ШЕСТИФАЗНАЯ МЕТОДОЛОГИЯ CISCO SYSTEMS ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СЕТЕЙ ОПЕРАТОРОВ СВЯЗИ

БЕЗОПАСНОСТЬ ОПЕРАТОРОВ СВЯЗИ ВЧЕРА, СЕГОДНЯ И ЗАВТРА

Операторы связи меняются – меняется все, используемые технологии, оборудование и даже бизнес-модели. И если раньше сети преимущественно строились на коммутируемых телефонных сетях общего пользования, то сейчас ситуация коренным образом изменилась - операторы связи активно внедряют инфраструктуру IP/MPLS. За технологическим изменением следует и изменение в области обеспечения безопасности операторских сетей. Если раньше операторы фокусировались на пропускной способности, задержках и доступности, а защита касалась только собственной инфраструктуры, то сегодня ситуация коренным образом изменилась. На рынке появились новые игроки – ASP (Application Service Provider), NSP (Network Service Provider) и т.д. Бизнес все больше становится электронным, а заказчики начинают зависеть от доступа в сеть. Меняется и структура атак. Если раньше их целью являлись пользовательские компьютеры, то сегодня и инфраструктура оператора становится частой мишенью. При этом если раньше атаки на заказчиков никак не влияли на работоспособность сети провайдера сетевых услуг, то современные хакерские технологии давно перестали быть уделом только атакуемых ресурсов. Черви, сканирующие сеть в поисках своей жертвы, заполняют каналы связи бесполезным трафиком, который занимает столь дорогую пропускную способность, лишая операторов связи и их заказчиков возможности на полную мощность задействовать свои ресурсы.

Сегодня хакерским нападениям и вирусным эпидемиям подвластны даже самые именитые операторы связи. Уже известно множество случаев взломов или иных инцидентов с безопасностью известных провайдеров. Из западных имен можно назвать America Online, Akamai, Cable&Wireless, WorldCom, Swissonline, Earthlink, Qualcomm и т.д. Из работающих на территории России и СНГ – Укртелеком, МТУ-Интел, Арминко, Демос-Интернет и т.п. И такие атаки не ограничиваются одними простоями или временным снижением пропускной способности операторской сети. Отказ в доступе к сетевым ресурсам вынуждает заказчиков подавать в суд на своих операторов связи за нарушение договорных обязательств, упущенную выгоду и т.д. Но исками дело не ограничивается. Операторы вполне могут разделить участь английского сервис-провайдера CloudNine, который в 2002 году был вынужден объявить о своем банкротстве, наступившем в результате атаки «отказ в обслуживании» (Denial of Service, DoS) и невозможности дальнейшего ведения 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
Обмен сообщениями	1000

Есть и другая, такая же говорящая, статистика опасности атак на доступность сети – 93% компаний, лишившихся доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно. 43% компаний, столкнувшихся со сбоями в своей сети, вынуждены были немедленно покинуть бизнес. Еще 29% закрываются в течение ближайших 2-х лет.

Учитывая все вышесказанное, перед операторами остро встает вопрос обеспечения безопасности. И вопрос в том, как решить эту непростую задачу? При этом нельзя забывать о том, что обеспечивая безопасность своей инфраструктуры, оператор связи должен заботиться и о защите сетей заказчиков, что позволяет не только обезопасить их от возможных атак из сетей других операторов связи, но и блокировать атаки, исходящие от самих заказчиков. Также необходимо учитывать, что при современном развитии телекоммуникаций безопасность и устойчивость одного оператора связи является залогом эффективного ведения бизнеса и для других операторов, т.к. в случае нарушения функционирования сети сервис-провайдера это прямым образом сказывается и на бизнесе всех его «соседей». Поэтому единственно верная стратегия обеспечения информационной безопасности – защитить всех участников информационного обмена.

