



## Решение Cisco Systems “Clean Pipes” по защите от распределенных DOS атак для операторов связи их клиентов

Провайдером услуг и компаниям необходимо понимать принципы осуществления распределенных атак, направленных на отказ в обслуживании (DDoS-атак) и иметь в своем распоряжении технические средства для их подавления. В противном случае возможны убытки, а данные могут быть утрачены без возможности восстановления. В этом документе освещены важнейшие вопросы, связанные с DDoS-атаками, и приводятся рекомендации по применению решения Cisco Clean Pipes для защиты сетей.

### **Общие сведения о DDoS-атаках**

#### **Что такое DDoS-атаки?**

Распределенной атакой, направленной на отказ в обслуживании (DDoS-атакой) называется атака на систему конечного хоста или сетевую инфраструктуру, результатом которой являются перебои в предоставлении пользователям определенного сетевого сервиса. Перебои могут иметь различное проявление, включая:

- трудности с доступом к определенным ресурсам, таким как серверы
- снижение пропускной способности
- и, как худший вариант, "засорение" канала связи с Интернетом до такой степени, что невозможным становится всякий доступ к хосту извне


Перебои подобного рода могут обнаружиться в любое время, в любой день, и безо всякого предупреждения. В наши дни наблюдается быстрое изменение характера DDoS-атак: сейчас это уже не "случайное происшествие", а хорошо спланированные преступные операции.

Для нарушения нормальной работы целевого сетевого ресурса его "бомбардируют" трафиком в объемах, гораздо больших того, какой он в состоянии обработать. При этом очень важно понимать, что для блокады сетевого ресурса не обязательно нужно много усилий. Приведем пример: чтобы вызвать неработоспособность канала ТЗ, который крупная корпорация использует для выхода в Интернет, атакующим достаточно генерировать трафик со скоростями всего 50, 60 Мбит/с, а это довольно несложно.

Распознавание, изоляция и подавление DDoS-атаки является сложной задачей. Основным способом обнаружения DDoS-атаки заключается в распознавании аномалий в структуре трафика. Традиционные механизмы обеспечения безопасности – межсетевые экраны и системы обнаружения вторжений – не являются эффективными средствами для обнаружения DDoS-атак и защиты от них, особенно атак трафиком большого объема

#### **Как осуществляют DDoS-атаки?**

Чтобы разобраться с тем, как подавить DDoS-атаку, необходимо иметь четкое представление о том, как их осуществляют. Для выполнения DDoS-атаки используют так называемые "ботнеты" или сети "ботов", т.е. компьютеров, зараженных определенным трояном, которыми нападающая сторона может



управлять удаленно. Из-за своих огромных размеров (есть информация о десятках тысяч систем, соединенных в один ботнет) ботнеты могут представлять серьезную угрозу для сообщества пользователей Интернета.

В ходе подготовки к DDoS-атаке нападающий взламывает ряд хостов и устанавливает на них демона. Затем на такой демон посылают запрос на генерацию лавинообразного трафика пакетов того или иного вида в адрес целевого хоста. Обработка такого масштабного потока данных приводит к исчерпанию ресурсов хоста или маршрутизатора, на которые направлена атака, и приводит к недоступности сервиса или услуги, которую они предоставляли.

Ботнеты, используемые для проведения DDoS-атаки, могут состоять из нескольких десятков тысяч взломанных компьютеров и являются серьезной угрозой: даже относительно небольшой ботнет, состоящий всего из 1000 компьютеров, способен нанести серьезный ущерб. Общая пропускная способность ботов может быть выше пропускной способности соединения с Интернетом многих корпоративных систем. (Тысяча домашних персональных компьютеров со средним исходящим потоком 128 Кбит/с могут дать поток данных со скоростью свыше 100 Мбит/с). При этом создание, обслуживание и развертывание фильтров входного трафика вследствие распределенного характера IP-адресов ботов весьма затруднительно. Кроме того, ботнеты могут оставаться незамеченными из-за того, что с каждого из эксплуатируемых компьютеров исходит небольшой объем трафика атаки, и все же совокупное воздействие на цель атаки может быть значительным. Принятие мер противодействия также осложняется тем, что в один распределенный ботнет могут быть объединены компьютеры многих организаций, никак между собой не связанных.

Некоторые DoS-атаки против крупного, современного сайта, могут проводиться с использованием самых ограниченных ресурсов – их иногда называют "асимметричными атаками". Например, атакующий со старым персональным компьютером и медленным модемом может быть способен вывести из строя гораздо более быстрые и современные машины или сети.

## Тенденции DoS-атак

Число DDoS-атак, совершаемых против частных компаний, увеличивается угрожающими темпами. Эти атаки, носившие вначале спорадический характер и являвшиеся для взломщиков способом снискать себе славу в электронном мире, сейчас превратились в серьезные преступные операции с использованием ботнетов – теперь взломщики шантажируют частные компании и требуют отступных, угрожая нападением на сетевые ресурсы компании накануне проведения крупных запланированных мероприятий или непосредственно перед запуском новой линейки продукции, т.е. событий, имеющих для компании большое финансовое значение.

Сетевая безопасность в наши дни становится важной составляющей успешной деятельности предприятий. На основе безопасной инфраструктуры компании любого размера – большие или мелкие – расширяют спектр своих услуг. Сетевая безопасность всегда имела важное значение для провайдеров сетевых услуг и операторов. Однако в наши дни вопросы безопасности оказывают более сильное, чем когда-либо ранее влияние на то, какой дизайн сети выберет провайдер услуг и на то, какое техническое решение он приобретет. Все чаще предприятия выбирают таких провайдеров услуг, которые предлагают услугу защиты их активов от широкомасштабных DDoS-атак и средства для противодействия блокированию их сетевых ресурсов.

Эксперты по сетевой безопасности имеют много описаний таких атак, имеющих документальное подтверждение. Приведем несколько примеров:

- "Резкий рост ботнетов – это огромная проблема. Только почитайте, что пишут эти ребята на своих электронных досках объявлений в андеграунде: для распределенной DoS-атаки и нарушения работы корпоративной сети средних размеров – говорят они – достаточно ботнета из 500, 1000 машин". Кен Данхэм (Ken Dunham), директор по исследованиям вредоносного кода в компании iDefense (г. Рестон, шт. Вирджиния), специализирующейся в области разведки и безопасности, из статьи на TechWeb от 10 марта 2005 г., которая называется *More Than One Million Bots On The Attack ("Более миллиона ботов к бою готово")*

- "Из-за широкого распространения в прошлом году вирусов, переносимых по электронной почте, и автозагружающихся троянов число ботнетов и их размеры значительно увеличились, и сейчас они являются предметом купли-продажи, имеющим свою стоимость и используемым в качестве средств для рассылки спама, а также инструментов для схем шантажа с угрозами осуществления DDoS-атаки. Машины-зомби с нарушенной безопасностью недавно были обнаружены в сетях Министерства обороны и Сенате США". Из статьи Addict3d "A huge DDOS Attack Botnet of 10,000 Machines @R.I.P" ("Покойся с миром, огромный ботнет для DDoS-атак из 10000 компьютеров!") от 19 сентября 2004 г. Полный текст статьи: <http://addict3d.org/index.php?page=viewarticle&type=news&ID=3031>
- "Надо понимать одну важную вещь, касающуюся DDoS-атак: их невозможно предотвратить, и они никуда не исчезнут. Существуют они уже очень давно, и их осуществление становится все проще, так как растет число плохо-защищенных домашних персональных компьютеров с постоянным подключением к Интернету, которые только и ждут, чтобы их обнаружили и захватили взломщики. Из захваченных персональных компьютеров составляют сети, предназначенные для проведения атак, но они бездействуют до тех пор, пока короткий командный импульс и управляющий пакет не активирует их, и не превратит их в сумасшедших атакующих зомби, бомбардирующих целевой хост данными до тех пор, пока – как надеется взломщик – он не исчезнет в потоке нежелательных пакетов". – Из статьи "Distribute This Denial of Service Checklist" ("Передай этот список отказов в обслуживании"), опубликованной на Enterprise IT Planet.com 27 августа 2004 г. Полный текст статьи: <http://www.enterprisitplanet.com/security/features/article.php/3400861>

В последнее время предприятия стремятся направлять больше средств на защиту своих сетей от атак. Они понимают, что гораздо дешевле быть подготовленным к атаке, чем думать о защите, после того, как был атакован. Из недавнего отчета Gartner 2004 года видно, что озабоченность надежностью сетевой безопасности сейчас возглавляет список основных проблем предприятий, обойдя операционные расходы.

## Какое влияние оказывают DDoS-атаки?

Сейчас компании для своих основных операций все чаще используют Интернет и IP-сети, поэтому хорошо-подготовленная DDoS-атака может привести к полной остановке работы на любом предприятии. В наши дни большинство предприятий среднего и крупного размеров для своих транзакций все чаще используют Интернет, а по мере усовершенствования технологии VoIP будут переходить на IP-коммуникации. О "видео-через-IP" сейчас говорят, как о новой прогрессивной технологии, и предприятия уже начинают задумываться о том, как они смогут использовать возможности видео для улучшения своих показателей. Эти тенденции определяют необходимость конвергентных сетей, которые в будущем станут для компаний основным способом уменьшения расходов.

