РЕШЕНИЯ CISCO ПО ОТРАЖЕНИЮ АТАК НА УРОВНЕ СЕТИ

Решения Cisco по защите от атак специально разработаны для эффективной защиты ваших данных и информационной инфраструктуры. Рост сложности хакерского инструментария и расширения спектра угроз безопасности ведет к необходимости применения различных технологий обнаружения и предотвращения вторжений, обеспечивающих эшелонированную оборону внешних и внутренних ресурсов компании любого масштаба – от домашних пользователей и надомных работников и заканчивая крупными компаниями и операторами связи.

Эффективность решений по отражению атак достигается за счет 4-х ключевых элементов:

- **Обнаружение и предотвращение многовекторных атак**. Программное обеспечение Cisco IDS/IPS является первым шагом в достижении всесторонней защиты от несанкционированной и вредоносной активности. Используемые методы обнаружения ориентированы на определение широкого спектра угроз на всех уровнях инфраструктуры, начиная с канального и заканчивая прикладным. К этим угрозам можно отнести сканирование, «отказ в обслуживании», переполнение буфера, троянцы, черви, атаки на приложения, нападения на инфраструктуру IP-телефонии и других.
- **Интеллектуальный анализ угроз**. Технологии Cisco Threat Response, Threat Risk Rating и Meta Event Generator, интегрированные в решения Cisco и не требующие дополнительной оплаты, помогают не только существенно снизить число ложных срабатываний, но и позволяют администраторам реагировать только на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам корпоративной сети. При этом все малозначительные или неприменимые в данный момент сигналы тревоги будут отсеиваться, чтобы не отвлекать администратора безопасности от более важных событий безопасности.
- **Удобное управление**. Web-ориентированная консоль управления облегчает настройку сенсоров предотвращения атак, а также контроль их состояния и мониторинг событий безопасности (включая функции их анализа и корреляции).
- **Гибкость внедрения**. Широкий выбор моделей сенсоров (от выделенных устройств до специальных модулей в коммутаторы и маршрутизаторы) позволяет эффективно защитить различные участки корпоративной сети, включая центры обработки данных, магистрали и внутренние сегменты корпоративной сети.

Все 4 элемента комбинируются, чтобы достичь безопасной, эффективной и всесторонней защиты от атак.

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ МНОГОВЕКТОРНЫХ АТАК

Cisco IDS/IPS является центральным компонентом решения Cisco Systems по отражению атак. Наряду с традиционными механизмами, позволяющими идентифицировать вредоносную активность по шаблонам и сигнатурам, в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки.

Множество методов обнаружения

Компания Cisco, обладая более чем семилетним опытом в области защиты от атак, улучшила и реализовала множество различных механизмов обнаружения, охватывающих большое количество атак и злоупотреблений. Для каждого типа вредоносных программ и действий применяются свои собственные методы – контроль сигнатур, сравнение с шаблоном, контроль состояния соединения, контроль аномалий в сетевом трафике, обнаружение отклонений от нормального поведения сетевых

приложений, эвристический анализ, контроль соответствия RFC и другие. Отличительной особенностью Cisco IDS/IPS является отражение атак ниже сетевого уровня, а также защита от методов, используемых злоумышленниками для обхода систем обнаружения атак (фрагментация атак, перекрытие сегментов, повторная передача и нарушение порядка фрагментов и т.п.).

Расширенная поддержка протоколов

Cisco IDS/IPS позволяет обнаруживать атаки во всех основных протоколах стека TCP/IP, включая, но не ограничиваясь, IP, ICMP, TCP и UDP. Помимо протоколов канального, сетевого и транспортного уровней, Cisco IDS/IPS может контролировать и большое количество протоколов прикладного уровня – HTTP, FTP, SMTP, DNS, RPC, NetBIOS, NNTP, Telnet и т.п.