ШЕСТИФАЗНАЯ МЕТОДОЛОГИЯ ЗАЩИТЫ ОПЕРАТОРОВ СВЯЗИ

Компания Cisco Systems совместно с рядом операторов связи разработала 6-шаговую методологию построения инфраструктуры информационной безопасности для сервис-провайдеров, которая включает в себя следующие этапы:

- Подготовка
- Идентификация
- Классификация
- Отслеживание
- Реагирование
- Расследование инцидентов

Подготовка

Попытка отразить атаку без соответствующей подготовки будет безуспешной и похожа на сдачу экзамена без предварительного обучения. Безопасность оператора связи начинается не с применения технических средств и механизмов – она начинается гораздо раньше – с понимания проблемы и формирования соответствующей команды, на плечи которой и ляжет основной груз забот по обеспечению устойчивости и защищенности своей сети.

У многих операторов есть центр сетевого управления (Network Operations Center, NOC), но... в нем, как правило, отсутствуют регламентирующие документы и руководства по защите, нет инструментов, нет или катастрофически не хватает квалифицированных специалистов по защите информации и т.д. Однако при современном уровне развития вредоносных программ, необходимо создавать у оператора центр управления безопасностью (Security Operations Center, SOC), на который и будет возложено:

- оперативные вопросы реагирования на атаки и расследования инцидентов, но и
- взаимодействие с производителями используемого сетевого оборудования,
- соседними операторами,
- разработка организационно-распорядительных документов по вопросам обеспечения защищенности и устойчивости деятельности оператора связи
- контроль их исполнения всех защитных мероприятий и т.д.

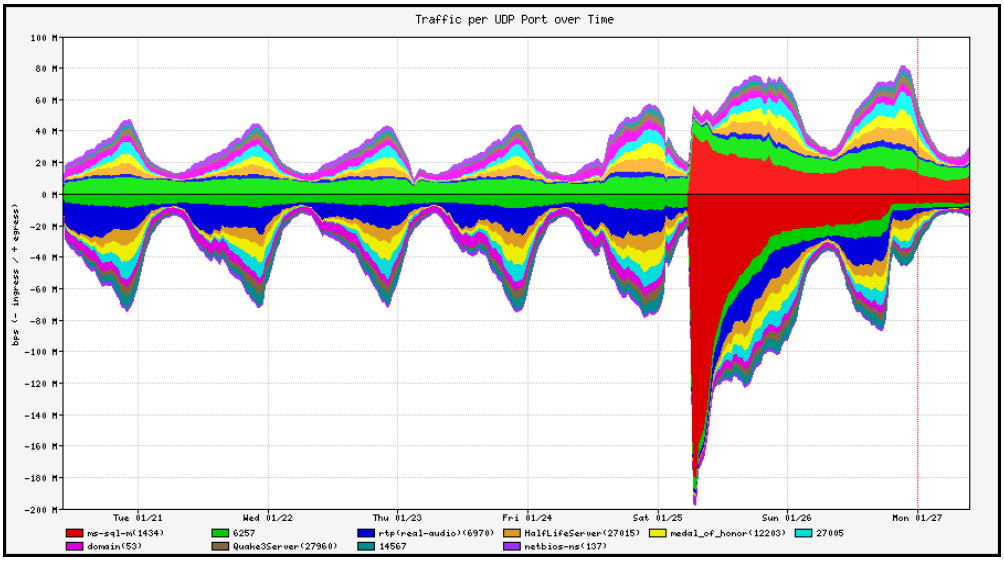
Но каким бы мощным не был SOC, он не может контролировать все и вся – ему необходима помощь других аналогичных объединений специалистов. Например, группы североамериканских операторов связи (http://www.nanog.org/) или инженеров, входящих в закрытый список рассылки NSP-SEC (http://puck.nether.net/mailman/listinfo/nsp-security).