Атака, вызывающая простой сети, уменьшает чистую прибыль компании. Даже если влияние атаки на сеть незначительное, восприятие сети компании, как уязвимой, способно подорвать доверие к компании у клиентов, а такой ущерб может иметь гораздо более серьезные финансовые последствия, чем ущерб от самой атаки. Например, давайте рассмотрим организацию среднего или крупного размера, работающую в сфере финансов, большая часть деятельности которой происходит в режиме онлайн. Простой, исчисляемый несколькими минутами, может обойтись в сотни миллионов долларов потерь на транзакциях, не говоря уже о расходах, связанных с заглаживанием эффекта от публикаций материалов негативного характера в средствах массовой информации.

DDoS-атаки могут быть направлены на различные сетевые устройства в сети компании и иметь различные формы, включая:

- Попытки наполнить сеть "лавинообразным" трафиком, в результате чего блокируется прохождение корректно-сформированного сетевого трафика или растут задержки трафика
- Попытки нарушить соединение между парой маршрутизаторов или серверов с целью вызвать недоступность сервиса

- Попытки заблокировать доступ к сервису для определенного оконечного устройства
- Попытки вызвать недоступность сервиса для конкретной системы или пользователя

## Против кого осуществляются DDoS-атаки?

От DDoS-атак не застрахована ни одна компания вне зависимости от ее размера или вида деятельности. В новости попадают только атаки на крупные предприятия. Однако, гораздо чаще, чем это получает огласку, целями DDoS-атак также становятся малые и средние предприятия. Как показано выше, особенно значительных ресурсов для того, чтобы нарушить работу сети, не требуется.

Если сначала основными целями атак были компании, осуществляющие свой бизнес через Интернет, то теперь опасности DDoS-атак подвержены все вертикальные рынки, включая финансовый, розничную торговлю, средства массовой информации и развлечений, производство, услуги и правительственные учреждения. Уже начинают атаковать даже отдельных потребителей. Провайдеры широкополосных услуг должны обращать более пристальное внимание на механизмы защиты, которые они используют для защиты от этих атак своих сетей и сетей своих клиентов.

Целью атаки становится любая компания, использующая сайт в Интернете в качестве основного способа ведения своей деятельности, особенно во время крупных акций, таких как выпуск на рынок новой продукции, проведение ежеквартальных конференций т.п. Атакующие используют такие моменты в своих целях, и, зная о том, что компании не могут рисковать доверием со стороны своих клиентов во время проведения этих важных мероприятий, вымогают отступные у компаний, ресурсы которых не защищены, угрожая им неблагоприятными финансовыми последствиями.

От Интернета, в котором доверие было чем-то естественным, мы перешли к Интернету всеобщего недоверия. Так, из результатов недавних исследований становится понятно, что четверть старших сотрудников служб безопасности в сфере ИТ в крупных компаниях Объединенного королевства рассматривают DDoS-атаки, как "единственный серьезный риск для деятельности своего предприятия" (октябрь 2004 г., обзор NetSec, составленный на основе опроса 40 сотрудников уровня высшего руководства, преимущественно из банковской и финансовой сферы). За дополнительной информацией обращайтесь по адресу:

[http://www.theregister.co.uk/2004/10/27/netsec\\_security\\_survey/](http://www.theregister.co.uk/2004/10/27/netsec_security_survey/)

DDoS-атаки могут быть направлены против различных элементов сетевой инфраструктуры:

- **Приложение** – При осуществлении таких DDoS-атак атакующий использует известное поведение таких протоколов, как TCP и HTTP, в своих целях: для истощения вычислительных ресурсов и блокирования обработки транзакций или запросов. Примером являются атаки вида HTTP half-open и HTTP error. Эти атаки могут не израсходовать полностью все ресурсы общего пользования – таким образом, другие приложения остаются доступными.
- **Хост/Серверы** – Целью атак на эти элементы является превышение нормальной загрузки или авария хост-системы. Примером такой атаки является атака вида TCP SYN. Последствия таких атак можно минимизировать, если запускать на хосте протоколы со всеми необходимыми пакетами исправлений (патчами).
- **Пропускная способность** – Эти DDoS-атаки истощают пропускную способность входящего канала за счет отправки атакующих пакетов, адреса назначения которых являются частью адресного пространства сети. Маршрутизаторы, серверы и межсетевые экраны, являющиеся целью такой атаки и имеющие ограниченные ресурсы, могут оказаться недоступными для обработки корректно-сформированных транзакций, а также могут давать сбой под нагрузкой. Наиболее распространенным видом атак на пропускную способность является атака, заключающаяся в лавинообразной отправке пакетов, при которой большое количество разрешенных на первый взгляд TCP, UDP или ICMP пакетов направляют в определенный пункт назначения. Чтобы еще сильнее осложнить обнаружение атаки и сделать невозможной

распознавание нападающей стороны, при проведении таких атак также могут использовать спуфинг (подмену) IP-адреса источника.

- **Инфраструктура** – DDoS-атаки против инфраструктуры направлены против таких сетевых ресурсов, как DNS-серверы, программные коммутаторы VoIP, опорные маршрутизаторы, а также узкие каналы связи, которые важны для работы определенного сетевого сервиса или для всей сетевой инфраструктуры.
- **Косвенный ущерб** – Косвенным ущербом называется повреждение элементов сети, не подвергавшихся DDoS-атаке напрямую. Например, DDoS-атака против одного хоста в сети клиента, имеющей связи с несколькими другими сетями, с основным и резервным каналами связи. Если атака достаточно велика для того, чтобы истощить основной канал связи, она вызывает завершение BGP-сессии основного канала. В результате DDoS-трафик переключается на атаку хоста на резервном канале связи. Теперь истощение пропускной способности наблюдается на резервном канале связи, его BGP-сессия завершается, а DDoS-трафик переходит на основной канал и атакует хост. Так, в результате изменения маршрута DDoS-атака, направленная на хост, вызывает косвенный ущерб.

Принимая во внимание то, какое влияние DDoS-атаки могут оказывать на деятельность компании, необходимо иметь в своем распоряжении механизмы защиты для того, чтобы не оказаться застигнутыми врасплох. Общая стоимость владения этими механизмами защиты может оказаться значительно ниже чем объем возможного ущерба.

## **Решение Cisco Clean Pipes**


Решение Cisco Clean Pipes позволяет провайдерам услуг предлагать своим клиентам услугу защиты от DDoS-атак, одновременно укрепляя и защищая собственные сети. Cisco Systems определяет “Clean Pipes”, как хорошо продуманное и проверенное архитектурное решение для защиты потока данных (data pipe), обеспечивающего сами сервисы и их доступность. Поток данных может означать различные понятия в зависимости от типа клиента:

- Компания – канал последней мили
- Госучреждение – обмен критическими данными
- Оператор – все, что можно атаковать (точки пиринга, центр обработки данных, граничное устройство)

Наибольшую угрозу представляют собой распределенные DOS атаки, черви и вирусы. Фундаментальной целью решения “Clean Pipes” является удаление злонамеренного трафика из потока данных и доставка только истинного трафика с целью предотвращения исчерпания ресурсов.

## **Механизмы защиты, используемые в решении**

Существует много вариантов, позволяющих защититься от DDoS-атак и минимизировать вред, который они наносят. С точки зрения защиты DDoS-атаки являются одной из самых сложных сетевых угроз, поэтому принятие эффективных мер противодействия является исключительно сложной задачей для организаций, деятельность которых зависит от Интернета. DDoS-атаки сложно предотвращать и распознавать потому, что запрещенные пакеты неотличимы от разрешенных. Сетевые устройства и традиционные технические решения для обеспечения безопасности сетевого периметра, такие как межсетевые экраны и системы обнаружения вторжений (IDS), являются важными компонентами общей стратегии сетевой безопасности, однако, одни эти устройства не обеспечивают полной защиты от DDoS-атак. Чаще всего при проведении таких атак используется спуфинг (подмена) IP адресов источника, из-за чего становится невозможной идентификация с помощью инструментальных средств мониторинга аномалий трафика, следящих за необычайно высоким объемом трафика от конкретного источника.



Защита от текущей DDoS-атаки требует специализированной архитектуры, которая включает возможности обнаружения все более изощренных, сложных и обманчивых атак конкретного вида, и противодействия им. В отличие от существующих способов защиты от DDoS-атак решение Cisco Clean Pipes может точно отличать "хороший" трафик, направляемый на важный хост или приложение, от "плохого". Решение не только обнаруживает факт атаки, но также отфильтровывает "плохой" трафик и пропускает "хороший", обеспечивая непрерывность деятельности и предоставления услуг. Защиту сети от DDoS-атак обеспечивают три основные функции, которые предлагает решение:

- **Обнаружение** – Фундаментальной предпосылкой для обнаружения атак является построение контрольных характеристик трафика при работе сети в штатных условиях с последующим поиском аномалий в структуре трафика (отклонения от контрольных характеристик). Аномалия сетевого трафика – это событие или условие в сети, характеризующее статистическим отклонением от стандартной структуры трафика, полученной на основе ранее собранных профилей и контрольных характеристик. Любое отличие в структуре трафика, превышающее определенное пороговое значение, вызывает срабатывание сигнала тревоги.

