Cisco pxGrid: автоматизация передачи данных по нескольким платформам благодаря унифицированной архитектуре

Обзор

ИТ-среды буквально утопают в потоках сетевых данных и данных безопасности, что еще больше усложняет управление безопасностью и развертывание систем защиты от угроз. Традиционные API-интерфейсы обладают чрезвычайно ограниченным набором функций, небезопасны, поддерживают конкретные платформы и поэтому не способны предоставить практическое решение. Cisco Platform Exchange Grid (pxGrid) позволяет всем разнообразным платформам разных поставщиков в одной среде безопасно обмениваться информацией с обеспечением абсолютного контроля в обоих направлениях. Все это реализовано автоматически в реальном времени без необходимости использования API-интерфейсов для конкретных платформ.

В настоящей статье рассматриваются следующие вопросы:

- трудности, с которыми сегодня сталкиваются заказчики при эксплуатации разных систем безопасности, которые не могут взаимодействовать между собой или обмениваться информацией;
- как платформа Cisco Platform Exchange Grid (pxGrid) обеспечивает мгновенный автоматический обмен данными между системами;
- архитектура и эксплуатация Cisco Platform Exchange Grid (pxGrid);
- как разработчики могут сегодня начать интегрировать свои платформы с pxGrid для обмена контекстом между своими платформами и продуктами безопасности Cisco, а также с другими партнерам по разработке, поддерживающими pxGrid.

Увеличение проблем, связанных с безопасностью и эксплуатацией

Для обеспечения безопасного и бесперебойного функционирования ИТ-среды предприятия уже используют целый ряд инструментов и платформ, зачастую от разных поставщиков. К ним могут относиться платформы управления доступом и идентификацией (IAM), платформы внедрения политик, системы управления информацией и событиями безопасности (SIEM), системы защиты от угроз и многое другое. Все эти инструменты критически важны для защиты предприятия и его деятельности. Но, к сожалению, они не могут «разговаривать» друг с другом, что создает многочисленные «пробелы» в информации и представляет значительную трудность с точки зрения эксплуатации.

Переход от одного инструмента к другому только добавляет сложности и увеличивает затраты на обеспечение безопасной эксплуатации. Кроме того, снижается общая эффективность безопасности ИТ-среды, так как для получения информации, необходимой от этих инструментов для принятия соответствующих действий или реагирования на угрозы, требуется затратить много времени и ручного труда. А это время, которое предприятие могло бы потратить на устранение сложной угрозы, которая стремится проникнуть вглубь среды или получить конфиденциальные данные.

Традиционный ответ в данным случае подразумевал использование платформы API-интерфейсов для обмена информацией между платформами. Однако в современных ИТ-средах такой подход не поддается масштабированию. API-интерфейсы исторически обеспечивают отдельную связь с конкретной целью между двумя системами. Сегодня обмениваться информацией приходится с очень большим числом платформ, предприятия не могут в реальных условиях устанавливать связь одного инструмента с другим через API-интерфейсы одного назначения.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

В первую очередь такие API-интерфейсы просто не существуют. Поставщики должны постоянно разрабатывать новые и новые способы поддержки десятков API-интерфейсов одного назначения и повторно тестировать их при каждом незначительном обновлении ПО, а это неимоверные усилия. Даже если бы они смогли сделать это, предприятия просто скоро бы утонули в потоках информации. API-интерфейсы работают на основе базовой модели опросов, просто отправляя запросы на получение информации снова и снова. Такой тип коммуникаций может быть хорош только в случае обмена данными между одной-двумя системами. Но если это одновременно начинают делать 20 систем, это чревато возникновением больших проблем с производительностью и масштабированием.

API-интерфейсы также обычно небезопасны. Очень часто в них используется простая (и относительно ненадежная) аутентификация по имени и паролю. В этом случае обычно не предоставляется информация о том, как используются эти данные. Как только API-интерфейс открывает путь в систему, другие системы могут получить доступ к этой информации и делать с ней все, что захотят.

