Правило-ориентированная безопасность

Обзор функциональных возможностей Cisco Security Agent – представителя одного из наиболее быстро развивающихся секторов продуктов обеспечения информационной безопасности серверов/ПК на основе правил и политик, постепенно становящихся стандартным компонентом корпоративной ИТ-инфраструктуры.

Время изменяемой безопасности

Понедельник. Утро. Большая компания. Все системные администраторы, включая стажеров, ходят по сотрудникам. Одни спрашивают, как настроить Safari, другие пользуются The Bat вместо Outlook, третьи "принесли" вирусы из домашних сетей. Да еще в сети появился Slammer.

Знакомая ситуация? Но, конечно, приведенная зарисовка является преувеличением.

Однако чем больше становится компания, тем больше разрастается ИТ-сеть и тем сложнее ею управлять. Иногда наступает момент, когда сеть, вместо того чтобы помогать зарабатывать деньги, мешает это делать.

В настоящий момент вопросы информационной безопасности сети выходят на первые места в перечне проблем крупных предприятий. Существует большое количество продуктов, систем, архитектур для обеспечения информационной безопасности (ИБ). В данной статье мы дадим описание одного из таких механизмов – Cisco Security Agent (CSA) из общей архитектуры Cisco Safe.

Почему мы выбрали именно эту архитектуру?

Сегодня достаточно большое количество корпоративных сетей построено на базе оборудования Cisco Systems. Помимо непосредственно производства сетевого оборудования, компания значительное внимание уделяет безопасности сети в целом. Компанией Cisco разработана архитектура, которая обеспечивает высокий уровень сетевой безопасности. Описание Cisco Safe выходит за рамки данной статьи, поэтому мы остановимся лишь на особенностях, напрямую связанных с обеспечением безопасности. А именно:

- модульность – каждый модуль системы работает независимо от других модулей;
- эшелонированность – архитектура обеспечивает защиту на всех ключевых узлах (FireWall, IPS, HIPS, AW и т.д.).

Продуктовая линейка компании Cisco Systems имеет достаточно много средств безопасности: системы обнаружения и предотвращения атак IPS/IDS; межсетевые экраны PIX/ASA; системы антивирусной проверки трафика; средства безопасности, встраиваемые в сетевое оборудование (IOS FW, L2 Security, NAC, и т.д.). При этом, описывая архитектуру безопасности, часто авторы не указывают такой компонент защиты, как безопасность рабочих станций.

Мало у кого вызывает сомнение, что на корпоративном компьютере (сервер/ПК) должны быть установлены системы антивирусной защиты. Мы же уверены, что на нем должен присутствовать еще один компонент, который будет отвечать не только за антивирусную безопасность на основе распознавания их сигнатур, но и за контроль над действиями программ/пользователя/системы. Вследствие изменчивости вирусов и угроз типа "day zero" необходимы совершенно новые механизмы защиты (рис. 1). С каждым годом компьютеры и программы, используемые на них, становятся все сложнее и сложнее. Меняется список задач, которые решает современный ПК. На нем можно писать документы, рисовать таблицы, просматривать презентации, играть. В компании любого размера существуют определенные правила пользования ПК, ПО, корпоративной сетью. Например, на ПК работников установлена операционная система MS Windows XP, офисный пакет MS Office 2003, бухгалтерская программа 1С.

А можете ли вы сказать, что могут делать эти программы? Разрешен ли программам MS Office доступ в Интернет, может ли это ПО модифицировать файлы? А системные файлы MS Windows

	CSA	Антивирус
Защита от вредоносного содержимого		
Защита от известных червей	X	X
Блокирование неизвестных червей	X	
Сканирование зараженных файлов		X
«Лечение» зараженных файлов		X
Идентификация червей по имени		X
Отказ в необходимости обновления	X	
Распределенный межсетевой экран	X	
Защита операционной системы	X	
Корреляция событий между агентами	X	

Рис. 1. Сравнение функциональных возможностей CSA и "традиционного" антивирусного ПО.

в папке Windows/System32? В большинстве случаев ответ – да.