Для определения аномалий в этом решении можно использовать продукты Cisco Traffic Anomaly Detector XT, модуль услуг Cisco Traffic Anomaly для маршрутизаторов Cisco серии 7600/коммутаторов Catalyst серии 6500, а также устройство Arbor Networks Peakflow SP.

- **Подавление** – Подавлением в решении Cisco Clean Pipes называется процесс "чистки" трафика (анти-спуфинг, распознавание аномалий, проверка пакетов и очистка: отбрасывание "плохого" трафика и разрешение прохождения "хорошего" трафика до конечного назначения).

Для подавления аномалий в этом решении можно использовать продукты Cisco Guard XT, модуль услуг Cisco Anomaly Guard для маршрутизаторов Cisco серии 7600/коммутаторов Catalyst серии 6500.

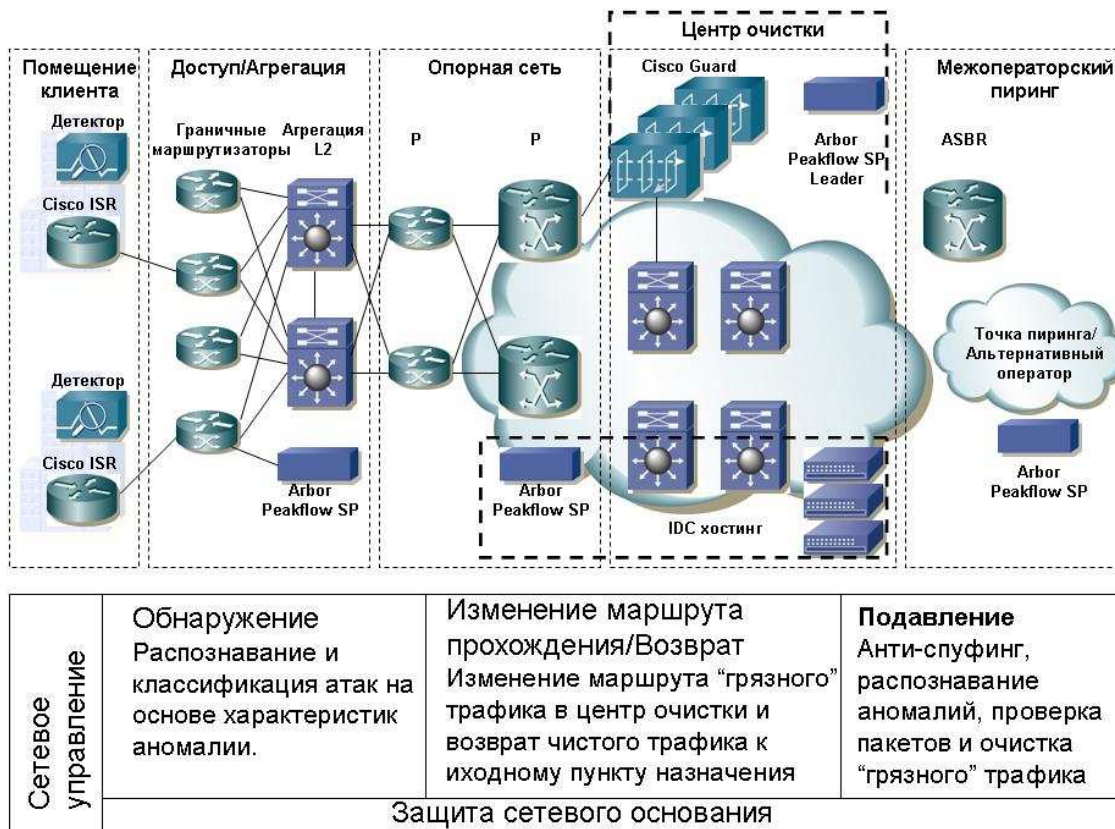
- **Изменение маршрута прохождения трафика и возврат трафика** – В рамках механизма изменения маршрута прохождения трафика на маршрутизатор в опорной сети направляются инструкции об изменении маршрута прохождения "грязного" трафика (лавинообразный поток пакетов с установленным битом SYN, пакеты с измененным адресом и т.п.) таким образом, чтобы он проходил через устройство Cisco Guard. По окончании "чистки" устройство Guard возвращает очищенный трафик обратно в сеть.

Поэтапное описание работы решения можно найти в разделе ["Как работает Cisco Clean Pipes?"](#).

## Принципы построения решения

Решение Cisco Clean Pipes – это не просто набор продуктов, обеспечивающих безопасность конкретного объекта; оно является тесно интегрированной системой, готовой к защите от самых разрушительных DDoS-атак сегодняшнего дня. Полная архитектура решения (цветом выделены ключевые элементы) показана на [рис. 1](#).

Рис. 1 Архитектура решения Cisco Clean Pipes



Решение Cisco Clean Pipes, объединяющее в себе целый набор продуктов для обнаружения и подавления DDoS-атак, значительно превосходит такой вариант решения, при котором эти устройства просто подключаются к маршрутизаторам. Решение служит надежной и комплексной архитектурой, предоставляя следующие преимущества:

- Решение предлагает методы построения решения, обеспечивающие эффективную интеграцию с сетью провайдера услуг, построенную на таких платформах Cisco, как Cisco 12000 и 7600/Catalyst 6500. Основываясь на результатах лабораторных исследований и проверок, Cisco предоставляет рекомендации в отношении оптимальных комбинаций маршрутных процессоров, линейных карт и конфигураций другого аппаратного обеспечения (основных платформ Cisco для маршрутизации и коммутации) в сети провайдера услуг, которые способны противостоять растущему числу DDoS-атак.
- Решение предлагает рекомендации по обеспечению безопасности, позволяющие укрепить сеть провайдера услуг и подготовить ее для быстрого противодействия и максимальной защиты от сетевых угроз различных видов.
- Решение обеспечивает систему сетевого управления, предназначенную для управления работой сети и предоставления абонентам отчетов об атаках.
- Решение поддерживает три конкретных модели развертывания услуг, основанных на общей архитектуре Clean Pipes, а также рекомендации по схемам защиты от DDoS-атак, оптимизированным для различных участков инфраструктуры провайдера услуг и сетей клиентов:

- **Управляемая защита сети от DDoS-атак** – Предлагает корпоративным клиентам эффективную защиту от DDoS-атак на их участке "последней мили" и в своих внутренних инфраструктурах посредством подписки на услугу Cisco Clean Pipes у провайдера услуг.
- **Управляемая защита хостинга от DDoS-атак** – Предлагает хостерам средства для защиты своих web-услуг и иных услуг хостинга от DDoS-атак.
- **Защита от DDoS-атак на границе обмена трафиком** – Предлагает провайдерам услуг средства, позволяющие не допустить истощения пропускной способности в результате DDoS-атак на точки обмена трафиком.

## Развертывание сетевой инфраструктуры безопасности с защитой сетевого основания (NFP)

Несмотря на то, что решение Cisco Clean Pipes предлагает комплексное решение для защиты от DDoS- для клиентов провайдеров услуг и собственных сетей провайдера, провайдерам услуг настоятельно рекомендуется внедрять набор технологий безопасности, известный как защита сетевого основания (NFP). NFP защищает уровень данных, уровень управления и уровень услуг от различных угроз безопасности. Преимущества развертывания NFP заключаются в том, что эти технологии:

- Предлагают защиту сетевых устройств не только от DDoS-атак, но также и от других векторов угроз, таких как разведка, проникновения в сетевое устройство и угроза услуге.
- Минимизируют уязвимость важных сетевых услуг провайдера услуг (DNS, электронная почта, WWW и VoIP) к сетевым атакам, увеличивая таким образом доступность сети и услуг для клиентов
- Используют сетевую телеметрию, например, систему NetFlow, для изучения структуры трафика в реальном времени, построения контрольных характеристик трафика, обнаружения аномалий и ошибок, а также для составления характеристик атакуемых интерфейсов, определения силы атаки и т.п. Аномалии затем сравнивают в масштабе всей сети для прослеживания атаки и определения ее точки входа.
- Дополняют решения Cisco Clean Pipes для защиты от DDoS. Технологии NFP подавляют DDoS-атаки примитивных видов, высвобождая мощности устройства Cisco Guard для борьбы против более изощренных атак, эксплуатирующих аномалии.

