Технология CLEAR-Flow

Одно из принципиальных ограничений большинства существующих методов управления трафиком связано с тем, что они слабо интегрированы в саму сеть. Новый подход воплощен в технологии CLEAR-Flow, которая встраивает функции мониторинга, анализа и реагирования непосредственно в коммутационную матрицу Ethernet. Это мощный инструмент для задач, которые ранее было очень трудно или вообще невозможно решить, например, для выявления и предотвращения угроз в высокоскоростных сетях.

В документе дан общий обзор технологии CLEAR-Flow, представлены ее основные преимущества, а также приведены примеры реализации приложений безопасности, использующих возможности CLEAR-Flow.

Введение

Согласно оценке экспертов Cyber Secure Institute, в 2009 году сетевой червь Conficker/Downadup мог заразить около 10 млн компьютеров по всему миру, нанеся экономический ущерб на сумму 9,1 млрд. долларов. В ходе опроса, проведенного институтом Computer Security Institute (данные из документа 2009 CSI Computer Crime and Security Survey приведены с разрешения CSI), 29% респондентов сообщили об инцидентах, связанных с атаками типа «отказ в обслуживании» (Denial-of-Service, DoS), а 64% – о заражении вредоносными программами. Червь Sapphire/Slammer способен сканировать более 55 млн IP-адресов в секунду и за 10 минут может заразить 90% уязвимых хостов в Интернет. Эти примеры показывают, что черви и вирусы становятся все более разрушительными, используют все более скоростные алгоритмы и несут все больше вредоносной нагрузки и троянов.

По мере увеличения размеров корпоративных сетей, объема передаваемого в них трафика и повышения значимости их нормального функционирования для бизнеса компаний, ИТ-отделам приходится все глубже вникать в особенности сетевых приложений, структуры трафика и угроз безопасности. Последние возникают неожиданно и распространяются по всему миру за считанные часы или даже минуты, а убытки от их негативных последствий могут исчисляться миллиардами долларов.

Эффективная борьба с угрозами безопасности требует исследования каждого передаваемого по корпоративной сети пакета, а это все сложнее сделать при росте скорости передачи трафика, которая сегодня достигает 10 Гбит/с. Чтобы упростить решение данной задачи, компания Extreme Networks разработала технологию CLEAR-Flow (Continuous Learning, Examination, Action, and Reporting of Flows), которую поддерживают коммутаторы Summit серий X450a, X450e, X480 и X650, а также коммутаторы BlackDiamond всех серий. Новые функции, реализованные непосредственно в аппаратуре коммутации, обеспечивают проактивную (упреждающую) идентификацию аномалий в действиях пользователей, хостов и приложений.

Технология CLEAR-Flow нацелена на решение широкого набора задач, связанных с безопасностью, включая следующие группы задач:

- Сетевая безопасность – обнаружение вторжений, предотвращение распространения сетевых червей и вирусов, подавление атак типа DoS.
- Сетевое управление – планирование емкости, анализ тенденций, классификация приложений, реализация алгоритмов гарантированного качества обслуживания (Quality of Service, QoS).
- Сетевая тарификация – учет трафика и реализация процедур, необходимых для выполнения соглашений по уровню обслуживания (Service Level Agreement, SLA).

Раннее обнаружение угроз безопасности, таких, как вирусы, черви, DoS-атаки, – одна из важнейших задач для администраторов корпоративных сетей. Для ее решения необходимо просматривать весь трафик для выявления необычных пакетов. Однако большинство существующих систем раннего обнаружения, например системы IDS (Intrusion Detection Systems), не способны масштабироваться для соответствия растущим требованиям к повышению скорости передачи и снижению времени задержки в корпоративных сетях.

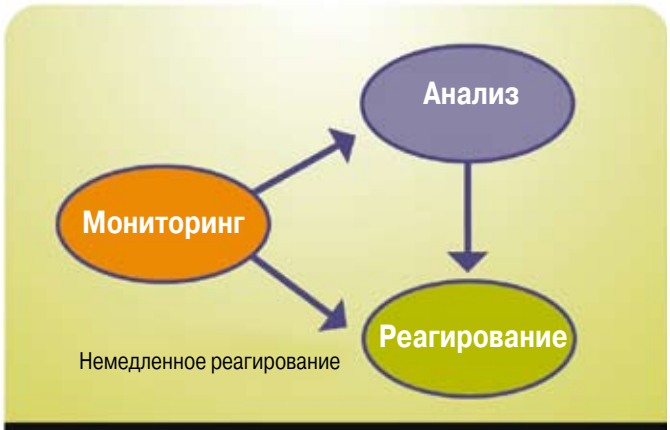


Рисунок 1. Структура процессов CLEAR-Flow

Основы CLEAR-Flow

Технология CLEAR-Flow знаменует собой новый подход к управлению сетевым трафиком. Впервые задачи мониторинга, анализа и реагирования реализованы в рамках единого процесса в коммутационной матрице Ethernet.

