ЗАЩИТА ОТ АТАК «ОТКАЗ В ОБСЛУЖИВАНИИ» С ПОМОЩЬЮ CISCO GUARD

СОВРЕМЕННЫЙ БИЗНЕС И ИНТЕРНЕТ

Сегодня Интернет стал центром развития новых технологий, в корне меняющих методы взаимодействия и ведения бизнеса между конечными пользователями, поставщиками, партнерами и сотрудниками компаний. Обмениваясь данными через сеть, особенно при использовании ресурсов сетей общего доступа, например Интернет, пользователи должны быть уверены в том, что важная информация и ресурсы компании всегда будут доступны для ведения бизнеса. С развитием возможностей сети Интернет обострилась и проблема атак на ее ресурсы.

DDOS-АТАКИ

По статистике каждые 5 минут в мире происходит 2 атаки, направленные на выведение сетевых ресурсов из строя (т.н. атаки «отказ в обслуживании» или Denial of Service). Генерация большого числа паразитного трафика снижает способность атакуемых узлов (принадлежащих не только операторам связи, но и обычным компаниям) обслуживать легитимных пользователей. Ситуация усугубляются тем, что при современном уровне развития хакерских технологий для нарушения работоспособности даже мощного сервера, имеющего производительный канал доступа в Интернет, достаточно обычного модемного соединения. Разумеется при условии, что их много. В этом случае достигается эффект лавины, когда множество «слабых» каналов в сумме перекрывают возможности даже крупного оператора связи. Такие атаки «отказ в обслуживании» получили название распределенных (Distributed Denial of Service, DDoS) и в отличие от обычных сетевых атак, которые приводит к взлому отдельных узлов и краже конфиденциальной информации, DDoS-атаки могут даже парализовать работу целых сетей.

На сегодняшний день DDoS-атаки являются серьезной угрозой для бизнеса – они уже являются причиной многомиллиардных убытков – от них пострадали известные компании, порталы и платежные системы – CNN, Amazon, eBay, ZDNet, WorldPay, PayPal и т.п. В январе 2001 DoS-атака на Microsoft привела к ущербу в 500 миллионов долларов. А зимой 2002 года был зафиксирован первый случай банкротства компании, пострадавшей от DDoS-атаки. Помимо финансового ущерба распределенные DoS-атаки приводят к снижению производительности, потере доходов, росту затрат на восстановление атакованной системы, падению репутации, искам со стороны пострадавших и т.п. В таблице 1 приведена стоимость одной минуты простоя для различных приложений для электронного бизнеса.

Таблица 1. Стоимость одной минуты простоя

Приложение	Стоимость минуты простоя, долл. США
Управление производством	13000
Управление поставками	11000
Электронная коммерция	10000
Электронный банк	7000
Сервисный центр	3700
Переводы денег	3500

Приложение	Стоимость минуты простоя, долл. США
Обмен сообщениями	1000

Есть и другая, такая же говорящая, статистика опасности DoS- и DDoS-атак – 93% компаний, лишившихся доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно.

Растущая зависимость бизнеса от Интернет и информационных технологий делает его подверженным DoS-атакам и заставляет задуматься о необходимости защиты. Однако отразить их, и в особенности их распределенные варианты, не такое простое дело, как может показаться на первый взгляд.

НЕДОСТАТКИ ТРАДИЦИОННЫХ ПОДХОДОВ

Традиционные решения, часто используемые для обнаружения и отражения DoS- и DDoS-атак неэффективно решают эту задачу по ряду причин:

- Межсетевые экраны если и обнаруживают атаку, то блокируют доступ с адреса, с которого эта атака исходит. При этом запрещается передача любого трафика и плохого и хорошего. А учитывая, что DoS-атаки часто совершаются с подменой адреса, то применение межсетевых экранов только усугубляет ситуацию и может заблокировать даже легитимных пользователей.
- Маршрутизаторы с функциями защиты часто используют те же подходы, что и межсетевые экраны, а, следовательно, также неэффективны. Кроме того, выделение ресурсов под задачу обнаружения распределенных атак приводит к снижению производительности маршрутизатора.
- Системы обнаружения вторжения, как видно из их названия, способны только обнаруживать атаки – функции отражения в них ограничены. Развитие этой технологии – системы предотвращения, могут блокировать DoS-атаки, но только ограниченное их число. Это связано с тем, что большинство современных защитных систем данного класса построено по сигнатурному принципу и не способны обнаруживать действия, для которых не созданы шаблоны-сигнатуры. Кроме того, далеко не каждая DoS-атака состоит из сплошь вредоносных пакетов, которые легко отследить. Зачастую в рамках атак «отказ в обслуживании» реализуются нормальные действия (например, обращение к сайту), только их слишком много.
- Последний класс средств, используемых для защиты от DoS-атак – балансировщики нагрузки (load balancer), которые отслеживают большое число соединений и в случае превышения порогового значения перенаправляют избыточный трафик на резервные узлы. Однако данный подход позволяет обнаруживать только один тип DoS-атак – SYN Flood.