Примерный перечень возможностей NFP, которые обычно внедряют провайдеры услуг, приводится ниже:

- **Списки контроля доступа к инфраструктуре (iACL)** – Предназначены для защиты уровня управления маршрутизатора на пограничных устройствах сети и точках пиринга оператора
- **Списки контроля доступа на прием (rACL)** – Ограничивают прохождение пакетов на процессор маршрутизатора в зависимости от IP-адреса источника и назначения, а также от протокола и номера порта
- **Anycast** – Метод адресации IP, основанный на объявлении неуникальных IP-адресов из нескольких исходных точек и последующем использовании динамической маршрутизации для доставки апусаст-пакетов до элемента сети, ближайшего внутри сетевой топологии с точки зрения достижимости.
- **uRPF** – Заключается в отбрасывании IP пакетов, не содержащих верифицируемого IP адреса источника. Предназначена для борьбы с проблемами, вызванными подменой IP-адреса источника в сети.

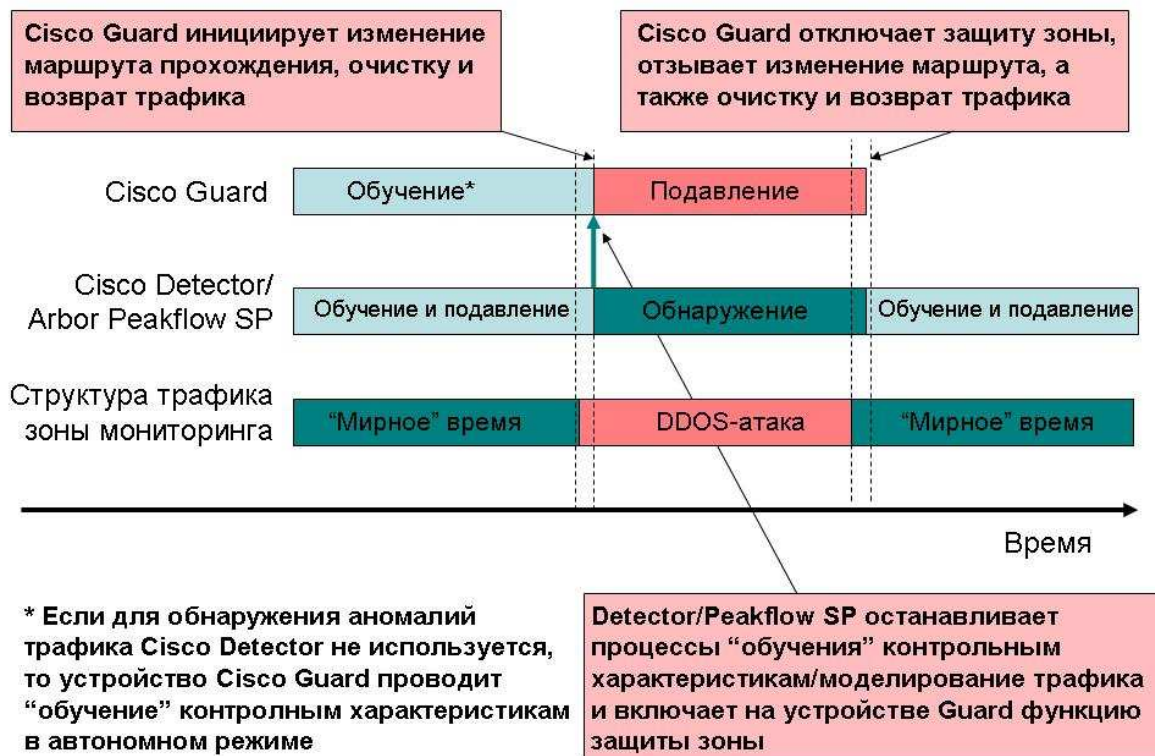
- **Удаленный запуск "черной дыры" (RTBH)** – Способ фильтрации, предназначенный для отбрасывания злонамеренного трафика на границе обмена трафиком данной сети.
- **Распространение политики управления качеством обслуживания с помощью протокола маршрутизации BGP (QPPB)/удаленный запуск ограничения скорости (RTRL)** – Механизм QPPB, также известный как RTRL, классифицирует злонамеренные пакеты на основании списков доступа, BGP community lists, а также на основании путей к автономным системам BGP, которые отправляет по BGP удаленное устройство, выступающее в роли инициатора данной политики.
- **Полисинг панели управления (CoPP)** – Функциональность, которая позволяет классифицировать пакеты, направляемые на центральный процессор, управлять потоком трафика (ограничивать скорость для определенного трафика). Обеспечивает защиту уровня управления маршрутизаторов и коммутаторов с ПО Cisco IOS от разведки и DDoS-атак.

За дополнительной информацией о NFP обращайтесь по адресу:  
<http://www.cisco.com/warp/public/732/Tech/security/infrastructure/>

## Как работаем Cisco Clean Pipes?

Как описано выше, решение Cisco Clean Pipes охватывает несколько компонентов, предназначенных для построения системы безопасности, включая Cisco Guard, Cisco Detector и Arbor Peakflow SP. Схема работы компонентов в составе решения Cisco Clean Pipes показана на [рис. 2](#).

**Рис. 2** Схема работы компонентов решения Cisco Clean Pipes



Ниже приведено последовательное описание этапов защиты зоны от DDoS-атак с помощью решения Cisco Clean Pipes (определения терминов, таких как «зона», а также других ключевых терминов, используемых в этом документе, приводятся в глоссарии на стр. 20) в следующем порядке: DDoS-атаки нет, атака начинается, атака подавлена.

Обратите внимание, что и детектор Cisco Detector, и устройство Arbor Peakflow SP предназначены для обнаружения аномалий, однако взаимоисключающими устройствами не являются. В то же время, существуют модели развертывания, которые лучше работают с определенными методами обнаружения. Эти варианты развертывания описаны в разделе "Модели развертывания Cisco Clean Pipes" на стр. 16.

**1-й этап "Обучение" контрольным характеристикам.** До момента начала DDoS-атаки компоненты решения Cisco Clean должны построить контрольные характеристики для нормальной структуры трафика в конкретной зоне, на основании которых можно было бы определять аномалии структуры трафика при DDoS-атаке на сетевое устройство (см. [рис. 3](#) ниже).

В сценарии, связанном с развертыванием устройств Arbor Peakflow SP и Cisco Guard, они обучаются структуре трафика независимо друг от друга. Peakflow SP моделирует структуру трафика на основе статистических данных, получаемых в "мирное время" по протоколу NetFlow, а Cisco Guard "обучается" нормальной структуре трафика для определенной зоны с помощью изменения маршрута прохождения трафика из внешней сети, и на основе полученных данных создает политики для потоков трафика разных сервисов, приходящих в зону (принципы работы изменения маршрута трафика будут объяснены описании 3-его этапа ниже). В том случае, если на зону нападают в процессе обучения, процесс обучения устройства Guard останавливается, и оно переключается в режим защиты.

В сценарии развертывания детектора Cisco Detector и устройства Cisco Guard созданием конфигурации зоны и построением результатов обучения нормальной структуре трафика занимается детектор. Оператор может отдавать инструкции детектору по загрузке созданных конфигураций в устройство Guard. Иными словами, в отличие от предыдущего сценария, при синхронизации работы с детектором от Guard не требуется ни конфигурировать зону, ни создавать политики для изменения маршрута трафика. Чтобы контрольные характеристики, необходимые для работы Guard и детектора, отвечали реальной сложившейся ситуации, можно проводить "обучение" раз в сутки. В том случае, если атака происходит в процессе обучения для определенной зоны, процесс обучения детектора останавливается, и он переключается в режим защиты.

**2-й этап Обнаружение.** После завершения процесса обучения для зоны, детектор Cisco и Arbor Peakflow SP переводятся в режим мониторинга трафика, идущего в зону, и при обнаружении аномалии сигнализируют о тревоге или активируют Cisco Guard.

