснащены комплексным и сложным оружием, которое может парализовать оборонительную мощь традиционных брандмауэров и антивирусных программ корпоративной веб-среды. IDS/IPS повышают вероятность успешного противостояния APT. Выполняя визуализацию сетевого трафика, для минимизации потерь, вызванных APT, IDS будет отправлять сигналы тревоги после обнаружения его аномалий. Благодаря взаимодействию с локальной системой анализа угроз и на основе анализа образцов APT и поведенческого анализа IPS может обнаруживать продвинутые вредоносные коды, скрытые в трафике, и динамически настраивать стратегию защиты с целью блокировки вредоносного трафика в режиме реального времени.

Требования к аппаратной платформе NSFOCUS NIDS/NIPS

NSFOCUS – это компания, специализирующаяся на отслеживании актуальных тенденций в уязвимости сетевой безопасности. Благодаря проводимым по всему миру исследованиям компания постоянно расширяет базу анализа уязвимостей, а также совершенствует методы борьбы с ними, повышая технические стандарты систем IDS/IPS, anti-DDoS (Distributed Denial of Service), обнаружения вредоносного ПО и поведенческого анализа. NSFOCUS предоставляет сервисы безопасности на основе программного обеспечения как услуги (Software as a Service – SaaS). За последние два года NSFOCUS Security Labs опубликовала интегрированные отчёты о тенденциях в угрозах безопасности следующего поколения, безопасных архитектурах, исследования по безопасности в сетях IPv6 и промышленных системах управления. По состоянию на конец 2017 года NSFOCUS имела 96 публикаций об исследованиях уязвимостей безопасности. Компания сотрудничала с Microsoft, Cisco и Oracle в обнаружении и решении более 94 проблем уязвимости безопасности. База данных уязвимостей NSFOCUS (NSVD) является ведущей базой данных уязвимостей в Китае.

NSFOCUS предлагает новые решения для защиты от вторжений – NIDS (Network Intrusion Detection System – систе-

Рис. 2. Основные возможности технологии NSFOCUS NIPS

ма обнаружения сетевых вторжений) и NIPS (Network Intrusion Prevention System – система сетевой и компьютерной безопасности, предотвращающая вторжения), дающие возможность клиентам отслеживать, обнаруживать и предотвращать атаки (рис. 2). В дополнение к наличию расширенной библиотеки правил атак для обнаружения известных угроз безопасности продукт NIDS NSFOCUS оснащён постоянно обновляемой библиотекой функций репутации, которые могут уменьшить опасности, вызванные неизвестным вредоносным ПО, и эффективно предотвратить перманентное проникновение в интрасеть с помощью своей функции безопасности интрасети, таким образом сводя к минимуму утечки конфиденциальных данных и аномальные внешние подключения к серверам.

Система NSFOCUS NIPS оснащена одной из лучших в мире библиотек признаков атак и библиотекой репутации реального времени. Для реагирования на расширенные угрозы используется встроенная функция обнаружения – «песочница», реализующая трёхмерную защиту как от известных, так и от новых угроз. Использование технологии потокового обнаружения вирусов позволяет улавливать вирусы непосредственно в горячих точках, что максимально повышает эффективность антивируса. Встроенная защита мобильных устройств реализует безопасные запросы и безопасный мониторинг состояния в режиме реального времени, что снижает нагрузку на обслуживающий и эксплуатационный персонал.

Для обеспечения поддержки характеристик безопасности и ожиданий от платформ NIDS/NIPS следующего поколения 100G+ компания NSFOCUS установила следующие требования к вычислительной платформе.

- **Высокая пропускная способность и плотность ввода-вывода**

Для лучшего соответствия требованиям сценариев высокопроизводительных операторских приложений, таких как магистральные сети, центры облачных вычислений, крупные предприятия и точки доступа IDC, NSFOCUS требует обеспечить на вычислительных платформах поддержку интерфейса 100 Гбит/с, суммарного трафика до 800 Гбит/с и наличия минимум 64×10 Гбит/с портов на каждом модульном устройстве. Сетевые порты должны поддерживать согласованность восходящего и нисходящего потоков и технологию RSS (Receive Side Scaling – масштабирование на стороне приёма).

- **Параллельность и плотность вычислений**

Для обеспечения глубокой проверки пакетов и других методов обнаружения NSFOCUS требует, чтобы компьютерные платформы NIDS/NIPS поддерживали возможность параллельной обработки. В частности, платформы обработки сетевых пакетов должны обладать возможностью передачи данных на скорости проводной сети, иметь максимально возможную плотность вычислений на единицу объёма стойки и нулевой коэффициент потери пакетов для небольших пакетов размером 64 байта.