CISCO GUARD

Учитывая описанные сложности, компания Cisco Systems предлагает свое решение для обнаружения традиционных и распределенных DoS-атак – Cisco Guard. Оно использует целую комбинацию различных подходов, построенных по принципу обнаружения отклонений от заранее известного поведения сетевого трафика (т.н. аномалии). Все реализованные в Cisco Guard подходы, каждый из которых имеет свои достоинства и ограничения, вместе обеспечивают эффективное обнаружение различных типов атак «отказ в обслуживании» (в т.ч. и с подменой адреса):

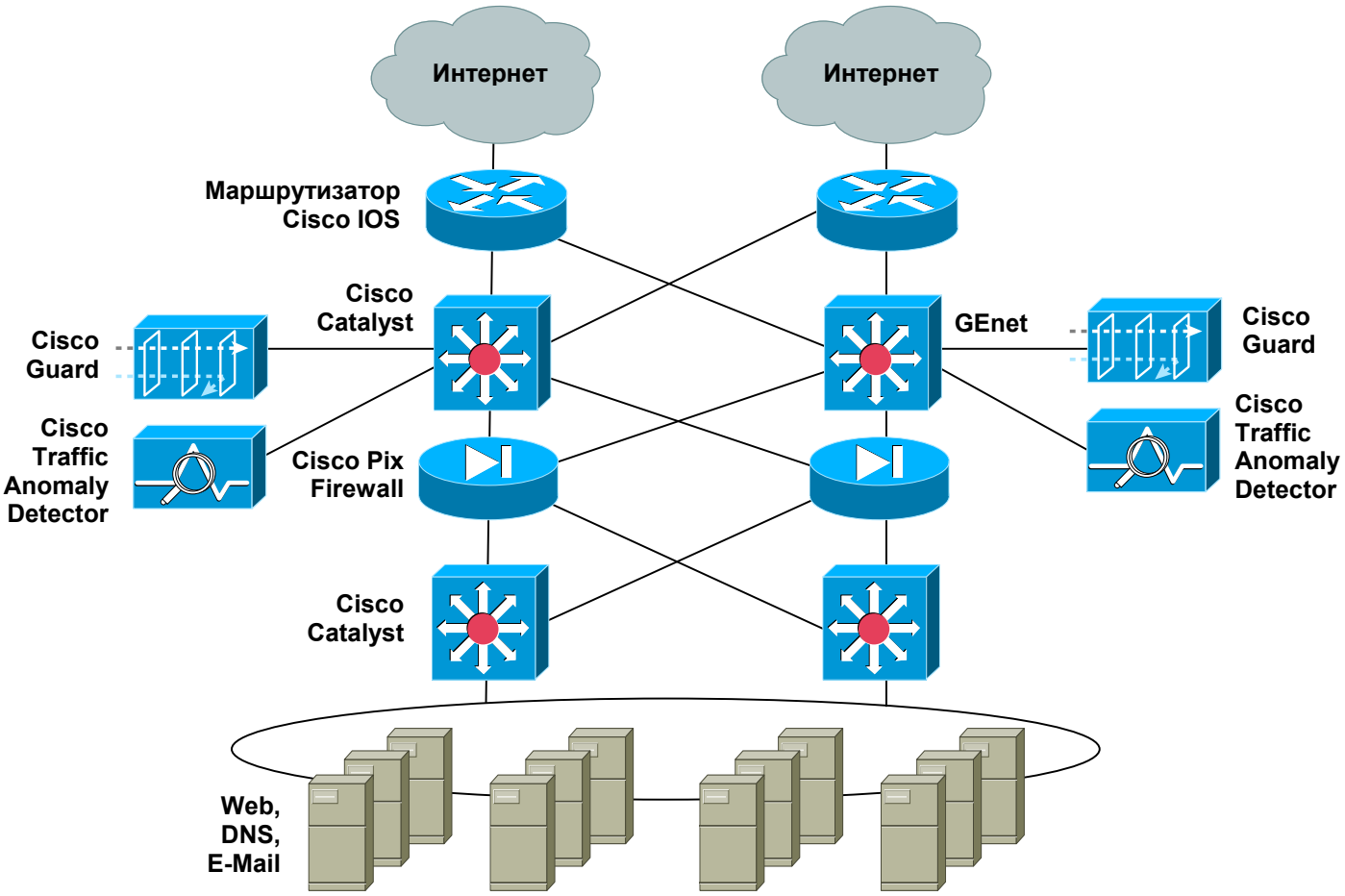
- Лавина, шторм
    - TCP Flood, UDP Flood, ICMP Flood
    - Spoofing Flood
    - FIN Flood
    - SYN/ACK Flood