Технология анализа протоколов Deep Packet Inspection позволяет «взглянуть вглубь» многих протоколов и обнаруживать нарушения политики безопасности даже в разрешенных типах трафика. С помощью данной технологии Cisco IDS/IPS может обнаруживать скрытые каналы утечки информации (например, ICQ и Интернет-пейджеры) в Web-трафике.

Уникальной возможностью Cisco IDS/IPS является:

- обнаружение атак в трафике, инкапсулированном в MPLS и GRE-туннели,
- возможность контроля VoIP-протоколов и обнаружения в них нападений на голосовые приложения, шлюзы и IP-телефоны,
- а также распознавание атак в протоколе IP версии 6 (IPv6).

Большое число типов обнаруживаемых атак

В Cisco IDS/IPS разработаны специальные микромодули Cisco Threat Analysis Micro Engine (T.A.M.E.), оптимизированные для обнаружения различных типов нападений:

- Атаки на приложения – попытки воспользоваться слабыми местами в программном обеспечении, таком как, например, ERP- и CRM-системы, Web-сервера и почтовые системы и т.д.
- DoS-атаки – попытки нарушить нормальную работу ресурсов корпоративной сети путем посылки большого объема паразитного трафика или путем генерации некорректно сформированных пакетов.
- Черви и троянцы – вредоносные программы, заражающие узлы корпоративной сети и распространяющиеся по ней.
- Сетевая разведка – попытки идентифицировать узлы и приложения в сети с целью определения наиболее уязвимых точек для последующих атак.
- Утечка конфиденциальной информации – нарушение политики безопасности, выражающееся в виде передачи критичной для бизнеса компании за пределы периметра корпоративной сети с помощью ICQ, электронной почты и т.п.
- Шпионское и рекламное ПО – вредоносные программы, незаметно устанавливаемые на компьютеры пользователей, и переадресующие все Web-запросы на рекламные сайты, а также крадущие и отсылающие конфиденциальную информацию на заранее определенные адреса.
- Скрытые каналы утечки информации через разрешенный на межсетевом экране 80-ый порт, отвечающий за обработку HTTP-трафика. Таким образом обнаруживается и блокируется работа пиринговых сетей (Kazaa, eMule, eDonkey и т.д.) и Интернет-пейджеров (ICQ и т.п.).
- Нарушения политики безопасности работы с приложениями. Cisco IDS/IPS может разрешить выполнение тех или иных команд, а также типов передаваемой информации в рамках определенных протоколов. Например, Cisco IDS/IPS может разрешить использование метода HTTP GET, запретив метод HTTP POST, или фильтровать трафик по типам MIME.

Предотвращение атак

Сенсоры Cisco IDS/IPS могут быть установлены в одном из двух режимов:

- классическая система обнаружения атак, имеющая дело с копией сетевого трафика
- система предотвращения атак, в которой весь трафик пропускается через нее, за счет чего и достигается эффективное блокирование атаки и недопущение ее до своей цели.

При этом сенсоры Cisco IDS/IPS могут функционировать параллельно в двух режимах, что позволяет в одном устройстве одновременно реализовать и задачу обнаружения атак (например, в демилитаризованной зоне или внутренней коммутируемой сети), и задачу их предотвращения (например, на периметре).

В обоих вариантах Cisco IDS/IPS предлагает широкий выбор вариантов реагирования, обеспечивающих высокий уровень защиты корпоративных ресурсов от различных угроз. К ним можно отнести:

- блокирование вредоносного пакета или соединения, а также злоумышленника (в режиме предотвращения),
- разрыв соединения (в режиме обнаружения),
- реконфигурация МСЭ или маршрутизатора с целью блокирования опасного соединения или узла-нарушителя (в режиме обнаружения).

Помимо реагирования на обнаруженные атаки, Cisco IDS/IPS предлагает для каждого события безопасности в отдельности и различные варианты уведомления администратора безопасности, начиная от посылки сигнала тревоги на консоль и генерации SNMP Trap и заканчивая регистрацией всех сетевых пакетов, в которых обнаружено нападение с целью их последующего анализа.