- **Балансировка нагрузки, источник и хост**

В NIDS/NIPS NSFOCUS весь трафик данных подключается с помощью платы коммутатора, балансирующей нагрузку трафика на отдельные платы процессора. При обнаружении ошибок платы процессора плата коммутатора может перенаправить трафик. Чтобы гарантировать обработку одного диалога на одном и том же узле ЦП и автоматически объединять поток данных в рамках одного диалога, коммутатор должен использовать один и тот же источник и один и тот же хост.

- **Высокая доступность операторского уровня**

Поскольку платформа NIPS включается в тракт трафика, NSFOCUS требует модульного промышленного дизайна вычислительных платформ на операторском уровне, обеспечивающего бесперебойность услуг для пользователей и возможность «горячей» замены неисправных компонентов (вычислителя, коммутатора, блока питания, вентилятора и хранилища данных).

- **Поддержка стандартизированного управления API**

Чтобы снизить затраты на разработку на низком уровне, NSFOCUS требует поддержки стандартизированного API-управления аппаратными платформами с поддержкой набора стандартизированных API-интерфейсов для управления трафиком и оборудованием всех компонентов в стойке, управления портами и VLAN, обычно используемыми стеками протоколов коммутаторов L2/L3, удалённой перезагрузкой.

Особенности платформы сетевой безопасности ADLINK CSA-7400

Используемая в качестве высокопроизводительной платформы телекоммуникационной COTS DPI и сетевой безопасности нового поколения **CSA-7400** (рис. 3) создана на основе открытой вы-

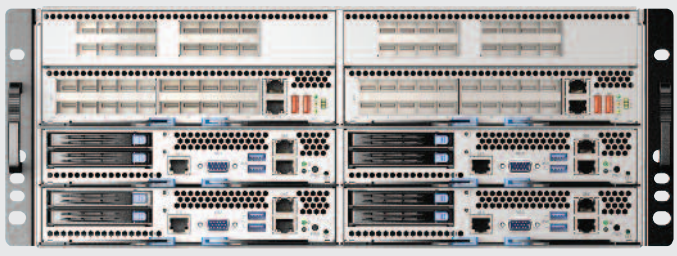

Рис. 3. Высокопроизводительное устройство нового поколения для телекоммуникаций CSA-7400

Таблица 1

Соответствие оборудования ADLINK требованиям NSFOCUS

Требования к вычислительным платформам NSFOCUS NIDS/NIPS	Особенности ADLINK CSA-7400
Поддержка интерфейсов со сверхвысокой пропускной способностью и оснащение интерфейсами 100, 40 и 10 Гбит/с	Модульный ввод-вывод, рассчитанный на масштабируемую полосу пропускания в соответствии с фактическими потребностями, поддерживает высокоскоростные интерфейсы 100/40 Гбит/с и обеспечивает интерфейсы до 72×10 Гбит/с по сравнению с популярным в настоящее время оборудованием для сетевой безопасности 2U, которое поддерживает до 64 интерфейсов по 10 Гбит/с в одной стойке 4U
Поддержка параллельной обработки высокой плотности и высокопроизводительная пакетная обработка данных; возможность обработки малых 64-байтовых пакетов данных	Поддерживает до четырёх двухпроцессорных плат Intel® Xeon® E5-2600 v3/v4 или вычислительные узлы с масштабируемым процессором Intel® Xeon®, обеспечивая лучшую в отрасли производительность и плотность обработки в объёме 4U. CSA-7400 4U обладает отличной производительностью при обработке малых пакетов (64 байта). Каждый вычислительный узел может обрабатывать более 50 Гбайт данных с нулевой потерей пакетов
Балансировка нагрузки, поддержка технологии одного источника и хоста	В дополнение к функциональности балансировки нагрузки, позволяющей пользователям устанавливать различные веса нагрузки для отдельных вычислительных узлов, коммутатор поддерживает автоматическое устранение неисправных узлов в процессе балансировки нагрузки, что обеспечивает надёжную обработку потока данных. Плата коммутатора также аппаратно поддерживает технологию единого источника и хоста, что повышает эффективность сетевых коммуникаций
Высокая доступность и полная защита для обеспечения стабильности работы оборудования	Высокая доступность оборудования достигается за счёт конструкции, обеспечивающей резервирование блоков питания и «горячую» замену компонентов. Оборудование поддерживает внеполосный мониторинг работы модуля в реальном времени через IPMI
Стандартизированный интерфейс API для управления пакетным трафиком и оборудованием	ADLINK PacketManager на платформе CSA-7400 обеспечивает управление портами и VLAN, а также реализует стеки протоколов для LACP, LLDP, RSTP и VRRP. Кроме того, CSA-7400 обеспечивает высокую производительность интеллектуальной передачи трафика через ACL, а также удалённый мониторинг и перезагрузку