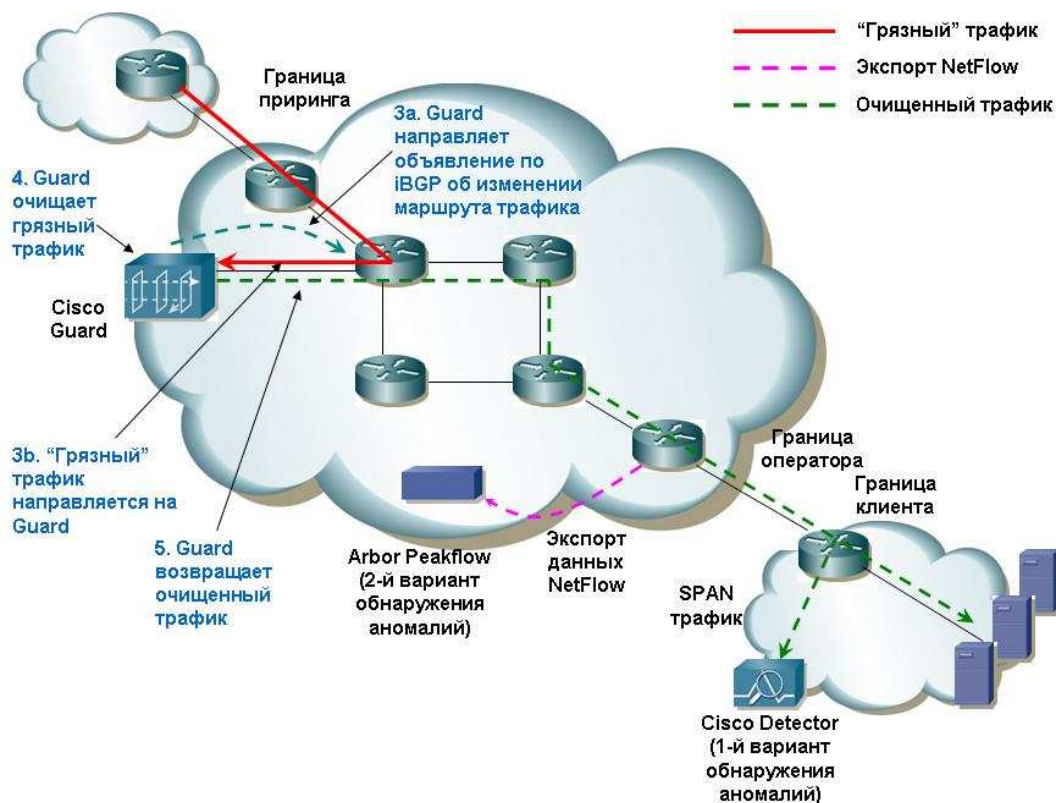
- a. **Детектор Cisco Detector.** Детектор Cisco Detector выполняет мониторинг зеркального трафика канала в непрерывном режиме. При обнаружении трафика, который в соответствии с его политиками определяется, как аномальный или злонамеренный (т.е. трафик, характеристики которого превышают определенные пороговые значения), детекторы проводят динамическое конфигурирование группы фильтров (динамические фильтры) с регистрацией события в системном журнале детектора, а сотрудникам технической поддержки отправляется уведомление. Если подлинность тревоги подтверждена, они могут в ручном режиме активировать Guard и перевести атакуемую зону в режим защиты. Также можно настроить детектор Cisco Detector на автоматическую активацию удаленного Guard по SSH сразу же после обнаружения DDoS-атаки. (См. [рис. 4](#) ниже).
- a. **Устройство Arbor Peakflow SP.** Устройства Arbor Peakflow принимают статистические данные, собранные по технологии NetFlow с разных маршрутизаторов в сети провайдера услуг. В том случае, когда Peakflow регистрирует превышение структурой трафика определенного уровня, оно выдает сигнал тревоги на Leader, и направляет ему характеристики информации аномального трафика для дальнейшего анализа. Далее мониторингом этого извещения продолжает заниматься Leader. При превышении определенного порогового уровня и длительности, заданных пользователем, как "опасные", Leader относит событие к разряду событий высокой важности ("красная" тревога"). В этот



соответствующий модуль защиты для аутентификации трафика, который отбрасывает трафик, не прошедший аутентификацию. Guard затем направляет трафик на ограничитель скорости, который отбрасывает трафик, превышающий определенную скорость. Затем очищенный трафик возвращается в зону и направляется в исходный пункт назначения. (См. [рис. 4](#) ниже).

**5-й этап Возврат трафика.** Очищенный трафик с выхода Guard возвращается в зону (см. [рис. 4](#)). Доступны различные методы в зависимости от того, на каком уровне построена топология опорной сети (уровень 2 или уровень 3). Они гарантируют, что возвращенный трафик не вернется обратно на Cisco Guard. Примеры этих методов включают маршрутизацию на основе политики (PBR), виртуальную маршрутизацию/коммутацию (VRF), схемы инкапсуляции GRE и виртуальные частные сети на основе MPLS. Подробное описание этих методов выходит за рамки настоящего документа.

**Рис. 4. Процессы Cisco Clean Pipes (2<sup>я</sup> половина): Подавление DDoS-атаки на зону модулем Cisco Guard**



**6-й этап Завершение очистки трафика.** Динамические фильтры устройства Guard имеют ограниченный жизненный цикл и стираются после отражения DDoS-атаки. По умолчанию Guard продолжает работать в режиме защиты до тех пор, пока пользователь не отключит его. Как вариант, Guard можно настроить на отключение режима защиты в том случае, если динамические фильтры не используются и никаких динамических фильтров не было добавлено за заданный период времени. После выхода устройства Guard из режима защиты оно отзывает прежнее объявление по BGP, и трафик возвращается на обычный путь данных до зоны. Если для изменения маршрута трафика используется устройство Arbor Peakflow SP или запускающий маршрутизатор, тогда объявление по BGP об изменении маршрута трафика необходимо удалять в ручном режиме.

## **Компоненты решения Cisco Clean Pipes**

### **Аппаратно-программное решение Cisco Guard XT и модуль услуг Cisco Anomaly Guard**

Аппаратно-программное решение Cisco® Guard XT 5650 для подавления DDoS-атак и модуль услуг Cisco Anomaly Guard предлагают мощную и полнофункциональную систему защиты от DDoS-атак. Решение Cisco Guard XT разработано в соответствии с требованиями в отношении производительности и масштабируемости, выдвигаемыми самыми крупными и наиболее сложными корпоративными сетями, и предлагает беспрецедентные уровни защиты от все более усложняющихся и трудноопределимых атак современности. За дополнительной информацией о решении Cisco Guard XT обращайтесь по адресу:

<http://www.cisco.com/en/US/products/ps5888/index.html>

Программно-аппаратное решение Cisco Guard XT с двумя интерфейсами Gigabit Ethernet способно обрабатывать трафик атаки на линейной скорости вплоть до полного гигабита в секунду. Модуль услуг Cisco Anomaly Guard является интегрированным модулем услуг для коммутаторов Cisco Catalyst серии 6500 и маршрутизаторов Cisco серии 7600 и может получать трафик по Ethernet со скоростью до 1 Гбит/с. Для инкрементального масштабирования и поддержки мультигигабитных скоростей можно объединять несколько аппаратно-программных решений Cisco Guard XT или модулей услуг Cisco Anomaly Guard в одно расширяемое решение, которое быстро адаптируется под расширение сферы деятельности крупного провайдера услуг и корпоративные сети.

Для обработки растущего числа DDoS-атак аппаратно-программные решения Cisco Guard или модули услуг можно линейно масштабировать и создавать из них кластер, известный, как "чистящий центр".


Платформа Cisco Guard (аппаратно-программное решение или модуль услуг) является составным элементом комплексного решения обнаружения и подавления атак, которое защищает сети корпораций, центры хостинга, правительственные учреждения и провайдеров услуг от DDoS-атак. В сочетании с устройствами обнаружения аномалий, такими как Cisco Traffic Anomaly Detector XT, модуль услуг Cisco Traffic Anomaly Detector или Arbor Peakflow SP, которые обнаруживают трафик DDoS, червей и другие атаки, платформа Cisco Guard проводит подробный анализ трафика на уровне потока, а также предлагает услуги определения и подавления, необходимые для блокирования трафика атаки и предотвращения его вредоносного влияния на работу сети. За дополнительной информацией о модулях услуг Anomaly Guard для Cisco Catalyst серии 6500 и Cisco серии 7600 обращайтесь по адресу:

<http://www.cisco.com/en/US/products/ps6235/index.html>

В целом аппаратно-программное решение Cisco Guard и модуль Cisco Anomaly Guard следует располагать максимально высоко по потоку трафика в защищаемые зоны, как можно ближе к источнику трафика атаки. В этом случае устройство Guard сможет защитить от трафика DDoS-атаки все нижерасположенные ресурсы: серверы, маршрутизаторы, коммутаторы, межсетевые экраны, системы обнаружения вторжений. Модуль Anomaly Guard также должен располагаться перед межсетевым экраном, чтобы обрабатывать трафик на этапе до преобразования сетевых адресов (NAT) и защищать от DDoS-атаки сам межсетевой экран.

### **Аппаратно-программное решение Cisco Traffic Anomaly Detector XT и модуль услуг Cisco Traffic Anomaly Detector**

Аппаратно-программное решение Cisco Traffic Anomaly Detector XT и модуль услуг Cisco Traffic Anomaly Detector являются комплексными решениями, помогающими крупным организациям защищаться от распределенных DoS-атак и позволяющими пользователям быстро включать услуги подавления и блокировать атаку прежде, чем она смогла бы оказать негативное влияние на деятельность предприятия.



Решение Cisco Traffic Anomaly Detector XT 5600 является высокопроизводительным автономным устройством для обнаружения DoS-атак. Оно получает копию трафика, идущего в защищаемую зону, либо за счет возможности зеркалирования, предлагаемой, например, используя SPAN, либо посредством сплиттера. Модуль детектора Cisco Traffic Anomaly является интегрированным модулем услуг для коммутаторов Cisco Catalyst серии 6500 и маршрутизаторов Cisco серии 7600. Он получает копию трафика, идущего в зону или используя SPAN или списки контроля доступа к виртуальной частной сети (VACL).