Гибкость настройки

Так как сенсоры могут быть установлены на различных участках корпоративной сети с различными требованиями по безопасности, то Cisco IDS/IPS позволяет создавать и модифицировать политики в зависимости от своего места расположения. При этом система Cisco IDS/IPS может быть настроена на специфичное сетевое окружение любой компании, что достигается за счет возможности изменения любого контролируемого параметра – адреса и порты источника и получателя, TCP-флаги и IP-опции, пороговые значения и т.п.

Автоматизированное обновление

Механизм Active Update, реализованный в Cisco IDS/IPS, позволяет автоматизировать процесс распределения обновлений сигнатур и программного обеспечения. При этом обновление осуществляется по защищенному от несанкционированного доступа каналу, а целостность самих обновлений контролируется криптографическими механизмами. Эта возможность позволяет существенно снизить издержки не только на развертывание системы отражения атак, но и на ее поддержку и эксплуатацию.

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ УГРОЗ

В Cisco IDS/IPS реализован ряд уникальных технологий, не требующих дополнительной оплаты, и существенно повышающих эффективность и точность обнаружения несанкционированной активности. Это технологии Cisco Threat Response, Threat Risk Rating и Meta Event Generator.

Cisco Threat Response

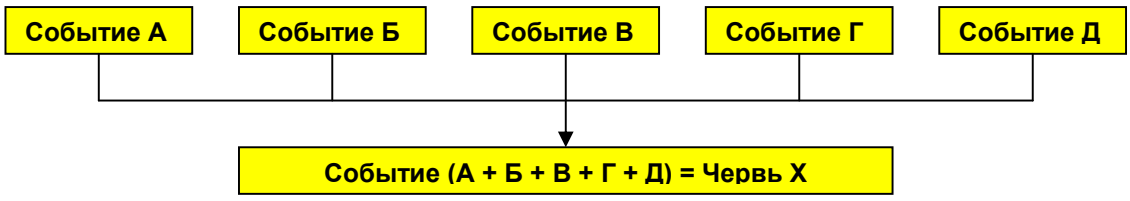
Cisco Threat Response (CTR) – технология, встроенная в каждый сенсор и обеспечивающая анализ узлов с целью определения их уязвимости и подверженности атаке. Только зная это, можно отсеивать серьезные атаки, несущие угрозу ресурсам корпоративной сети, от не представляющих никакой опасности. CTR обеспечивает снижение числа ложных срабатываний за счет прохождения 2-х этапов (последний с помощью CiscoWorks VPN Security Management Solution):

- Пассивное сканирование узлов сети с целью определения подверженности атаке. При этом сканирование защищаемого сегмента осуществляется в реальном режиме времени. Если атака, применимая только к системе Windows, направлена на Linux-узел, то она автоматически помечается как неуспешная.
- Второй этап заключается в загрузке и анализе журналов регистрации приложений и операционной системы, позволяющих точно идентифицировать успешность/неуспешность атаки.

Технология Cisco Threat Response работает 24 часа в сутки 7 дней в неделю, при этом не требуя установки на контролируемых узлах специальных агентов, осуществляющих анализ защищенности.