Предприятия сталкиваются с серьезной проблемой эксплуатации систем безопасности, которую не так просто решить. Возможно, было бы лучше, если бы все разрозненные инструменты в ИТ-среде могли говорить друг с другом? Что, если бы поставщики платформ могли получать контекстную информацию и возможности других систем и использовать их в своей среде, предоставляя своим сотрудникам все, что им необходимо для решения реальных проблем и быстрого реагирования на угрозы?

Это именно то, что делает Cisco pxGrid.

Основные сведения о решении pxGrid

Решение pxGrid позволяет разным сетевым системам и системам безопасности в ИТ-среде говорить на одном языке. Вместо того чтобы каждая система зависела от отдельных API-интерфейсов одного назначения, эти интерфейсы можно один раз интегрировать с pxGrid, чтобы обмениваться контекстной информацией друг с другом. Коммуникации между системами теперь могут происходить автоматически и мгновенно без необходимости ручного вмешательства.

pxGrid обеспечивает межплатформенное взаимодействие между сетевыми системами разных поставщиков по разным компонентам ИТ-инфраструктуры. Сюда включаются системы мониторинга безопасности и обнаружения вторжений, платформы определения сетевых политик, управление ресурсами и конфигурациями, платформы управления идентификацией и доступом и практически любые другие ИТ-платформы. Поставщики ИТ-решений и решений безопасности могут использовать pxGrid для обмена контекстом с платформами Cisco, использующими pxGrid, а также с системами любого другого партнера экосистемы pxGrid. Благодаря такой унифицированной структуре они могут обмениваться контекстом в обоих направлениях с большим числом других платформ без необходимости использования API-интерфейсов специального назначения. Решение pxGrid можно внедрить только один раз, а затем использовать его снова и снова для интеграции с любой платформой, поддерживающей pxGrid.

pxGrid полностью безопасно и может настраиваться заказчиком в соответствии со своими потребностями. Партнеры могут делиться только той, информацией, которой хотят делиться, и получать только ту информацию с других платформ, которая действительна важна для них. Благодаря такому уровню пользовательской настройки, а также архитектуре pxGrid «публикация — подписка — запрос», обмен контекстом очень просто масштабировать даже при обмене данными со множеством систем. Более того, позволяет платформам экосистемы партнеров pxGrid выполнять сетевые действия с использованием сетевой инфраструктуры Cisco. Специалисты по безопасности не только получают релевантную информацию об угрозах быстрее, но могут также быстрее предпринимать соответствующие меры.

Решение pxGrid не зависит от информационной модели и формата данных, так как ориентировано на передачу данных безопасности с учетом контекста. В результате обеспечивается необходимая гибкость и возможность работы с разными типами данных, которые нужны для разных вариантов внедрения. И, наконец, эти возможности обмена контекстом и сетевого управления, позволяют поставщикам ИТ-инфраструктуры использовать больше вариантов внедрения, более эффективно выполнять свои функции и получать более глубокое представление о сетевой инфраструктуре.

Возможности и преимущества

Решение pxGrid обеспечивает следующие возможности и преимущества.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

- **Единая структура для обмена контекстом для большого числа систем:** с помощью pxGrid любая партнерская платформа может подключаться к любым другим платформам в ИТ-среде (включая платформы Cisco и третьих фирм, использующих pxGrid), чтобы обмениваться релевантным контекстом. Этот контекст может включать статус эксплуатации в реальном времени, накопленную информацию о событиях, данные телеметрии об эксплуатации, статистику использования и любую другую информацию, которая может потребоваться ИТ-платформе для обмена или потребления.
- **Полный контроль над тем, каким контекстом и с какими платформами можно обмениваться:** так как решение pxGrid полностью настраиваемое, партнеры могут публиковать только ту конкретную контекстную информацию, которой они готовы обмениваться, и могут контролировать, с какими партнерскими платформами они будут обмениваться этой информацией.
- **Обмен контекстом в обе стороны по схеме «многие со многими»:** pxGrid позволяет платформам обмениваться контекстом с других подключенных платформ и потреблять его. При этом все коммуникации будут централизованно организовываться решением, и так же централизованно будет обеспечиваться безопасность, после чего данные будут предоставлены каждой платформе в своем первоначальном формате.
- **Масштабированное одновременное подключение к нескольким платформам:** pxGrid позволяет платформам публиковать только контекстные данные, релевантные для партнерских платформ. Можно настроить самые разные «темы» для разных партнерских платформ, при этом обмениваться ими через одну и ту же повторно используемую структуру pxGrid. Более того, за счет обмена только релевантными данными, платформы, которые являются одновременно публикующими и подписанными, могут легко масштабировать то, чем они делятся, удаляя нерелевантные данные.
- **Интеграция с платформами Cisco:** pxGrid обеспечивает унифицированный способ публикации и подписки на релевантный контекст для все большего числа платформ Cisco, использующих pxGrid для интеграции с третьими фирмами.
- **Автоматическое реагирование на сетевые угрозы:** благодаря внедрению сетевых инструментов pxGrid, платформы с поддержкой pxGrid смогут предпринимать действия по реагированию на сетевые угрозы просто путем запроса на pxGrid, даже если платформа, которая посылает запрос, сама не имеет сетевой топологии или возможности контроля.