В обеих платформах обнаружения Cisco, основанных на уникальной архитектуре патентованного процесса мульти-верификации (MVP), для упреждающего обнаружения и идентификации нападений используются новейшие поведенческие технологии анализа и распознавания атак. Детектор Cisco Detector в непрерывном режиме проводит мониторинг трафика, пунктом назначения которого является защищаемое устройство, такое как Web-сервер или сервер приложения электронной торговли, и составляет подробные профили того, как отдельные устройства ведут себя в штатных рабочих условиях. Любые отклонения от профиля, замеченные в любом из потоков, детектор Cisco Detector расценивает как угрозу атаки и в соответствии с пользовательскими настройками принимает ответные действия, направленные на обеспечение надежной защиты сетей и трафика, важного для деятельности предприятий: отправляет оператору предупреждение о необходимости включения мер реагирования в ручном режиме или запускает существующую систему управления (или аппаратно-программное решение Cisco Guard XT или модуль услуг Cisco Anomaly Guard) для быстрого включения услуги подавления и удаления злонамеренного потока атаки без ущерба для разрешенных транзакций.

Используемый в детекторе Cisco графический пользовательский Web-интерфейс показывает информацию в простом интуитивно-понятном виде и значительно упрощает конфигурирование, управление, а также обнаружение и анализ атак. В логической схеме аппаратно-программное решение детектора Cisco Detector и модуль детектора Cisco Traffic Anomaly Detector располагаются ниже аппаратно-программного решения Cisco Guard и модуля Anomaly Guard, но выше межсетевых экранов. В "мирное" время устройство Detector (аппаратно-программное решение или модуль детектора) просматривает входящий и исходящий трафик, пунктом назначения которого указана защищаемая зона. В ситуации, когда для подавления атаки устройство Guard (аппаратно-программное решение или модуль Guard) изменяет маршрут трафика из целевой зоны, устройство "детектор" будет видеть на выходе устройства Guard только "очищенный" трафик, пунктом назначения которого является целевая зона.

За дополнительной информацией о детекторе Cisco Traffic Anomaly Detector обращайтесь по адресу: <http://www.cisco.com/en/US/products/ps5887/index.html>

За дополнительной информацией о модуле услуг детектора аномалий трафика для коммутаторов Cisco Catalyst серии 6500 или маршрутизатора Cisco серии 7600 обращайтесь по адресу:

<http://www.cisco.com/en/US/products/ps6236/index.html>

## Технология Cisco NetFlow

Cisco NetFlow является основной и наиболее часто используемой технологией, применяемой для обнаружения DDoS-атак и анализа сетевого трафика в современных IP-сетях. Технология NetFlow поддерживают практически все маршрутизаторы провайдеров услуг с программным обеспечением Cisco IOS, а также некоторые платформы коммутации класса high-end с программным обеспечением CatOS, а с недавнего времени – через специализированные интегральные схемы (ASIC) – аппаратно. Технология предназначена для предоставления важной информации о качественных и количественных характеристиках трафика, использовании канала связи и о профилях трафика в сети.

NetFlow классифицирует пакеты по потокам. Каждый поток определяется своей уникальной характеристикой, состоящей из семи ключей: интерфейс входа, тип IP-протокола, байт типа сервиса (ToS), IP-адреса источника и назначения, номера портов источника и назначения. Такой уровень гранулярности сведений о потоке дает возможность коллектору NetFlow легко справляться с мониторингом больших объемов трафика. Семь ключей NetFlow предоставляют достаточно информации

для профилирования контрольных характеристик и полной ("кто, что, где, когда и как") идентификации сетевого трафика .

Аномалия сетевого трафика – это событие или условие в сети, характеризующее статистическим отклонением от стандартной структуры трафика, полученной на основе ранее собранных профилей и контрольных характеристик. NetFlow дает пользователям возможность проведения подробного учета потока трафика и распознавания аномалий. Отклонения от стандартной структуры трафика свидетельствуют об изменении структуры и являются первыми признаками потенциальной атаки. NetFlow обычно разворачивают по всей границе сети провайдера услуг для мониторинга входящего трафика на границе и на пиринговых интерфейсах, то есть, на "обычных" для большинства атак точках входа. Для слежения за текущими потоками маршрутизатор сохраняет активный кэш Cisco IOS NetFlow.

Для проведения дальнейшего анализа внешний коллектор может импортировать информацию об IP-потоке из кэша NetFlow, а для определения того, какие из сетевых узлов находятся под DDoS-атакой и для определения ее характеристик, данные потока с нескольких коллекторов можно сопоставлять. Примером таких приложений-коллекторов является Arbor Peakflow SP. Это инструментальное средство с графическим пользовательским интерфейсом, которое может применять такие способы защиты от DDoS-атак, как входящие списки контроля доступа (input ACL), распознавание приложений в сети (NBAR), uRPF и активацию устройства Cisco Guard.

За дополнительной информацией о Cisco NetFlow обращайтесь по адресу: <http://www.cisco.com/warp/public/732/Tech/nmp/netflow/>

## Arbor Networks Peakflow SP

Arbor Networks® Peakflow® SP (сокращенно Peakflow SP) – это масштабируемая платформа, предлагающая провайдерам услуг и их клиентам комплексное решение с мощными возможностями в отношении DDoS-атак, управления трафиком и маршрутизации. Она состоит из трех устройств: управляемые услуги (Managed Services), инфраструктура безопасности (Infrastructure Security), а также трафик и маршрутизация (Traffic and Routing). Возможности Peakflow SP в отношении управляемых услуг позволяют провайдерам услуг предлагать своим корпоративным клиентам масштабируемые инструментальные средства для защиты от DDoS-атак и управления трафиком. Возможности в отношении инфраструктуры безопасности предлагают сетевым операторам возможности упреждающего обнаружения и подавления в масштабах всей сети таких аномалий, как DDoS-атаки и сетевые черви. Возможности Peakflow SP в отношении трафика и маршрутизации моделируют сетевой трафик и дают операторам необходимую информацию для принятия бизнес-решений в отношении маршрутизации, транзита, партнеров и клиентов.

В схеме решения Cisco Clean Pipes платформа Peakflow SP предлагает упорядоченный подход к обнаружению, отслеживанию источника и подавлению DDoS-атак. Сначала платформа создает модель нормального поведения в пределах сети, используя поток данных, доступный с маршрутизаторов, развернутых в сети. В отличие от встроенных методов сбора данных (например, с помощью детектора Cisco Detector), платформа Peakflow SP собирает статистические данные потока по технологии Cisco NetFlow от маршрутизаторов Cisco по выделенным каналам, то есть, Peakflow SP можно масштабировать по мере роста сети. Технология NetFlow, используемая для сбора, не влияет на режим работы сети: не уменьшает ее производительности и надежности. Проводя сравнение трафика с контрольными характеристиками в режиме реального времени, система сигнализирует об аномалиях и предоставляет информацию об атакуемых интерфейсах, серьезности атаки и т.п. Аномалии затем сравнивают в масштабе всей сети для прослеживания атаки и определения ее точки входа. Наконец, на основании специфических характеристик аномалии, Peakflow SP рекомендует соответствующие меры противодействия, способствующие обеспечению непрерывности услуги. Если для защиты от DDoS-атак платформа Peakflow SP работает в паре с устройством Cisco Guard, то при получении характеристик аномалии для определенной зоны с коллектора она устанавливает соединение по SSH для активации устройства Cisco Guard и перевода зоны в режим защиты.

Для определения аномалий и распознавания атак в масштабах сети Peakflow SP использует два наиболее эффективных метода, доступных в наше время: анализ сигнатур и динамическое профилирование. При

анализе сигнатур (обнаружении нецелевого использования) осуществляют поиск заранее определенных отклонений от установленных норм, являющихся признаками DDoS-атаки: например, большое количество эхо-запросов (ICMP-пакетов) за очень короткий промежуток времени – нормальная работа сетевых устройств такую структуру трафика не создает, поэтому такую аномалию легко обнаружить и распознать.

Для обнаружения более изощренных атак в масштабах всей сети в Peakflow также используют динамическое создание профилей. Основой для этого метода обнаружения является модель нормального поведения, которую Peakflow создает в масштабах всей сети, и с которой, как с "контрольными характеристиками" сравнивают текущий трафик. Динамические профили, обновляющиеся по мере изменения структуры трафика с течением времени, включают, как временные, так и топологические компоненты, и позволяют создавать сложные модели поведения сети. Затем система Peakflow применяет специализированные алгоритмы реального времени, позволяющие отличить разрешенный нормальный трафик от DDoS-атак.