Почему возникают эти вопросы? Дело в том, что мы привыкли доверять программному обеспечению. При этом мы забываем (или пытаемся забыть) о том, что программы пишут люди, а им свойственно ошибаться. Такие ошибки сами по себе могут привести к зависанию компьютера. В этом нет ничего хорошего. Но гораздо хуже, если этими ошибками сможет воспользоваться злоумышленник и получить доступ к содержимому вашего компьютера или всей корпоративной сети. Ведь, как мы уже узнали, MS Word имеет права на запись в каталоги ОС и доступа ко всей сетевой подсистеме.

Для решения этих проблем мы должны описать набор правил, которые определяют, кто, что и как может делать на защищаемом компьютере. В некоторых источниках данный свод правил называют корпоративной политикой безопасности.

После того как определена политика безопасности, нам необходимо применить ее на компьютерах корпоративной сети. В качестве одного из механизмов внедрения политики безопасности как раз и может быть использован продукт Cisco Security Agent.

Почему именно CSA?

Почему мы рекомендуем CSA? Ответ прост. Он удобен.

CSA удобен для специалистов по информационной безопасности. Все управление построено на политиках, которые могут объединяться в группы/подгруппы. Специальный мастер – CSA Profiler – позволяет автоматизировать создание политик для всех известных приложений. Уровень безопасности можно наращивать постепенно, начиная с простейших правил блокирования "случайного" доступа (рис. 2).

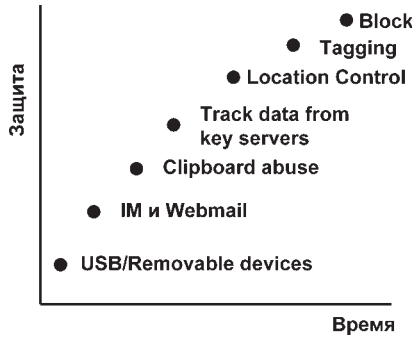

Рис. 2. CSA позволяет реализовать постепенное наращивание уровня защиты данных от случайных и намеренных угроз.

В качестве примеров политик можно привести следующие:

– "подозрительное приложение/процесс должно быть направлено на карантин на всех агентах";

– "приложение, получившее доступ к конфиденциальному документу, не может подключаться к сети";

– "приложения, которые читают загруженные файлы, не могут создавать command shells";

– "web-серверы могут писать только логи и временные файлы";

– "офисные приложения не могут читать или исполнять приложения";

– "сетевые серверы не могут вызывать почтовые приложения";

– "любая попытка модифицировать системные файлы будет сопровождаться запросом пользователя: не инсталлирует ли он новое ПО?";

– "почтовый клиент не может инсталлировать ПО";

– "политика VPN: VPN-клиент не подключается к сети, пока не запущен CSA".

Сфера применения CSA:

– web-серверы;

– почтовые, DNS- и другие Интернет-серверы;

– серверы приложений (ERP, CRM, биллинг и т.д.);

– серверы баз данных;

– рабочие станции и лэптопы (агенты для ПК и серверов отличаются друг от друга);

– устанавливается на все решения Cisco в области IP-телефонии и центров обработки вызовов.

Поддерживаемые ОС:

– Windows NT, 2000, XP, 2003 (включая локализованные версии), Windows Cluster;

– VMWare и Windows XP Tablet PC Edition 2005;

– Solaris;

– RedHat Linux Enterprise 3.0 AS, ES, WS (версии для серверов и рабочих станций).

Web-интерфейс сервера управления позволяет очень гибко настроить политику безопасности. При применении иерархичности правил возможно повторное использование уже разработанных политик. При этом CSA позволяет работать на достаточно высоком уровне абстракции.