Идентификация и классификация

Не нужно ждать, пока об атаке вам сообщит ваш пользователь – упредите его, а еще лучше защитите его, недопустив атаку до его ресурсов. Для этого и используются процессы идентификации и классификации атак, которые зачастую происходят параллельно. Для решения этой задачи компания Cisco использует множество различных механизмов, каждый из которых используется в зависимости от типа атак:

- Контроль полосы пропускания
- Анализ NetFlow
- Фильтры с ведением учета
- Ловушки
- Сетевые системы обнаружения атак
- Системы обнаружения аномалий и DoS-атак

Наиболее перспективным для операторов связи признаны системы обнаружения аномалий, которые позволяют обнаруживать основную угрозу для операторских сетей – атаки «отказ в обслуживании», выводящие из строя сетевое оборудование или заполняющие сеть не несущими полезной нагрузки пакетами. При этом, зачастую, данные атаки не могут быть описаны никаким сигнатурами и они ничем не отличаются от обычного разрешенного трафика, а, следовательно, их невозможно обнаружить и блокировать такими средствами защиты, как традиционные системы обнаружения атак (intrusion detection systems), межсетевые экраны, списки контроля доступа и т.п. Один из эффективных методов идентификации и классификации – анализ данных NetFlow, экспортируемых из маршрутизаторов в системы обнаружения аномалий. Другой метод – анализ всего проходящего трафика в поисках несанкционированной активности. Такие системы как Arbor PeakFlow, Arbor DoS, Cisco Traffic Anomaly Detector или Cisco Guard обнаруживают такую активность в несколько мгновений, что позволяет блокировать атаки в самом начале их развития. И это тогда, когда многие другие компании только анализируют трафик и пытаются идентифицировать вредоносную активность.



Отслеживание

Когда сервис-провайдер обнаруживает атаку, следующий логический шаг – определить источник несанкционированной активности с целью применения вариантов реагирования или информирования владельцев других сетей, если атака «принадлежит» не вам. Источник атаки может быть двух типов – реальный и подмененный. С реальными адресами применять специальные методы отслеживания не требуется, т.к. вы можете легко идентифицировать узел, инициировавший атаку с помощью WHOIS, traceroute или DNS. Однако данные методы требуют времени и не применимы в случае с подменой адресов. В этом случае может использоваться метод Backscatter Traceback, реализованный в оборудовании компании Cisco и позволяющий отследить злоумышленника, используя протоколы маршрутизации. Помимо Backscatter Traceback существуют и другие методы идентификации источника атаки, которые реализованы в маршрутизаторах Cisco 7200, 7600, 10000, 12000 (GSR) и CRS-1. К ним относятся IP Source Tracker, а также трассировка с помощью NetFlow и ACL. Отслеживание и сбор данных об атаке, реализуемые с помощью указанных механизмов, могут использоваться для:

- Проведения расследования и сбора доказательств несанкционированной деятельности для судебного преследования
- Предотвращения повторных атак
- Разбора спорных вопросов с тарификацией
- Анализа последствий после атаки.

Реагирование

Когда вредоносная активность обнаружена и классифицирована, а ее источник идентифицирован, приходит время реагирования, которое может заключаться в отражении атаки, сигнализации администратору безопасности, а также выполнению других необходимых действий.

Самый первый, самый важный и самый простой метод защиты – фильтрация трафика. При правильном использовании он позволяет отсеять очень многое из того, что не должно попадать в сеть оператора или покидать ее пределы. Кроме того, надо помнить, что эффективная фильтрация в сети оператора позволяет защитить весь Интернет в целом, т.к. Интернет – это и есть по сути объединение операторов. Следуя этому принципу, мы можем локализовать любую угрозу в рамках сети одного клиента, защищая тем самым всех остальных.