Высокотехнологичный механизм для межплатформенной коммуникации

pxGrid предоставляет намного более удобный способ обмена информацией, чем обычные API-интерфейсы, и этому есть целый ряд причин. Во-первых, он обеспечивает возможность коммуникаций по схеме «многие со многими» для самых разных сетевых платформ, что означает, что это изначально намного более масштабируемый вариант, чем архитектуры, построенные по принципу опроса.

Во-вторых, он обеспечивает гораздо большие возможности для пользовательской настройки. Каждому инструменту нет никакого смысла принимать всю информацию, сгенерированную всеми другими системами, которая не будет масштабироваться. Но, в отличие от API-интерфейсов, которые не предоставляют больших возможностей в плане пользовательской настройки того, что и как будут передавать системы, pxGrid позволяет каждой подключенной системе получать только ту информацию от других систем, которая ей нужна, и обмениваться только той информацией, которая релевантна для других систем, с которыми она общается.

И, наконец, pxGrid обеспечивает надежную защиту и контроль. Она обеспечивает конфиденциальность системных данных намного более эффективно, чем API-интерфейсы, за счет предоставления полностью контролируемого доступа, аутентификации и авторизации для каждой системы в этом решении. Точно так же, как пользователям в сети может быть предоставлен доступ к определенным ресурсам, так и ИТ-поставщики могут предоставить системам, подключаемым к pxGrid, доступ к информации, которую им необходимо получить с их платформ, но больше ни к чему другому.

Принцип работы pxGrid

Базовая архитектура pxGrid состоит из центрального контроллера pxGrid с несколькими системами (узлами), подключенными к нему через клиентскую библиотеку. Контроллер выполняет роль оператора-коммутатора для сети, устанавливая связь с каждым агентом узла, чтобы позволить каждой подключенной системе обмениваться разрешенной контекстной информацией с другими узлами.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

На рис. 1 представлен пример работы решения pxGrid в общих чертах. Здесь вы видите все разнообразие платформ, которые участвуют в обеспечении безопасности обычного предприятия. Каждая играет свою важную роль, но для эффективного выполнения своей работы каждой платформе нужна информация из других систем.

Рисунок 1. Обмен контекстом в pxGrid

В качестве простого примера возьмем пример внедрения концепции «принеси на работу свое устройство» (BYOD), когда предприятие хочет внедрить разные уровни привилегий доступа, в зависимости от устройств, которые используют его сотрудники, и местоположения сотрудников. Для этого необходима информация от трех компонентов: платформы управления идентификацией и доступом (IAM) для предоставления разрешений для приложений, платформы управления мобильными устройствами (MDM) для проверки статуса регистрации устройства и платформы SIEM для доступа и информирования о рисках угрозы, связанных с конкретным сотрудником.