CSA удобен для системных администраторов. CSA состоит из следующих компонентов: консоли управления (Cisco Security Agent Management Console – CSA-MC), отвечающей за внедрение политик, получение и хранение сигналов тревоги в SQL БД, сигнализацию администратору, обновление ПО, настройку политик и просмотр событий через браузер, и самого агента CSA, отвечающего за применение политик, полученных от сервера управления, посылку сигналов тревоги. Одна инсталляция управляющей консоли может обслуживать до 100 000 агентов CSA. При этом архитектура CSA обеспечивает возможность автономной работы CSA. Если агенты не имеют связи с CSA-MC, то они продолжают работу на основе последних загруженных правил.

"Удобна" система и с финансовой точки зрения. Инсталляция системы не подразумевает больших финансовых затрат на оборудование. Инсталляция на 100 000 агентов требует для работы всего три сервера типовой (необязательно максимальной) конфигурации. Не требуется и обновление аппаратного обеспечения станций, куда будет устанавливаться агент. CSA расходует не более 5% времени процессора.

Удобна ли система для пользователя? Система безопасности, призванная ограничивать пользователя, не может быть удобной для него. При этом можно настроить CSA таким образом, что пользователь не будет знать о присутствии на его машине этого программного обеспечения, пока не попытается выполнить "недопустимую" операцию. Как реакцию на "нежелательное" действие можно настроить запрет действия, разрешение, запрос у пользователя. Удобным механизмом является настройка записи этих действий. Например, если корпоративной политикой безопасности запрещается записывать на диск C: файлы *.mp3, а некий пользователь нарушил это правило, то, в зависимости от настроек в CSA-MC, он либо не сможет выполнить операцию копирования, либо файл будет скопирован с информированием системных администраторов.

CSA позволяет достичь компромисса между удобством пользователей и необходимым уровнем безопасности. Ключевым отличием CSA от других продуктов, представленных на рынке, является то, что при использовании этого продукта вы сами, а не производитель ПО можете выбрать, что является именно этим компромиссом именно для вас.

Для лучшего понимания возможностей Cisco Security Agent представим его структуру. CSA – клиент-серверное приложение, устанавливаемое на защищаемый компьютер. У агента есть встроенный набор правил (политик), согласно которым он работает. Для управления агентами используется консоль управления CSA-MC, устанавливаемая на отдельный сервер. CSA работает за счет перехвата обращений к ядру операционной системы. Он может обрабатывать запросы к файловой системе, реестру, сети. Основные особенности CSA с точки зрения управления следующие:

- иерархичность правил;
- детальная статистика о нарушениях политики безопасности;
- возможность повторного использования элементов политики;
- централизованное управление;
- гибкость управления настроек;
- возможность выбора компромисса между безопасностью и удобством пользования;

Рис. 3. Сферы применения Cisco Security Agent.

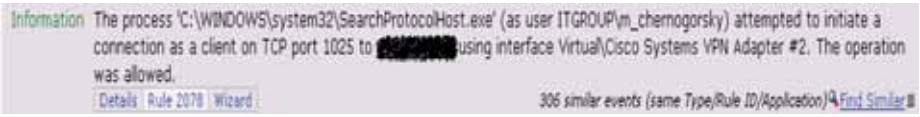

Рис. 4. Сообщение системы межсетевого экранирования в CSA-MC.

- возможность предотвращения атак без необходимости обновлений;
- низкие требования к аппаратным ресурсам (Windows – 1-5% CPU, Solaris – 3-10% CPU, ОП – 7-20 Мбайт).

Функционал CSA

Как уже было сказано ранее, CSA обладает очень широкими возможностями по контролю над действиями ПО/пользователей. Агент возможно настроить для выполнения как по отдельности, так и вместе нескольких функций (рис. 3):

- межсетевой экран;
- защита приложений;
- сетевой оптимизатор;
- предотвращение утечки данных;
- сбор сведений о системе.

Помимо этого, поддерживается расширенная защита системы (защита от Synflood/от некорректных пакетов, перезапуск сбойных сервисов); контроль доступа COM-компонентов; контроль исполняемого контента (защита от e-mail-червей, защита от автоматически загружаемого и исполняемого кода или элементов ActiveX) и ряд других функций.