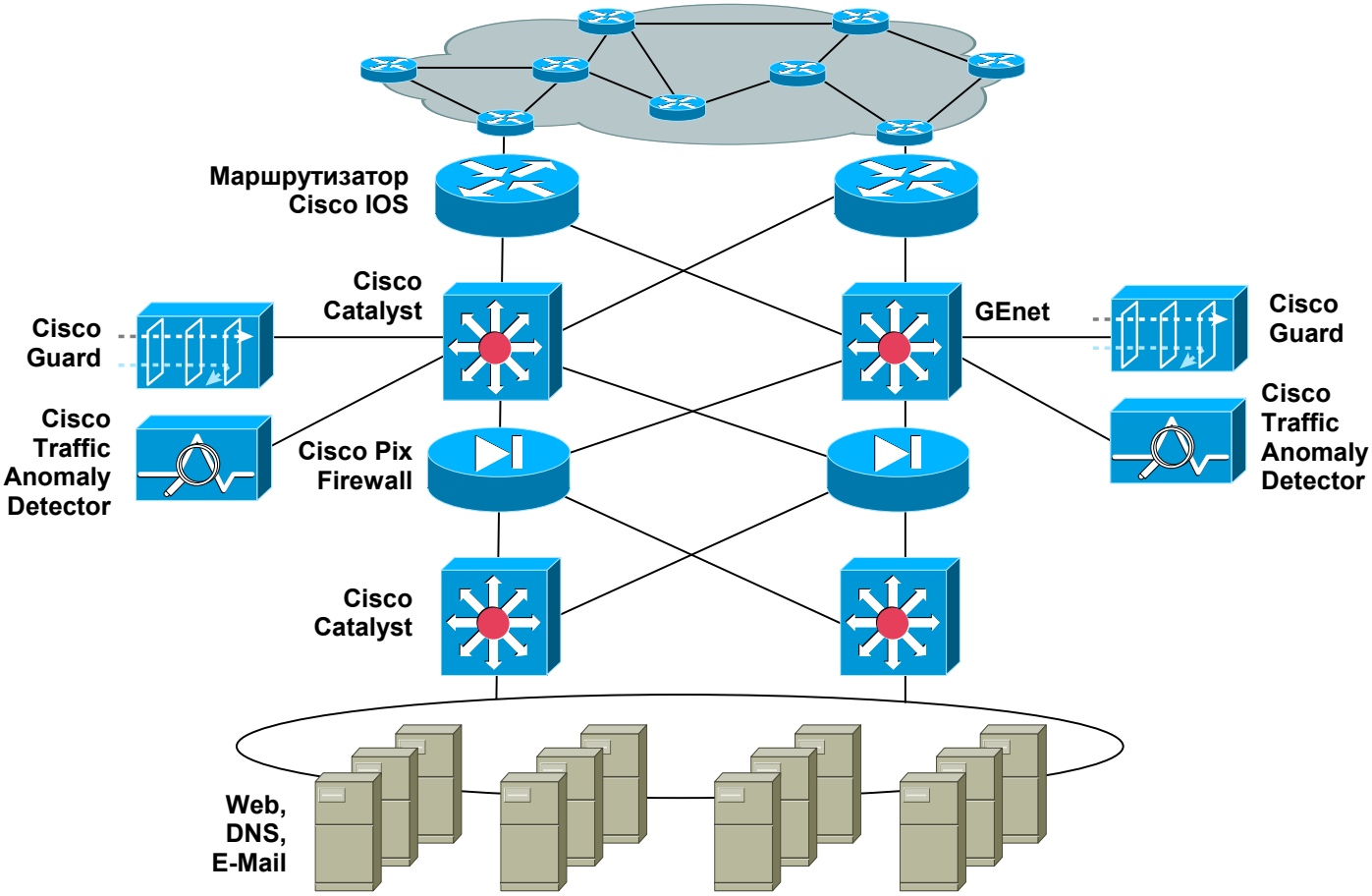
Какие методы существуют для реализации фильтрации в оборудовании Cisco Systems? Самый первый из них – списки контроля доступа (access control list, ACL), которые позволяют фильтровать исходящий и входящий трафик на основе IP-адресов получателя и отправителя, портов получателя и отправителя, а также типа сервиса/протокола.

Особенность работы списков контроля доступа заключается в последовательной проверке каждого пакета на соответствие правилу в ACL. А раз так, то в какой-то момент может наступить ситуация, когда большая часть ресурсов маршрутизатора вместо выполнения своего основной задачи будет тратиться на фильтрацию. Поэтому надо учитывать этот момент при выборе данного метода фильтрации трафика и заранее учесть и скорость обработки пакетов и, как следствие, время задержки. Разумеется, технологии тоже не стоят на месте и сегодня существуют различные методы повышения быстродействия списков контроля доступа, например, TurboACL, выделенные для фильтрации микропроцессоры ASIC/TCAM и т.п.