Meta Event Generator

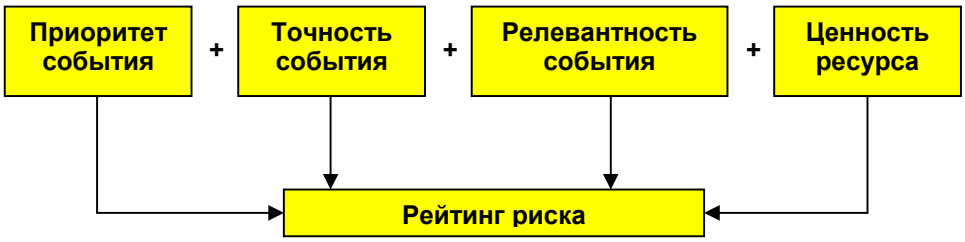
С целью снижения числа, а также улучшения понятности сообщений, отображаемых на консоли системы обнаружения атак, в каждом сенсоре Cisco IDS/IPS реализован встроенный механизм корреляции Meta Event Generator, который позволяет автоматически объединять несколько связанных сигналов тревоги в высокоуровневое мета-событие безопасности. Например, 5 событий “cmd.exe Access”, “IIS CGI Decode”, “IIS Unicode Attack”, “Dot Dot Execute” и “Dot Dot Crash”, произошедших в течение 3-х секунд, отображаются на консоли как всего одно событие “Червь NIMDA”. При этом последовательность событий, их число и временной интервал между ними настраиваются администратором, что позволяет учесть практически любые типы несанкционированной активности.



Threat Risk Rating

Каждая сигнатура, заложенная в базу Cisco IDS/IPS, обладает таким настраиваемым администратором параметром как «точность», который определяет, насколько точно данная сигнатура описывает обнаруживаемую несанкционированную активность. Также администратор может указать для любого из защищаемых узлов его ценность с точки зрения бизнеса компании, что позволяет разделить все сетевые ресурсы на 3 категории – большой ценности (например, SCADA-система или Интернет-банк), средней ценности (например, терминалы операционистов банка) и низкой ценности (например, компьютер секретаря или принтер).

Объединяя 4 показателя – приоритет атаки, ее релевантность, определяемая с помощью CTR, точность сигнатуры атаки и стоимость атакуемого ресурса, мы приходим к понятию рейтинг риска, который позволяет не только учесть опасность любой из идентифицируемых атак, но и оценить их вредоносное воздействие на бизнес-ресурсы.



Эта технология снижает нагрузку на администратора безопасности, которому больше не требуется вручную анализировать десятки и сотни атакуемых узлов с целью определения их подверженности несанкционированным действиям. Кроме того, рейтинг риска позволяет учесть ценность различных узлов корпоративной сети для бизнеса компании и реагировать в первую очередь на атаки, направленные на наиболее критичные ресурсы (например, на ERP- или платежную систему). С целью облегчения труда администратора безопасности в Cisco IDS/IPS реализована возможность автоматического выбора вариантов реагирования в зависимости от рейтинга риска обнаруженной угрозы.

УДОБНОЕ УПРАВЛЕНИЕ

Cisco IDS/IPS обеспечивает не только эффективную защиту корпоративных ресурсов от различных угроз, но и интуитивно понятное управление своими настройками, облегчающими внедрение, настройку и эксплуатацию десятков и сотен сенсоров. Настройка сенсоров и отображение сигналов тревоги от них возможно двумя путями – с помощью:

- Встроенной в каждый сенсор консолью управления IDS Device Manager
- Системой централизованного управления CiscoWorks VPN Security Managemenr Solution (CiscoWorks VMS).

Управление и мониторинг с помощью IDS Device Manager осуществляется с любого компьютера с установленным Web-браузером по защищенному каналу SSL. Помимо графического консоли, сенсоры Cisco IDS/IPS могут управляться и с помощью интерфейса командной строки, доступ к которому возможен с помощью защищенного протокола SSH.

Управление большим количеством сенсоров, наряду с другими средствами защиты компании Cisco Systems – межсетевыми экранами Cisco Pix, персональными системами защиты Cisco Security Agent, средствами построения VPN и т.д., осуществляется при помощи CiscoWorks VMS.

Cisco IDS/IPS – первая система на рынке, поддерживающая протокол Security Device Event Exchange (SDEE), разработанный компанией Cisco для консорциума разработчиков средств обнаружения атак ICSA. Данный стандарт позволяет передавать сигналы тревоги на системы мониторинга и управления безопасностью третьих фирм.