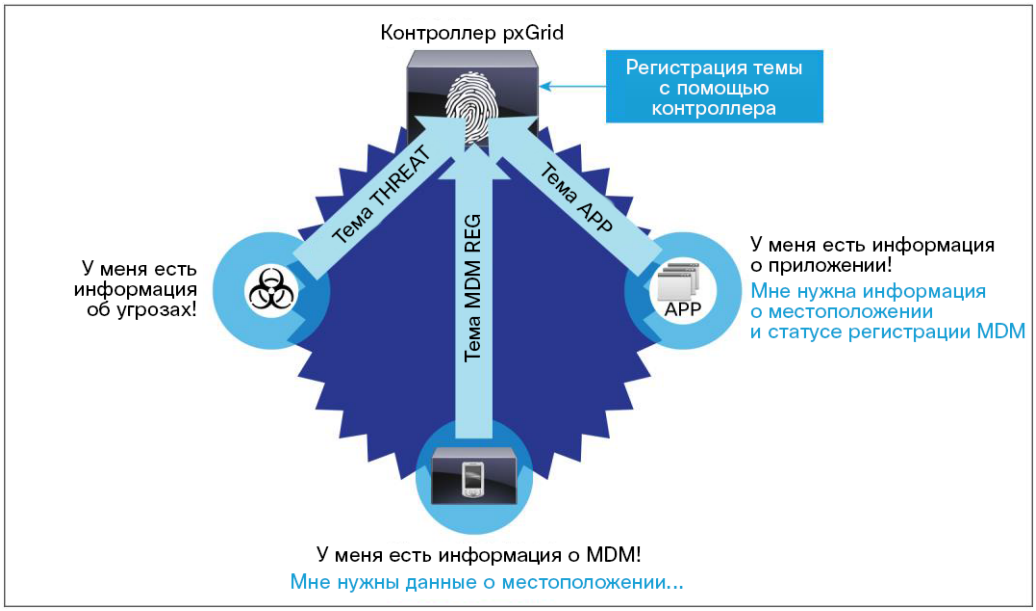
Здесь показано, как pxGrid обеспечивает коммуникации между платформами для упрощения этого процесса.

Сначала каждая платформа независимо аутентифицируется в pxGrid. pxGrid также обрабатывает авторизации, контролируя, какие платформы могут публиковать данные, какие могут подписываться на получение и что они могут запрашивать, а также то, какой определенной контекстной информацией могут обмениваться с другими платформами в сети решения. Это делается через модель «публикация/подписка». Каждая подключенная платформа публикует определенные «темы» в pxGrid и (или) подписывается на темы, которые релевантны для вариантов внедрения, с которыми она работает. Каждая тема регистрируется в каталоге тем pxGrid, чтобы затем ее могли найти платформы, заинтересованные в этой теме. Платформы могут подписываться на все обновления какой-либо темы в реальном времени, посылать запросы со специальными атрибутами по требованию или делать пакетные загрузки информации по этой теме.

Таким образом, в случае с BYOD, платформа IAM публикует тему «Приложения», предоставляя пользователям разрешения на доступ к приложениям. Платформа MDM публикует тему «Регистрация MDM», предоставляя информацию о статусе заданного устройства. SIEM публикует тему «Риск угрозы со стороны сотрудника», предоставляя информацию о риске угрозы, связанном с заданным пользователем (см. рис. 2).

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

Рисунок 2. Обмен контекстом в решении pxGrid для реализации BYOD и защиты от угроз



В то же самое время каждая платформа в pxGrid подписывается на темы, релевантные для ее конкретных операций. Платформа IAM может подписаться на темы «Регистрация MDM» и «Риск угрозы со стороны сотрудника». Платформа MDM может подписаться на тему «Приложение». SIEM публикует информацию о риске угрозы со стороны сотрудника для получения обеими платформами — MDM и IAM. После того как такая структура утверждена, каждая платформа может постоянно получать или запрашивать в оперативном режиме необходимую ей информацию из других платформ в сети pxGrid в соответствующем формате данных для выполнения своей роли в плане предоставления или запрета доступа для пользователей BYOD (см. рис. 3).