Одно из принципиальных ограничений большинства существующих методов мониторинга трафика и управления им связано с тем, что они не встроены в само инфраструктурное оборудование. Обычно на коммутаторе используется некая программа, которая отправляет трафик, его образцы или сводку по трафику на удаленное устройство управления. При этом на станцию управления пересылается масса трафика, который не представляет никакого интереса для задач выявления угроз.

Очевидная проблема такого подхода – плохое масштабирование. Коммутаторы просто не в состоянии перенаправлять каждый пакет на внешние анализаторы, а те в свою очередь не способны анализировать все пакеты в реальном времени.

Разработчики CLEAR-Flow выбрали принципиально иной подход, возложив задачу по изучению трафика на сами коммутаторы Ethernet. Если обычные коммутаторы просто «читают» адрес отправителя и получателя пакета и отправляют его по соответствующему пути уровня 2 (Layer 2) или 3 (Layer), то коммутаторы с поддержкой CLEAR-Flow способны более внимательно изучать трафик. Если окажется, что трафик соответствует определенному (администратором) критерию, коммутатор немедленно выполнит заданное действие или отправить копию трафика на внешний анализатор. Дополнительный анализ также может привести к активному реагированию, например, к блокированию DoS-атаки или ограничению полосы пропускания, доступной пользователю-нарушителю.

Базируясь на трех основных группах процессов – мониторинг, анализ и реагирование, – CLEAR-Flow реализует полное решение для выявления событий и трендов в сети, определения их влияния на ее работу и выполнения ответных действий для защиты.

Мониторинг

Технология CLEAR-Flow использует возможности аппаратной части коммутатора для сканирования и фильтрации каждого проходящего через него пакета. При этом отслеживаются только пакеты, которые отвечают критериям мониторинга, заданным администратором; не представляющие интереса пакеты система игнорирует. Если требуется немедленное реагирование, аппаратная часть коммутатора информирует его программную часть о необходимости изменения алгоритма обработки трафика.

- **Шаг 1 – Фильтрация.** Интегрированные в механизмы контроля доступа (Access Control) коммутатора специальные классификаторы CLEAR-Flow выявляют отвечающий заданным условиям трафик на скорости, равной скорости передачи данных по физической линии связи. При обнаружении подозрительного трафика коммутаторы незамедлительно выполняет заданное для него действие и увеличивает показание счетчика соответствующих событий. Технология CLEAR-Flow позволяет отслеживать до 112 тыс. уникальных типов трафика.

- **Шаг 2 – Подсчет.** При выявлении классификаторами CLEAR-Flow представляющего интерес трафика происходит увеличение показания соответствующего счетчика. Технология поддерживает до 112 тыс. счетчиков, реализованных аппаратно.

- **Шаг 3 – Контроль пороговых значений.** С механизмом счетчиков связаны тригерры, которые запускают присоединенные процедуры при превышении установленных пороговых значений. Порог может быть установлен на абсолютное значение счетчика, скорость увеличения его показаний, разницу между показаниями двух разных счетчиков. При превышении порогового значения система инициирует определенное действие или отправляет трафик для дальнейшего анализа.

Анализ

Часто коммутатор не располагает достаточными средствами для выявления истинной природы подозрительного трафика. В этих случаях он отправляется на внешнее устройство для дополнительного анализа. Его результаты позволяет принять более эффективное решение относительно того, что делать с этим трафиком. Существует несколько способов взаимодействия с внешним анализатором, и выбор одного из них определяется спецификой задачи.

- **Метод 1 – Дублирование трафика.** Копия представляющего интерес трафика зеркально отражается на один из портов коммутатора и далее передается на анализатор трафика или в систему IDS. В этом случае внешнее устройство получает полную картину трафика и может максимально тщательно исследовать пакеты.