ГИБКОСТЬ ВНЕДРЕНИЯ

Компания Cisco Systems предлагает широкий выбор различных устройств по отражению атак, давая возможность заказчикам выбрать то, что больше всего подходит под их требования. Вы можете выбрать программное или аппаратное решение, отдельное устройство или плату, интегрированную в коммутатор или маршрутизатор, решение для контроля низко- или высокоскоростного сетевого сегмента. При этом внедрение данных решений не только не мешает эффективному ведению бизнеса, но и обеспечивает его непрерывность.

Различные типы устройств

Cisco предлагает следующие типы решений по отражению атак:

- Сенсоры Cisco IPS 42xx – выделенные устройства, выпускаемые в виде 4-х разных моделей (с возможностью одновременного контроля до 4-х сегментов без дополнительной оплаты):
    - Cisco IDS 4215 – 80 Мбит/сек
    - Cisco IPS 4240 – 250 Мбит/сек
    - Cisco IPS 4255 – 600 Мбит/сек
    - Cisco IDS 4250-XL – 1 Гбит/сек

- Модуль Cisco IDSM-2 для коммутатора Cisco Catalyst 6500 – плата, инсталлируемая в шасси коммутатора, и эффективно контролирующая внутреннюю сеть без необходимости изменения ее топологии.
- Модуль Cisco IDS Network Module для маршрутизаторов Cisco 2600, 2800, 3600, 3700 и 3800 – платы, инсталлируемые в маршрутизаторы с целью эффективной защиты периметра в удаленных филиалах. Модуль NM-IDS может функционировать только в режим обнаружения.
- Модуль Cisco Advanced Inspection and Prevention Security Services Module для многофункциональных устройств ASA 5500 Series – платы, обеспечивающие все функции Cisco IDS/IPS в интегрированных устройствах Cisco ASA 5500.
- Сенсоры Cisco IOS IPS – программное обеспечение, интегрированное в операционную систему IOS каждого маршрутизатора и обеспечивающее защиту от атак начального уровня.
- Сенсоры в межсетевом экране – программное обеспечение, интегрированное в операционную систему PixOS каждого межсетевого экрана Cisco Pix с целью расширения его возможностей по контролю трафика.

Отказоустойчивость

Отказоустойчивость сети, защищаемой сенсорами IDS/IPS, может быть достигнута за счет применения различных методов:

- Балансировка нагрузки между несколькими защитными устройствами при помощи механизма Cisco EtherChannel
- Контроль состояния сетевого соединения при помощи протокола Hot Standby Routing Protocol (HSRP)
- Встроенный в каждый сенсор Cisco IDS/IPS механизм bypass, который позволяет в автоматическом или ручном режиме перенаправлять трафик в обход вышедшего из строя сенсора.

СЕРТИФИКАЦИЯ

Компания Cisco Systems приняла на себя обязательства по сертификации своих решений в соответствие с требованиями по информационной безопасности, принятыми в разных странах. В России компания Cisco Systems сертифицировала сенсоры системы обнаружения атак Cisco IDS 4200, а также модуль Cisco IDSM-2 для коммутатора Cisco Catalyst 6500 на соответствие руководящим документам и техническим условиям Федеральной службы по техническому и экспортному контролю (ФСТЭК).

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Cisco IPS 4200

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

Cisco ASA 5500

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

Cisco IOS IPS

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

Решения Cisco Systems по предотвращению атак

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

Решения Cisco Systems по отражению и локализации вирусных эпидемий

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

Cisco Catalyst 6500 IDS Module (IDSM-2)

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html

Cisco IDS Network Module for Cisco 2600, 3600 и 3700

http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008017dc22.html

CiscoWorks Security Information Management Solution

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

Решения Cisco Systems по информационной безопасности

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

IPS Alert Center

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

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