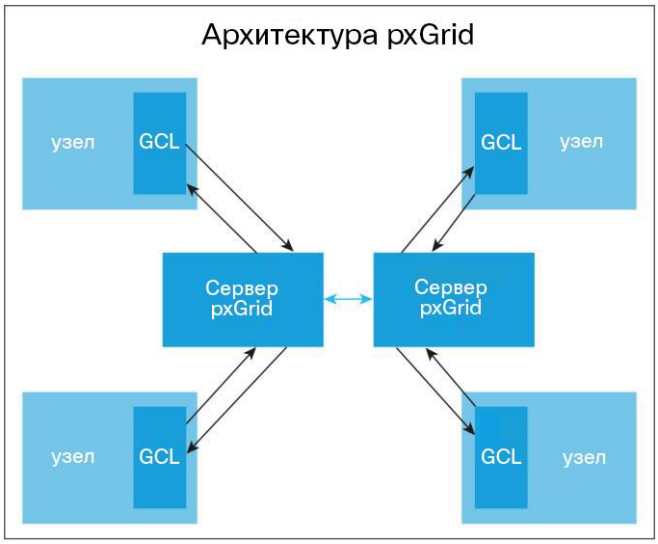
Рисунок 3. Использование pxGrid для упрощения обеспечения безопасности BYOD

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

Архитектура pxGrid

В центре архитектуры pxGrid находится контроллер и задействованные узлы (см. рис. 4). В стандартном развертывании у заказчика узлы локализованы на отдельных хостах, но в рамках одной сети. Однако они могут быть также распределены по разным средам заказчика. Как говорилось выше, каждый узел проходит аутентификацию, регистрацию и авторизацию, чтобы иметь возможность обмениваться данными по сети pxGrid, и может определить себя как «провайдера» или «потребителя» тем для обмена информацией. Сервер pxGrid обеспечивает маршрутизацию сообщений и контроль на основе обмениваемых контекстных данных и авторизации задействованного узла. Он поддерживает запросы, уведомления и пакетные загрузки контекстных данных. В зависимости от контекста pxGrid может установить внедиапазонный канал для пакетной загрузки.

Рисунок 4. Высокоуровневая архитектура pxGrid



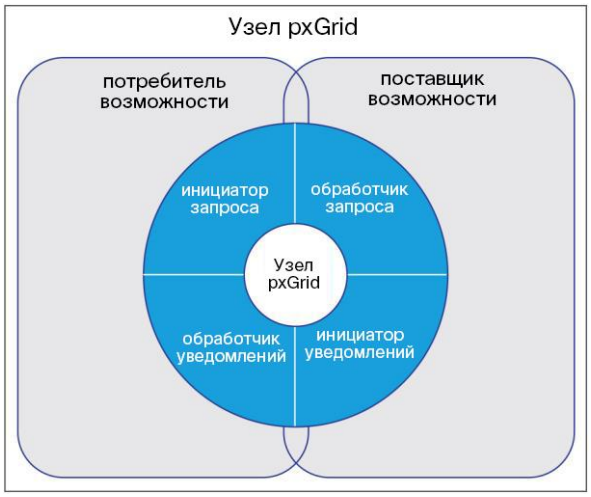
Узлы не связываются напрямую с pxGrid. Вместо этого узлы совершают запрограммированные вызовы в библиотеку Grid Client Library (GCL), которая, в свою очередь, подключается к сети pxGrid и запрашивает у нее информацию. В зависимости от примера внедрения в одном развертывании может быть только несколько узлов, а в других — тысячи. pxGrid поддерживает масштабирование в сторону увеличения узлов.

Двусторонние коммуникации

Решение pxGrid обеспечивает двустороннюю связь между узлами pxGrid. Узлы могут быть одновременно и «провайдерами», и «потребителями» возможностей при условии, что они авторизованы контроллером pxGrid на выполнение обеих функций (см. рис. 5). Как «провайдер» возможности узел обрабатывает запросы, создает уведомления или делает и то и другое. Как «потребитель» возможности, узел инициирует запросы, получает уведомления или делает и то и другое. (Примечание. «Возможность» в данном случае означает информационные каналы или темы для обмена контекстной информацией. pxGrid использует информационные модели для определения контекстных данных, интерфейсов или операцией для возможностей, связанных с этой моделью. Например, модель «Идентификатор» может включать возможность «Каталог сеансов», состоящую из интерфейсов для получения информации, относящейся к началу сеансов в сети.)