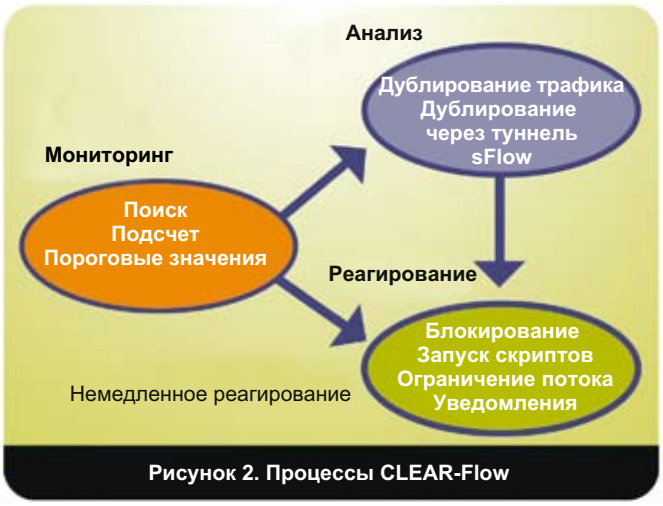


Рисунок 2. Процессы CLEAR-Flow

- **Метод 2 – Дублирование через туннель.** Этот метод аналогичен предыдущему за тем лишь исключением, что пакеты снабжаются дополнительным заголовком IP и по туннелю направляются на удаленную систему для анализа. Например, можно отправить трафик на порт мониторинга (mirror port) другого коммутатора. Данный метод позволяет более эффективно использовать средства анализа в крупных сетях.

- **Метод 3 – sFlow.** Метод предполагает передачу внешнему анализатору только статистических образцов трафика. Объем пересылаемых данных при этом значительно сокращается, что повышает масштабируемость процесса. Использование технологии sFlow особенно предпочтительно тогда, когда предполагается, что аномального трафика будет много – скажем, при мониторинге атаки DoS.

Реагирование

В ситуации, когда классификатор обнаружит серьезную угрозу, будет превышен установленный порог или внешний анализатор «забьет тревогу», коммутатор тут же предпримет адекватные действия. Здесь возможны следующие варианты:

- **Опция 1 – Блокирование трафика.** Вводится в действие правило из списка контроля доступа (Access Control List, ACL), которое полностью останавливает данный тип трафика.
- **Опция 2 – Запуск скрипта или команды CLI.** Выполнение набора команд, доступных из интерфейса командной строки (CLI) коммутатора.
- **Опция 3 – Ограничение потока данных.** Вводится в действие правило из списка ACL, ограничивающее скорость передачи данного типа трафика.
- **Опция 4 – Уведомления.** Для отправки уведомления на консоль сетевого управления может использоваться механизм «ловушек» (trap) SNMP или сообщения SYSLOG.

Примеры использования CLEAR-Flow

Выявление сетевых вирусов, червей, DoS-атак и предотвращение их негативного воздействия – одни из наиболее сложных задач, стоящих перед администраторами корпоративных сетей. Но если их не решить, негативные последствия могут оказаться очень серьезными, а потери – очень внушительными. Технология CLEAR-Flow предлагает эффективный инструмент для обеспечения безопасности сети.

Пример 1. Защита от вирусов и червей

Вовремя выявить и изолировать новые вирусы и черви непросто. Возможности CLEAR-Flow позволяют значительно сократить время, необходимое для выявления вируса и принятия защитных действий. Для этого фильтры CLEAR-Flow настраиваются таким образом, чтобы отслеживать и подсчитывать пакеты TCP SYN, посылаемые каждым хостом в сети (рисунок 3).

Появление пакета SYN означает, что хост пытается установить новое TCP-соединение с удаленной системой. Вообще это обычная ситуация. Но появление большого числа таких пакетов может указывать на присутствие вируса или червя, который для дальнейшего распространения пытается установить как можно больше соединение с соседними хостами.

Для начала включим функцию подсчета пакетов SYN, приходящих на конкретный порт:

```
entry detect-syn{
if{
TCP-flags SYN;
}then{
count detect-syn
}}
```

Для большей детализации при подсчете можно учитывать IP-адрес источника трафика:

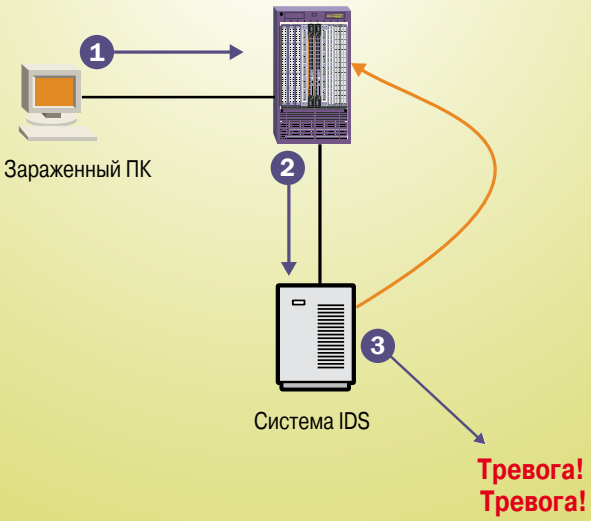
```
entry detect-syn-200{
if{
source-address 10.10.10.200;
TCP-flags SYN;
}then{
count detect-syn-200
}}
```