За дополнительной информацией о Arbor Peakflow SP обращайтесь по адресу: [http://arbor.net/products\\_sp.php](http://arbor.net/products_sp.php)

## **Модели развертывания Cisco Clean Pipes**

Решение Cisco Clean Pipes имеет своей целью собрать возможности продуктов Cisco для защиты от DDoS-атак, интегрировать их с продуктами сетевой инфраструктуры и "наилучшими методами" инфраструктуры безопасности и получить систему с проверенными рекомендациями по проектированию моделей развертывания, которые провайдеры услуг могут предлагать в качестве услуги своим корпоративным клиентам.

Многие из тех способов, которые обсуждаются в этом разделе, могут быть использованы самими провайдерами для защиты своих собственных сетей от атаки. Одним из таких примеров является модель точки обмена трафиком, которая обсуждается в разделе "[Защита от DDoS точки обмена трафиком](#)" на стр. 19.

## **Управляемая защита сети от DDoS**

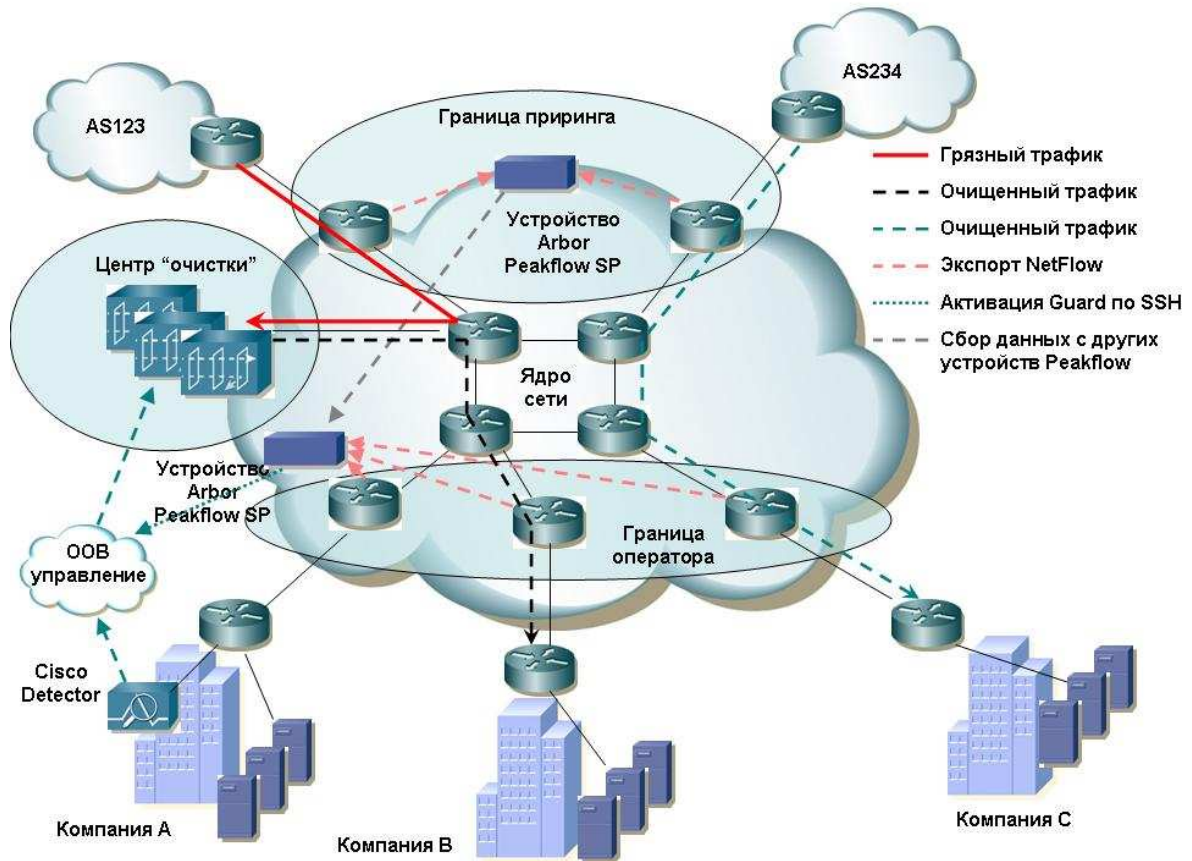
Эта модель услуги дает провайдерам услуг возможность подавлять DDoS-атаки из Интернета на сети своих корпоративных клиентов. Эти атаки не только влияют на хосты и приложения, работающие на них, но также наносят еще больший вред: огромное количество пакетов, создаваемых в ходе этих атак, истощают пропускную способность канала связи между сетью провайдера услуг и сетью клиента, блокируя доступ в корпоративную сеть разрешенного трафика из Интернет. Для клиентов, работающих в сфере финансов или электронной коммерции, результатом такой атаки может стать потеря клиентов. Кроме того, такая атака может нанести урон их репутации и привести к ситуациям, в которых возникает юридическая ответственность.

Эффективность подавления DDoS-атак тем выше, чем раньше было обнаружено их начало и чем выше по сети они остановлены. Услуги Cisco Clean Pipes предоставляет провайдерам услуг возможность предложить такой сервис своим корпоративным клиентам. В целом провайдер услуг может предлагать защиту от DDoS-атак для своих корпоративных клиентов услуги Cisco Clean Pipes по двум схемам:

- **Выделенная услуга** – Эта первоклассная услуга подходит для клиентов, бизнес которых зависит от Интернет: компании, занимающиеся онлайн-торговлей, финансовые круги и другие компании, занимающиеся электронной коммерцией. Выделенная услуга должна обеспечивать возможности очистки передаваемого трафика, "обучение" политикам и настройку, а также дополнительные возможности обнаружения DDoS-атак и активации процедур очистки трафика на стороне клиента.
- **Услуга коллективного пользования** – Эту услугу провайдер услуг предлагает по более приемлемой цене, и предназначена она для других корпоративных клиентов, которым необходим

определенный уровень защиты от DDoS-атак для своих онлайн-услуг, однако, эта проблема не стоит для них настолько остро, как для тех, которые подписываются на выделенную услугу. Услуга предлагает возможности по очистке трафика по принципу максимума усилий (коллективно для всех клиентов), стандартную политику для обнаружения DDoS-атаки и не предусматривает никаких возможностей по обнаружению DDoS-атак и активации процедур очистки трафика на стороне клиента.

**Рис. 5** Управляемая услуга защиты сети от DDoS-атаки



В проекте архитектуры выделенной услуги аппаратно-программное решение Cisco Guard или модули услуг Cisco Anomaly Guard, расположенные в центре очистки в сети провайдера услуг, предназначены только для одного клиента. Количество этих устройств определяется размером самой масштабной из DDoS-атак, от которой клиент хочет быть защищен. У провайдера услуг может быть более одного центра очистки в зависимости от того, сколько точек обмена трафиком соединяют провайдера с другими частями Интернета, и насколько далеко они разнесены. Целью проекта является подавление трафика атаки настолько далеко от целевой сети или устройства, насколько это возможно, с какой бы из точек обмена трафиком она ни приходила.

В рамках выделенной услуги для обнаружения DDoS-атак в помещениях клиента может быть развернуто аппаратно-программное решение Cisco Detector XT, а в сети провайдера услуг – Arbor Peakflow SP для получения данных статистики по NetFlow с опорных маршрутизаторов. Возможно также использование двух решений одновременно. Установка решения Cisco Detector XT предлагает клиентам необходимую гибкость: они могут сами настраивать политики на устройстве, определяющие чувствительность к аномалиям и пороговые значения для срабатывания тревоги.

В проекте услуги коллективного пользования аппаратно-программное решение Cisco Guard или модули услуг Cisco Anomaly Guard, установленные в центре очистки, находятся в коллективном пользовании нескольких клиентов. Услуга предлагает только очистку от DDoS-трафика по принципу максимума усилий, поэтому провайдер услуг не может принимать дополнительную заявку на подавление DDoS-атаки, если все аппаратно-программные решения Guard уже работают на полную мощность и занимаются подавлением существующих атак.

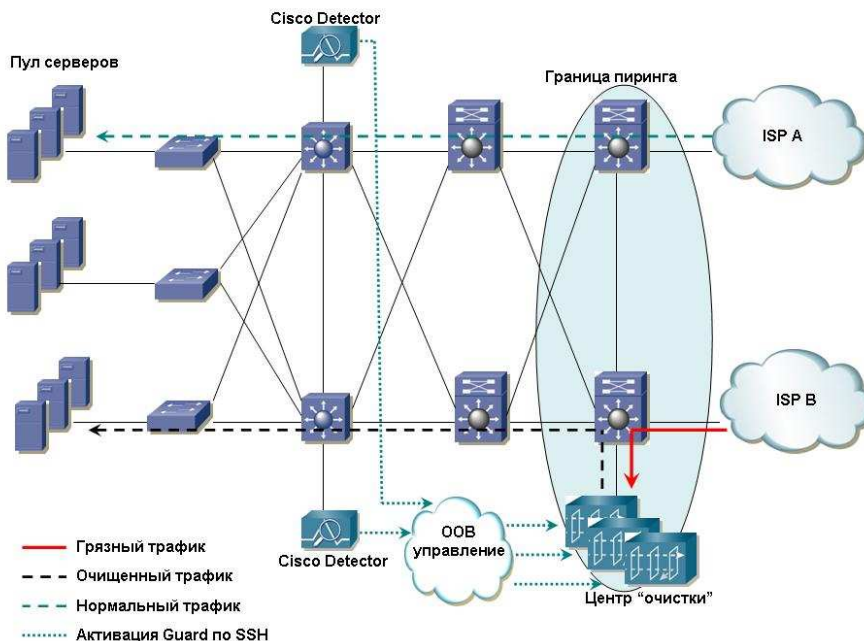
Для услуги коллективного пользования предпочтительным вариантом для обнаружения DDoS-трафика является развертывание только Arbor Peakflow SP. Arbor Peakflow SP является масштабируемым вариантом решения обнаружения, при котором статистику по протоколу NetFlow для распознавания аномалий собирают одновременно с нескольких маршрутизаторов. Это экономичный вариант: если клиентам не требуется подробное обнаружение DDoS-атак, тогда им не нужно приобретать устройства для обнаружения, устанавливаемые на стороне клиента.