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

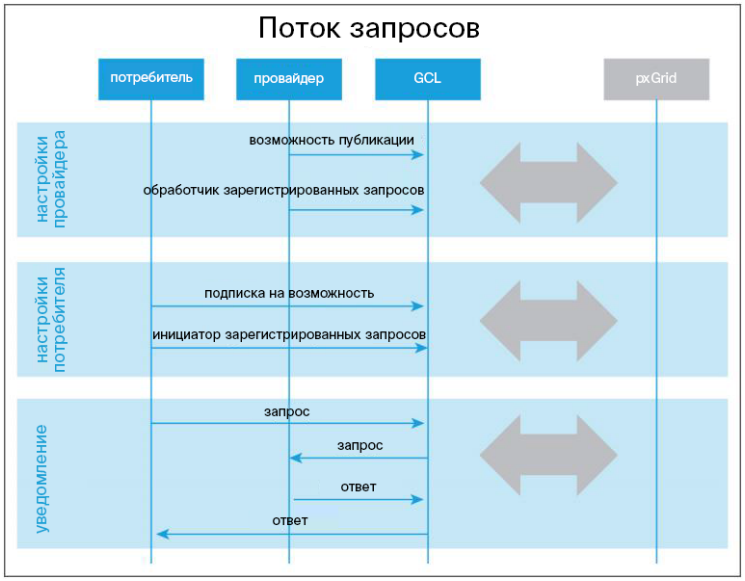
Рисунок 5. Двусторонние коммуникации в узле



Запросы

Запрос — это синхронный вызов, инициированный потребителем и обслуживаемый провайдером (см. рис. 6). С помощью GCL потребитель использует инициатор вызова запросов для начала установки соединения. Провайдер применяет обработчик запросов для программируемой обработки запросов и генерации ответов. pxGrid передает запрос через библиотеку GCL потребителя в библиотеку провайдера, аналогично передаче на другой узел в сети. Используя пользовательский код, указанный разработчиком в обработчике запросов, провайдер создает ответ, который pxGrid затем отправляет обратно потребителю. Потребитель ожидает получения ответа.

Рисунок 6. Поток запросов

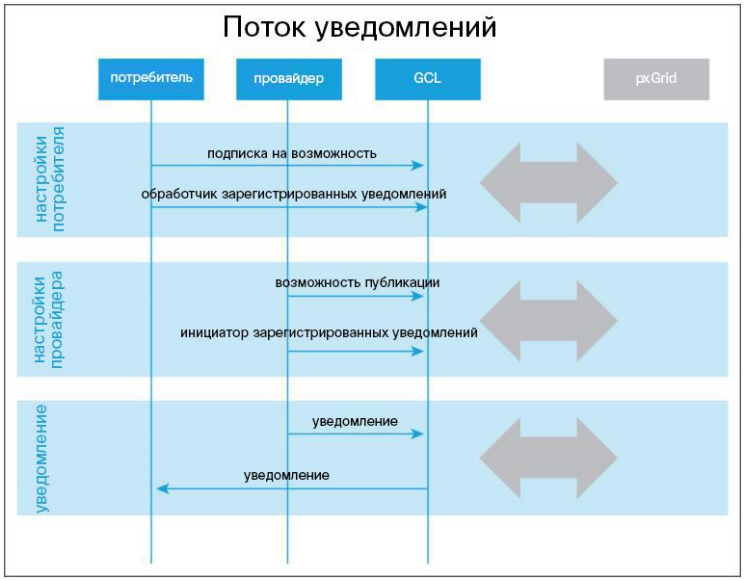


© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

Уведомления

Уведомление — это асинхронное сообщение, сгенерированное провайдером и полученное потребителем. Потребитель сначала должен зарегистрировать интересующую его информационную тему. Сравнивая с обменом сообщениями, можно сказать, что потребители подписываются на тему, а провайдеры публикуют темы. Библиотека GCL поддерживает связь с pxGrid, поэтому потребители и провайдеры могу сосредоточить свое внимание на написании кодов для получения и предоставления информации. Потребители не ждут информацию, как в случае с потоком запросов. GCL использует отдельный канал для активации инициатора уведомлений, поставляемого потребителем. На рис. 7 представлена схема потока.