- Ping Flood
- Smurf
- И т.д.

- Фрагментированные атаки (например, для протоколов TCP, UDP и ICMP)
- DNS-атаки
- HTTP-атаки (например, HTTP Get Flood)
- BGP-атаки
- Действия червей (например, сканирование сети в поисках новых жертв)
- И т.д.

Основная задача Cisco Guard – отражение атак, обнаруженных специализированными средствами обнаружения вторжения, в качестве которых могут выступать Cisco Anomaly Traffic Detector, Cisco IDS 42xx или Arbor Peakflow. Блокирование основано на методе «отвода» трафика и позволяет отделить вредоносные пакеты от несущих полезные данные. Этот программно-аппаратный комплекс:

- получает сигналы тревоги из различных источников,
- идентифицирует и блокирует вредоносный трафик,
- ограничивает полосу пропускания (в т.ч. и для нормального трафика),
- выделяет нормальный трафик и направляет его к цели, предотвращая выведения ее из строя.



Уникальная архитектура Multiverification Process (MVP) позволяет обеспечить очень высокую скорость обработки трафика и обнаружения DoS-атак без снижения производительности защищаемой сети. Технические характеристики Cisco Guard таковы:

- Скорость обработки трафика – 1,25 миллионов пакетов в секунду (возможность масштабирования до 10 миллионов пакетов в секунду путем использования кластеров Cisco Guard).
- Число параллельно обрабатываемых соединений – 1,5 миллиона.
- Защита от одновременной атаки со стороны свыше 100 тысяч зомби (механизм Zombie Killer).
- Число динамических фильтров – 150000 (добавление 1000 фильтров в секунду).
- Задержка – менее 1 мсек.

Управление всеми устройствами Guard, установленными в сети, осуществляется централизованно. При этом существует возможность интеграции с централизованной системой сбора сигналов тревоги от разнородных средств защиты – CiscoWorks Security Information Management Solution.

CISCO GUARD У ОПЕРАТОРОВ СВЯЗИ

Одно из основных применений Cisco Guard – защита ресурсов операторов связи от распределенных атак «отказ в обслуживании», от которых не способны обезопасить никакие другие средства. При этом использование Cisco Guard позволяет защитить оператора от исков со стороны клиентов, которые могли бы пострадать в случае отсутствия защиты. Такие прецеденты уже известны в США и Европе. В качестве примера операторов связи, использующих Cisco Guard, можно назвать AT&T, Sprint, RackSpace, DataPipe и другие. Кроме защиты собственных ресурсов оператор связи получает также возможность предложить своим заказчикам услуги аутсорсинга (Managed Security Service).

CISCO GUARD В КРУПНЫХ КОМПАНИЯХ

Помимо защиты операторов связи Cisco Guard позволяет отражать атаки на центры обработки данных и ресурсы компаний, ведущих электронный бизнес. При этом заказчики получают сразу множество уникальных возможностей:

- Защита полосы пропускания «последней мили».
- Повышение отказоустойчивости и доступности корпоративных ресурсов.
- Повышение качества обслуживание и соблюдение необходимого уровня SLA.
- Оплата только легитимного трафика.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Cisco Guard

http://www.cisco.com/go/guard

CiscoWorks Security Information Management Solution

http://www.cisco.com/go/sims

Решения Cisco Systems по информационной безопасности

http://www.cisco.com/go/security

Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **Cisco Connection Online Web site at http://www.cisco.com/ http://www.cisco.ru/**

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