Следующим вариантом фильтрации является фильтрация в «черную дыру» (blackhole), которая реализуется путем передачи ненужного трафика на псевдоинтерфейс Null0, который всегда включен, но никогда не пересылает и не принимает трафик. Следовательно, передача на Null0 трафика приводит к его сбросу, а процессор маршрутизатора при этом не перегружается, как в случае со списками контроля доступа. Однако и у данного метода есть свои ограничения. В отличие от ACL, позволяющего фильтровать трафик на основе конкретных протоколов и сервисов, метод «черной дыры» не обеспечивает такой же гибкости – он позволяет отсеивать весь трафик, поступающий на конкретный адрес или подсеть.

По статистике до 95% всех атак «отказ в обслуживании» совершаются с подменой адреса. При этом фальсифицированные адреса могут принадлежать клиентам, а, следовательно, списки контроля доступа или метод фильтрации в «черную дыру» будет малоэффективен. В такой ситуации возможно применение т.н. проверки по обратному пути (Unicast Reverse Path Forwarding, uRPF), которая позволяет проверять каждый пакет на предмет того, что адрес его источника доступен по тому же интерфейсу. Если проверка завершается неудачей, то такой пакет отбрасывается. Этот метод менее «прожорлив» к ресурсам процессора по сравнению с ACL и более легок в настройке и поддержке – на маршрутизаторе достаточно ввести всего одну команду, которая позволит автоматически отсеивать все пакеты с поддельными адресами.

Отдельным классом защитных механизмов можно выделить отражение атак «отказ в обслуживании», которые все чаще и чаще нарушают работоспособность сетей операторов связи по всему миру. По статистике каждые 5 минут в мире происходит 2 DoS-атаки, и это значение будет ухудшаться, что связано с существенным облегчением реализации этого типа несанкционированной активности. Следовательно, оператор связи должен иметь возможность защищать себя и своих клиентов от такого рода напасти. Одним из защитных механизмов, реализованных в оборудовании компании Cisco Systems, является ограничение полосы пропускания с помощью Committed Access Rate (CAR), который позволяет ограничивать определенные виды трафика для заданных адресов источников или получателей. Основное преимущество CAR заключается в том, что он может работать с пакетами по мере того как они поступают на интерфейс маршрутизатора – сбрасывая или ограничивая поток DoS-атаки еще до того как он начнет обрабатываться.



Другим средством защиты от DoS и DDoS-атак является применение специализированного устройства Cisco Guard, который 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). Уникальная архитектура Multiverification Process (MVP) позволяет обеспечить очень высокую скорость обработки трафика и обнаружения DoS-атак без снижения производительности защищаемой сети.

Расследование инцидента

Финальной фазой является расследование инцидента, в результате которого определяются наиболее эффективные защитные меры, анализируются сделанные промахи, оповещаются другие операторы связи и соответствующие правоохранительные органы, отвечающие за поимку преступников, совершивших атаку, и т.д. На этом этапе анализируются захваченные в результаты анализа трафика пакеты, журналы регистрации сетевого оборудования и т.д. Все это делается с целью составления целостной картины о состоянии защищенности сети оператора связи и эффективности реализованных защитных мер.

ПОДХОД КОМПАНИИ CISCO

Реализация данной шестифазной методологии была бы невозможной без соответствующих технических решений, предлагаемых компанией Cisco Systems своим заказчикам и которые можно разделить на 3 основные категории:

- Защита от вторжений (Threat Defense). Наиболее эффективная защита бизнес-ресурсов от злоумышленников и вредоносных программ достигается только в случае эшелонированной обороны, распределенной по всей сети, а не сосредоточенной в одной точке. Стратегия Threat Defense System позволяет защитить инфраструктуру оператора связи за счет интеграции различных защитных механизмов в маршрутизаторы и коммутаторы, а также предлагает выделенные защитные устройства для разграничения доступа, отражения атак и контроля Web-контента, а также позволяет защищать конечные устройства, такие как сервера и рабочие станции от широкого спектра угроз.
- Защищенное взаимодействие (Secure Connectivity). Рост точек присутствия и необходимости удаленного управления ими требуют обеспечения защиты данных передаваемых по открытым каналам связи. Сохранение конфиденциальности и целостности данных являются обязательным элементом современных приложений, и оказание подобной услуги оператором связи позволяет ему расширить свой бизнес. Это может быть достигнуто за счет стратегии Cisco Secure Connectivity System, которая, используя механизмы шифрования и аутентификации, одинаково эффективно защищает данные, голос и видео, передаваемые как по проводным, так и по беспроводным соединениям. Составной частью Secure Connectivity System являются такие технологии, как IPSec, SSL, SSH, GRE и MPLS.
- Идентификация и управление доверием (Identity & Trust Management System). Прежде чем заказчик, приложение или устройство получит доступ к необходимым ресурсам, он должен быть опознан средствами защиты. Именно эту задачу на сетевом уровне решают технологии и средства компании Cisco Systems – Network Admission Control (NAC), 802.1x, Cisco CNS Access Registrar и т.д.