числительной эталонной архитектуры операторского уровня (Open Compute Carrier-grade Edge Reference Architecture – OCCERA) **ADLINK** и обеспечивает высокоскоростное соединение вычислительных узлов с узлами коммутации с двойным резервированием. Платформа имеет порты ввода/вывода на передней панели до 800 Гбит/с. Для обеспечения безопасности и бесперебойной работы платформа CSA-7400 поддерживает «горячую» замену основных компонентов шасси, что делает её пригодной для построения высокопроизводительных систем IDS/IPS следующего поколения.

Далее мы приведём основные характеристики CSA-7400:

- до четырёх вычислительных узлов с двумя процессорами Intel® Xeon® E5-2600 v3/v4 или с процессорами Intel® Xeon® Scalable с поддержкой одинарного обновления или гибридного развёртывания;
- конструкция коммутатора с двойным резервированием и пропускной способностью 4×50 Гбит/с на узел для внутреннего соединения четырёх вычислительных узлов, в том числе 4 восходящих панелей ввода-вывода по 100 Гбит/с или 36 модулей ввода-вывода 10 Гбит/с;
- коммутатор поддерживает ускоренную обработку протоколов туннелирования NVGRE/VXLAN для удовлетворения потребностей уровня 2 в облачных вычислениях;
- программное обеспечение ADLINK PacketManager, обеспечивающее обычно используемые стеки протоколов коммутации уровней 2 и 3 и API стратегического управления на основе потоков, балансировку нагрузки, функциональность поддержки неизменного источника и хоста для ускорения разработки приложения;
- поддержка интеллектуального управления системой с использованием спецификаций на основе IPMI для удалённой диагностики системы, перенаправления, выключения и запуска.

Далее в табл. 1 перечислены требования к вычислительным платформам NIDS/NIPS нового поколения NSFOCUS (в левом столбце) и соответствующая функциональность CSA-7400 от ADLINK (в правом столбце).

Заключение

CSA-7400 – это высокопроизводительная платформа сетевой безопасности нового поколения, основанная на архитектуре Open Compute Carrier-grade Edge Reference Architecture. Граничная эталонная архитектура операторского уровня (OCCERA) от ADLINK, объединяющая сетевые интерфейсы, коммутаторы и необходимую вычислительную мощность, открытая аппаратная архитектура и масштабируемость платформы CSA-7400 поддерживают решения следующего поколения 100G+ IDS/IPS.

Гибкость и настраиваемость CSA-7400 позволяют развёртывать продукты в различных компаниях и легко интегрировать оборудование в межсетевые экраны и системы телекоммуникаций следующего поколения. Предоставляемая ADLINK библиотека API позволяет поставщикам решений безопасности сосредоточиться на их основных компетенциях, избавляя от рутинной работы по реализации стандартной функциональности. ●

Авторизованный перевод
Юрия Широкова
E-mail: textoed@gmail.com

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Встречайте: новый блог ICONICS

Компания **ICONICS** уже более трёх десятилетий поставляет передовые программные решения для автоматизации деятельности самых разных предприятий во множестве отраслей по всему миру.

В текущем году в связи с ограниченным социальным взаимодействием эта компания запустила свой блог, чтобы открыто делиться знаниями по программным решениям для цифровой трансформации.

Сотрудники ICONICS из различных подразделений с разными областями знаний поделятся опытом, мыслями и наработками по новым технологиям, тенденциям и решениям. К примеру, в блоге опубликован обзор бесплатных видеоуроков, которые доступны на новой обучающей платформе ICONICS Institute – уже сегодня на ней насчитывается 188 обучающих видео и ещё 55 готовятся к выпуску. Блог также станет местом, где можно прочесть важные объявления, обзоры событий ICONICS и узнать о приложениях клиентов в различных отраслях.

Можно настроить подписку в социальных сетях с оповещением, когда появляется новая запись в блоге, чтобы оставаться в курсе всех новинок.

Адрес блога: **https://iconics.com/Resources/ICONICS-Blog.** ●