Межсетевой экран (Firewall)

В настоящее время на рынке присутствует достаточно большое количество межсетевых экранов. Почему же мы предлагаем еще один вариант? Для ответа на этот вопрос рассмотрим возможности современных firewalls. Все решения умеют выполнять блокировку портов/протоколов. Многие серьезные решения имеют централизованное управление.

А вот возможность настройки определенных портов для определенных приложений встречается в единичных продуктах. Например, CSA позволяет разрешить доступ к 80-му порту только web-браузерам, а остальным приложениям будет запрещено использовать соединения с данным портом (рис. 4).

Новым элементом, который не встречается в современных межсетевых экранах, следует признать возможность агента

Табл. 1. Возможности подсистем межсетевого экранирования

Фильтрация на основе заголовков IP, TCP, UDP, ...	Возможность настроить классический межсетевой экран (МЭ) на рабочей станции, сервере. Простота и гибкость настройки.
Централизованное управление	Единая точка управления всеми МЭ пользователей. Удобство настройки и модификации политики сетевого доступа.
Настройка МЭ под приложения[new]	Централизованный контроль над тем, каким приложениям и куда разрешен доступ к сети.
Логические "состояния"	Возможность ужесточения или смягчения политики сетевого доступа в зависимости от условий. Например: если в системе обнаружен rootkit или вирус, то компьютеру разрешен доступ только к серверу с обновлениями.

применять политики на основе логических "состояний". Простой пример: пользователю, у которого на машине был обнаружен rootkit, будет запрещен доступ в корпоративную сеть. Более сложный пример: пользователю, открывшему файл с диска D:, доступ в сеть Интернет будет разрешен только после того, как он зайдет на сайт document-history-internal.local.

Приведенные примеры являются синтетическими, но они иллюстрируют возможности CSA по работе с логическими "состояниями".

Именно совокупность всех этих элементов позволяет нам говорить о том, что CSA можно и нужно использовать в качестве межсетевого экрана (табл. 1).

Рассмотрим возможности использования CSA в качестве межсетевого экрана с разными уровнями безопасности:

- *низкий:* разрешены все исходящие соединения. Входящие соединения блокируются, кроме явно указанных (необходимых для нормальной работы стандартного компьютера данного предприятия). Подходит для большинства пользователей. Не требует никаких дополнительных знаний о работе сетевого стека и межсетевых экранов.
- *средний:* разрешены явно указанные политикой исходящие/входящие соединения (которых достаточно для комфортной работы в данной сети). Для остальных соединений (как входящих, так и исходящих) выдается запрос пользователю об установке данного соединения. Пользователь может разрешить или заблокировать соединение, а также завершить приложение, инициирующее/принимающее данное соединение. Для любого ответа пользователь может указать опцию "сохранить ответ". В этом случае для таких соединений агент будет автоматически подставлять ответ пользователя. Средний режим безопасности подходит для квалифицированных пользователей, испытывающих необходимость в углубленной работе с сетью (например, системные администраторы, сетевые инженеры).
- *высокий:* разрешены только явно указанные политикой входящие/исходящие соединения. Все остальные соединения блокируются. Применяется для компьютеров, для которых необходим максимальный уровень сетевой безопасности. Не требует от пользователя знаний о работе сетевого стека. Но для этого режима необходимы дополнительные административные меры, которые позволят объяснить пользователю, что он может делать, а какие действия ему запрещены.

Защита приложений (App protection)

При описании политики безопасности чаще всего минимальным элементом (объектом) является пользователь/рабочая станция. Но на компьютере современного работника установлено большое количество приложений. Многие из них используются в бизнес-процессе, и от их защищенности зависит информационная безопасность всего предприятия.

CSA может помочь в решении данной проблемы. Система защиты позволяет определить, к каким компонентам (файлы, реестр, данные), кому (системные пользователи, администраторы, пользователи) и при каких условиях можно получить доступ.

Чтобы стало более понятно, приведем пример простой политики защиты приложения:

- доступ к ресурсам приложения разрешен всем на чтение (кроме конфигурационных ресурсов);
- доступ к конфигурационным ресурсам разрешен на чтение/запись только самому приложению;
- доступ к каталогу программы на запись разрешен только самому приложению, запущенному из-под учетной записи доменного администратора, когда компьютер находится в режиме инсталляции программ.