В обеих схемах устройство Cisco Guard можно переводить в режим защиты зоны после обнаружения DDoS-атаки в ручном или автоматическом режиме. Активация в ручном режиме дает возможность провайдеру услуг или клиенту сначала проверить, реальная ли это атака или ложное срабатывание. В том случае, если атака реальная, провайдер услуг по поручению клиента переходит к активации защиты зоны.

## Управляемая защита хостинга от DDoS-атак

Эта модель услуги дает возможность провайдерам хостинга предоставлять защиту от DDoS-атак своим клиентам, которые используют их модели управляемого web-хостинга и хостинга приложений. Услуга управляемой защиты от DDoS-атак предлагается в качестве дополнительного расширения набора существующих услуг хостинга провайдера. Это предложение подразумевает защиту от DDoS-атак по принципу максимума усилий и предлагает шаблоны политик для обнаружения и подавления трафика по умолчанию. Оно похоже на коллективные услуги, описанные ранее, как "услуга управляемой защиты сети от DDoS".

**Рис. 6** Управляемая защита хостинга от DDoS-атак

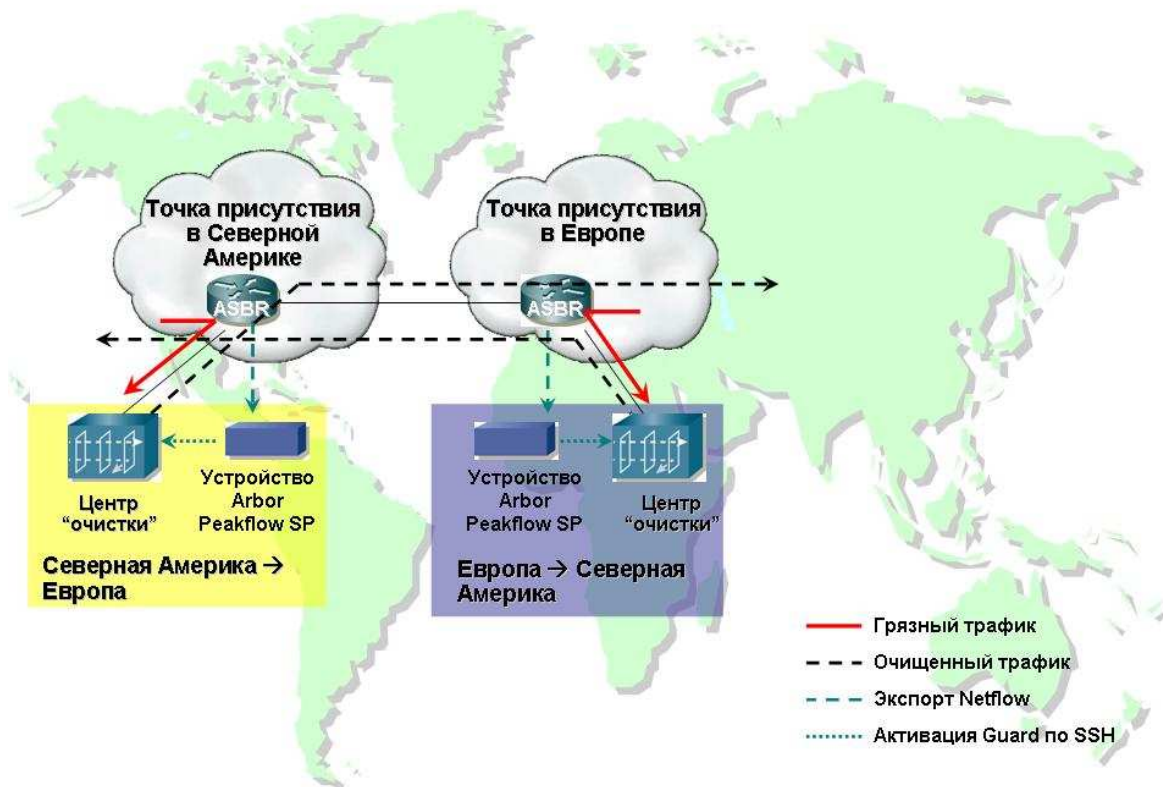



В этом проекте архитектуры для обнаружения DDoS-атак используют либо аппаратно-программное решение Cisco Detector XT, либо Arbor Peakflow SP (но не оба сразу!). Для подавления DDoS-атак аппаратно-программное решение Cisco Guard XT или модуль услуги Cisco Anomaly Guard, находящиеся в коллективном доступе, располагают в центре очистки рядом с точкой обмена трафиком сети провайдера хостинга, защищая пропускную способность опорной сети от истощения трафиком атаки.

## Защита точки обмена трафиком от DDoS-атак

Как показано на рис. 8, эта модель услуги предотвращает истощение трафика из-за DDoS-атак на точку обмена трафиком провайдера услуг или сетевые точки доступа. Если в сети не используется услуга Cisco Clean Pipes, тогда DDoS-атака может блокировать переход разрешенного трафика по соединению от одной точки обмена трафиком до другой. Эта услуга отличается от двух предыдущих моделей услуги защиты тем, что ее можно предлагать не только, как услугу управляемой защиты от DDoS-атак, но также в качестве эффективной системы защиты от DDoS-атак собственной инфраструктуры провайдера услуг. Пример использования этой модели в качестве управляемой услуги включает защиту каналов связи к нисходящим провайдерам услуг Интернет. Примерами использования этой услуги для инфраструктуры безопасности является защита каналов связи между двумя областями сети внутри иерархической сети одного провайдера услуг, трансатлантические каналы связи между автономными системами и каналы, соединяющие две разобщенные автономные системы одного провайдера услуг по инфраструктуре промежуточного провайдера магистральной.

**Рис. 7 Услуга защиты точки обмена трафиком от DDoS-атаки для трансатлантического канала связи**





В проекте этой модели устройство Arbor Peakflow SP предлагает масштабируемый подход к обнаружению DDoS-атаки и выполняет функции централизованной платформы для агрегирования статистических данных NetFlow с маршрутизаторов в различных точках обмена трафиком. Для подавления DDoS-атаки центр очистки следует располагать рядом с точкой обмена трафиком источника так, чтобы пакеты DDoS-атаки можно было отфильтровать прежде, чем они смогут истощить соединение с точкой обмена трафиком, являющейся пунктом назначения. Таким образом, если от DDoS-атак необходимо защищать трафик, проходящий по каналу связи между двумя точками обмена трафика в обоих направлениях, тогда необходимо устанавливать два независимых центра очистки на каждой стороне сети.

## Глоссарий

В следующей таблице приведены основные термины, используемые в этом документе, и дано их определение.

Термин	Определение
<b>Очищенный трафик</b>	Разрешенный трафик, который устройство Cisco Guard возвращает в сеть после очистки грязного трафика.
<b>Атака, направленная на отказ в обслуживании (DoS)</b>	Атака на компьютерную систему или сеть, заключающаяся в поглощении пропускной способности атакуемой сети или перегрузке вычислительных ресурсов атакуемой системы, приводящая к недоступности определенного сервиса для пользователей – как правило, сетевого подключения и услуг.
<b>Грязный трафик</b>	"Грязный" трафик, содержащий как разрешенные, так и DDoS-пакеты, направляемый на Cisco Guard.
<b>Распределенная атака, направленная на отказ в обслуживании (DDoS)</b>	DoS-атака, запущенная несколькими взломанными хостами, которыми взломщик может управлять удаленно.
<b>Зона</b>	Элемент сети, защищенный от DDoS-атак устройством Cisco Guard . Зоной может быть сетевой сервер, клиент или маршрутизатор; сетевой канал связи, подсеть или целая сеть; отдельный пользователь Интернет или компания; провайдер услуг Интернет или их любая комбинация.

Подготовил: Михаил Захватов (mzakhvat@cisco.com)

### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R) DM/LW7389 11/04

Cisco Systems, Inc.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.