Теперь задаем пороговое значение и реагирование на событие. Если число пакетов SYN, полученных за 5 с, превысит 1000, включается функция зеркального отражения трафика (mirror):

```
entry eval rate{
if{
(rate (detect-syn, 5) > 1000 )
then{
sendsnmp 7 "Too many SYNs detected,
starting mirror";
mirror add detect-syn;
}
```

Рисунок 3. Защита от вирусов и червей – пример интерфейса командной строки (CLI)

Если настольный ПК запрашивает установление нескольких десятков и более соединений в секунду, а сервер – более двух тысяч соединений в секунду, то очень вероятно, что они заразились вирусом, который пытается распространиться дальше (рисунок 4). Администратор сети может настроить средства CLEAR-Flow так, чтобы они незамедлительно блокировали зараженную систему или автоматически отправляли пакеты трафика для анализа во внешнюю систему IDS.



1. Зараженная система начинает массовое установление новых соединений
2. Порог числа пакетов SYN достигнут, коммутатор отражает трафика на систему IDS
3. Система IDS блокирует IP-адрес источника трафика и отправляет уведомление на станцию управления

Рисунок 4. Определение атаки с использованием вируса (IDS – система обнаружения вторжений)

В этом примере мы отслеживаем трафик ICMP, направляемый на ферму серверов.

```
entry icmpcnt{
if{
destination-address
10.203.134.0/24;
protocol icmp;
}then{
count icmpcnt;
}
}
```

Если за 1 с поступает более 100 ICMP-пакетов, этот тип трафика блокируется.

```
entry eval rate{
if{
(rate(icmpcnt) > 100)
then{
sendsnmp 7 "Too Many ICMP packets"'
deny icmpcnt;
}
```

Рисунок 5. Обнаружение атаки DoS – пример интерфейса командной строки (CLI)

Пример 2. Обнаружение атаки DoS

Атаки DoS представляют большую проблему для многих компаний. Такие атаки могут «положить» Web-сайты, порталы электронной коммерции, другие корпоративные системы. Оперативное обнаружение атаки и идентификация ее инициатора позволяет значительно снизить негативный эффект.

Технология CLEAR-Flow дает возможность просто и эффективно бороться с DoS-атаками. Большинства таких атак сводятся к направлению на сервер огромного потока бессмысленных обращений, которые перегружают его ресурсы и не дают нормально обслуживать полезные запросы. Обычно злоумышленники генерируют поток ICMP или TCP SYN пакетов.

Классификаторы CLEAR-Flow способны зафиксировать резкое увеличение объема указанных типов трафика и направить его на внешние средства анализа (рисунок 5). Любая система IDS, равно как и сборщик данных sFlow, незамедлительно определят источник атаки, после чего его можно будет заблокировать.

Пример 3. Отслеживание управляющего трафика

В системах, где требования к безопасности особенно высоки, желательно фиксировать весь управляющий трафик. Сеансы управления любят использовать хакеры, и наличие записей (журналов) таких сеансов часто служит единственным способом выявить атаку и вычислить злоумышленника.

Традиционные способы предусматривают ведение журналов на каждом сервере. Но хакеры хорошо это знают, поэтому стараются стереть соответствующие файлы и замести следы. Средства CLEAR-Flow позволяют отслеживать управляющий трафик (передаваемый по протоколу telnet или SNMP), направлять его на анализатор и сохранять в архиве (рисунок 6). Таким образом можно выявлять атаки самых изощренных хакеров, которые и не подозревают, что сеть способна сама отслеживать их действия.

Поиск пакетов telnet, следующих к серверам.

```
entry capture-telnet{
if{
destination-address
10.203.134.0/24;
protocol TCP;
destination-ort 23;
}then{
}
}
```

При обнаружении таких пакетов, они пересылаются для анализа.

```
entry eval threshold{
if{
(threshold(capture-telnet)>1)
then{
mirror add capture-telnet;
}
```

Рисунок 6. Отслеживание управляющего трафика – пример интерфейса командной строки (CLI)

Заключение

Ориентированная на реализацию интегрированного подхода к управлению трафиком, технология CLEAR-Flow гарантирует масштабируемое решение самых сложных проблем в самых скоростных сетях. Методология, основанная на трех ключевых шагах – мониторинг, анализ, реагирование, – обеспечивает гибкую модель, которая может адаптироваться к уникальным задачам конкретной сети. Помимо описанных в этом документе, существует масса других применений CLEAR-Flow, и их число будет увеличиваться по мере расширения функциональности этой технологии.

www.extremenetworks.com

Штаб-квартира
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Телефон: +1 408 579 2800

Представительство
Extreme Networks в странах СНГ
Смоленская площадь 3,
Бизнес-центр «Регус»
Москва, 121099, Россия
Телефон: +7 (495) 775-1067
Email: cis@extremenetworks.com