Такими простыми и, главное, понятными правилами мы можем установить достаточно жесткую политику безопасности для отдельного приложения. А так как в общем случае добавление нового приложения на предприятии требует от администратора выполнения всего лишь нескольких действий (скопировать политику существующего приложения, изменить переменные для соответствия новому приложению, нажать кнопку генерации правил), то это позволяет быстро и эффективно выполнить защиту всех приложений, используемых в компании.

Приведенные правила обеспечивают лишь общую защиту. Но при этом данная политика является эффективной. Для более тонкой защиты можно разработать другую, более сложную политику (табл. 2).

Табл. 2. Возможности подсистемы защиты приложений

Защита всех аспектов работы приложения	Повышение надежности системы за счет комплексной защиты (файловая подсистема, реестр, сеть, передача данных) приложения.
Простота защиты новых приложений	Снижение операционных затрат при внедрении защиты новых приложений. Повышение масштабируемости решения.
Совместимость со всем ПО	CSA не предъявляет никаких требований к защищаемым приложениям.
Централизованное управление	Снижение операционных затрат. Если защита приложения настроена для одного рабочего места, то включение ее на других компьютерах происходит очень просто (в несколько кликов).

Сетевой оптимизатор (Trusted QOS)

В сетях, построенных по рекомендациям Cisco Systems, коммутаторы не доверяют

информации о классе трафика, полученного с компьютера, а производят классификацию уже внутри сети. Это рекомендация появилась потому, что существует множество "сетевых оптимизаторов", которые устанавливают значения TOS, DSCP для обеспечения наилучшей производительности сети. Но эта производительность наилучшая с точки зрения данного приложения на данном компьютере. Конечно, хорошо, когда фильм с ftp скачивается за 5 мин вместо 20. Но что будет происходить при этом с голосовым трафиком? В основном из-за этого на коммутаторах доступа настроена политика сброса классов трафика, полученных с компьютера, с последующей классификацией на основе ACL, NBAR.

Применение CSA решает эту проблему по-другому. CSA позволяет явно переназначить параметры DSCP всего трафика в зависимости от разных факторов. Например: весь трафик, созданный программой управления базой данных, будет иметь DSCP=21, трафик IP Communicator – DSCP=ef, остальной трафик – DSCP=0. Это позволяет нам перенести границу доверия QOS с порта коммутатора на конечную рабочую станцию без негативных последствий для сети. Это может быть выполнено даже в очень крупных компаниях (50–60 тыс. компьютеров), если на них установлены CSA. Администраторам не нужно будет беспокоиться о том, что пользователь переназначит (сам или с помощью программных "оптимизаторов") параметры QOS.

Из сетевых функций CSA также следует отметить возможность выполнения rate limit. Это позволит быстро обнаружить и минимизировать последствия появления в сети рабочих станций с работающими flood-программами.

Например, установка ограничений в 500 соединений в минуту позволяет работать стандартному пользователю, но вызовет срабатывание правила для аномальной flood-активности. Дальнейшие ограничения, накладываемые на такой компьютер, определяются политикой сетевой безопасности: от сообщения в CSA-MC до полной сетевой блокировки пользователя. Общие преимущества использования CSA-MC приведены в табл. 3.

Табл. 3. Применение CSA для сетевой подсистемы

Trusted QOS	Повышение производительности сети за счет переноса границы доверия QOS с коммутаторов на рабочие станции.
Rate limit	Снижение времени простоя сети за счет быстрого и автоматического обнаружения и противодействия внутренним flood-атакам.

Предотвращение утечки данных (Thief data protection)

Еще одним применением агента может служить функция предотвращения утечки важных данных с локального компьютера (табл. 4).

Среди функционала, который может помочь при создании системы предотвращения утечки информации, следует отметить:

Табл. 4. Применение CSA для предотвращения утечки данных

Контроль съемных носителей	Возможность ограничения доступа к съемным носителям (flash, CD, floppy).
Контроль WiFi-подключений	Повышение безопасности сети.
Защита вне сети	Система работает даже при нахождении пользователя вне корпоративной сети.