ПОЧЕМУ ИМЕННО CISCO?

Компания Cisco Systems, признанный лидер в области сетевых решений, предлагает также широкий выбор продуктов в области обеспечения информационной безопасности – от межсетевых экранов и систем предотвращения атак до средств построения VPN и систем персональной защиты серверов и рабочих станций. При этом в каждой из этих областей компания Cisco Systems достигла лидирующих позиций и занимает первые места не только на мировом рынке, но также и в России и странах СНГ.

Такое положение было бы невозможно без исследований и разработок, на которые ежегодно тратится свыше 300 миллионов долларов – больше, чем зарабатывают в год многие другие игроки рынка информационной безопасности.

Учитывая, что компания Cisco Systems работает во многих странах мира, мы учитываем специфику каждого государства. В России наши решения проходят сертификацию в соответствующих регулирующих органах, например, в Федеральной службе по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России). В частности, решения компании Cisco имеют свыше 120 сертификатов по требованиям информационной безопасности, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

Работая на территории такой страны, как Россия, невозможно не учитывать различные часовые пояса и большую территорию, на которой могут располагаться сети наших заказчиков. Несмотря на это, все они могут быть уверены в получении своевременной помощи. Это достигается за счет удаленной круглосуточной технической поддержки и гарантии замены вышедшего из строя оборудования со сроком замены до 4-х часов (в Москве и Санкт-Петербурге) и с отгрузкой в день авторизации замены (для остальных регионов).

ЗАКЛЮЧЕНИЕ

Сегодня инфокоммуникации стали центром развития новых технологий, в корне меняющих методы взаимодействия и ведения бизнеса в среде сервис-провайдеров. Уверенность в том, что бизнес-процессы и ресурсы оператора связи защищены от посягательств злоумышленников и воздействия вредоносных программ является критическим фактором в современном мире. Компания Cisco Systems, в отличии от других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков операторской сети и их заказчиков, а комплексное решение, интегрируемое в инфраструктуру для обеспечения информационной безопасности бизнеса на всех уровнях.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная на защиту бизнес-процессов в условиях растущей угрозы со стороны вредоносных программ и злоумышленников, воздействующих на бизнес-процессы оператора связи изнутри и извне. Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от персонального компьютера до сетевого оборудования, участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса. Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных узлов, и реконфигурации сетевых устройств с целью предотвращения повторных атак.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Решения Cisco Systems по информационной безопасности

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

Решения Cisco Systems по безопасности операторов связи

ftp://ftp-eng.cisco.com/cons/isp/

Информация о Cisco NetFlow

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

Информация о Cisco Catalyst Network Analysis Module

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

Отражение червей с помощью оборудования Cisco Systems

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

Cisco Guard

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

Backscatter Traceback

http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac253/packet_service_provider_solution0900aecd800e015e.html

Объединение специалистов по защите операторов связи NSP-SEC

http://puck.nether.net/mailman/listinfo/nsp-security

Лучшее руководство по защите Интернет-операторов

http://www.getitmn.com/bootcampflash/launch.html

Информационный центр NetWorm

http://www.networm.org

Информация от Cymru

http://www.cymru.com

Центр мониторинга Интернет

http://www.renesys.com

Центр ресурсов для Интернет-провайдеров

http://www.ispbook.com

Рекомендации объединения североамериканских операторов связи

http://www.nanog.org/ispsecurity.html

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