- гибкий контроль доступа к файлам. Приложению может быть разрешен/запрещен доступ к файлам. Либо постоянно, либо по выполнении определенных условий. Например: приложению, прочитавшему файл с диска D:, будет разрешено выводить данные только на печать, а запись/копирование – в буфер обмена, передача данных по сети будет для приложения запрещена. Также можно запретить снятие копий с экрана;
- контроль доступа к съемным носителям. CSA позволяет ограничить доступ к flash, CD, floppy и другим устройствам, определяемым ОС Windows как съемные;
- контроль доступа к беспроводным соединениям. Используя CSA, можно запретить пользователю при работе в корпоративной сети использовать небезопасное WiFi-соединение;
- защита работает даже при нахождении пользователя вне корпоративной сети.

Например, на компьютере есть папка с важными данными, утечка которых может привести к финансовым потерям. CSA для данного случая может быть настроен следующим образом:

- существует папка с конфиденциальными данными C:/secret;
- пользователь может работать с данными в папке (при открытии любого файла из папки на запись будет записано сообщение в log);
- работа с папкой разрешена только при нахождении в корпоративной сети (локально, с использованием VPN);
- пользователю будет запрещено (с записью в log) копировать файлы из этой папки;
- доменному администратору разрешено копировать файлы из папки C:/secret на сервер \\spec-server\secret-backup. Остальная удаленная работа с папкой запрещена;
- запрещен обмен с использованием clipboard.

Сбор сведений о системе (Info Collection)

Комплекс Cisco Security Agent позволяет централизованно собрать разнообразную информацию о системе, на которой он установлен (табл. 5).

Табл. 5. Информативные возможности CSA

Информация об установленном на компьютере ПО	Построение отчетов об использовании корпоративных рабочих станций.
Детальная информация о деятельности ПО	Повышение надежности системы за счет полного понимания особенностей работы ПО.
Наличие Script API	Повышение масштабируемости решения.

Из "интересных" типов отчетов о системе можно выделить:

- информация об установленном на компьютере ПО. Показывает полный перечень установленного ПО, включая саму систему и все обновления;
- информация о текущих сетевых соединениях на машине;
- детальная информация о всех действиях определенного приложения (обращения к файлам, обращение к реестру, обращение к сетевым ресурсам). Этот отчет часто применяется для создания детальной политики для сложного приложения. *Данный вид отчета требует отдельной лицензии.*

Начиная с версии 5.2, CSA поддерживает механизм Script API, который позволяет внешним программам получать доступ к данным CSA-MC. Возможно, благодаря написанию программ-скриптов, упрощающих конфигурирование CSA.

Интеграция с продуктами Cisco

Мы в основном рассматривали CSA как отдельный продукт. Однако при построении комплексной системы информационной безопасности предприятия также могут применяться и другие решения. Агент может быть интегрирован с рядом продуктов компании Cisco Systems:

- *MARS.* Интеграция позволяет системе анализа и корреляции более точно и правильно построить карту сети, а также более точно выдавать графический вектор атак.
- *IPS.* Настройка интеграции IPS и CSA дает системе предотвращения атак возможность снизить количество ошибок типа false negative.
- *NAC.* При использовании NAC совместно с CSA можно настроить политику агента таким образом, чтобы она учитывала текущий NAC-статус. И в зависимости от него агент сменит применяемую политику.

Вместо заключения

В заключение кратко отметим преимущества, которые дает компании внедрение продукта Cisco Security Agent:

- *контроль процессов, происходящих на рабочих станциях;*
- *снижение административных затрат на внедрение политики безопасности;*
- *контроль над применением корпоративной политики безопасности;*
- *сокращение возможности использования рабочих компьютеров в непроизводственных целях;*
- *повышение стабильности и защищенности ИТ-инфраструктуры.*

Михаил Черногорский,
системный инженер,
компания INLINE Technologies