Рисунок 7. Поток уведомлений



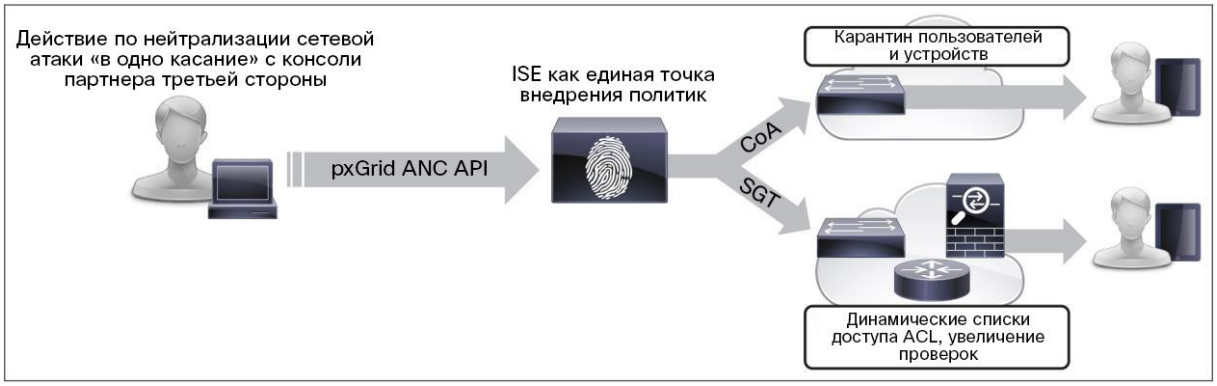
Автоматическое реагирование на сетевые угрозы

Решение pxGrid также предоставляет платформам с поддержкой pxGrid возможность предпринимать действия по защите сети от угроз в отношении пользователей или оконечных устройств непосредственно с партнерской платформы. Например, на платформе SIEM оператор может помещать в карантин пользователей или устройства или предпринимать действия по расследованию инцидентов, перенаправляя трафик. Благодаря pxGrid все это можно делать с консоли SIEM на той же структуре pxGrid, которая используется для обмена контекстом или его получения. В этом сценарии система вызывает API-интерфейс, который отвечает за реагирование на угрозы в рамках структуры pxGrid. Затем он может использовать возможности реагирования на угрозы, которые уже встроены в платформы, например Cisco Identity Services Engine, для выполнения действий по реагированию на угрозы. Благодаря этой архитектуре платформам с поддержкой pxGrid не нужно понимать, как нужно выполнять соответствующее действие. Через pxGrid они просто вызывают платформу, например, Identity Services Engine, которая понимает сеть и имеет все необходимые инструменты для выполнения требуемого действия.

На рис. 8 представлены возможности адаптивного управления сетью Adaptive Network Control (ANC) в модуле Identity Services Engine, которые инициирует платформа с поддержкой pxGrid, вызывающая API-интерфейс, отвечающий за реагирование на угрозы. Этот модуль изменяет параметры авторизации и выдает метку безопасности (SGT).

Рисунок 8. Реагирование на угрозы в решении pxGrid

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.



Использование протокола XMPP в решении pxGrid

pxGrid использует протокол Extensible Messaging and Presence Protocol (XMPP) в качестве основного протокола для обмена данными между системами в рамках сети pxGrid. Протокол XMPP использует язык XML и работает на децентрализованной архитектуре клиент-сервер, где клиенты безопасно подключаются к серверам, а сообщения между клиентами передаются через сервера XMPP, развернутые внутри кластера. XMPP широко использовался для систем публикации-подписки для выполнения целого ряда задач: передачи файлов, видео, работы в Интернете вещей и других приложений для совместной работы и социальных сетях.

XMPP обеспечивает несколько важных преимуществ для обмена данными безопасности в рамках решения pxGrid. Это следующие преимущества.

- **Открытая структура коммуникаций на основе стандартов** с децентрализованной и объединенной архитектурой, без сбоев.
- **Высокая безопасность** с поддержкой высокобезопасной сегрегации доменов и объединения с использованием механизмов Simple Authentication and Security Layer (SASL) и Transport Layer Security (TLS).
- **Обмен информацией и управление событиями в реальном времени** с использованием уведомлений «публикации — подписки».
- **Гибкость и расширяемость** как у структуры на языке XML, благодаря чему можно легко адаптироваться к новым вариантам внедрения и поддерживать функциональность с возможностью настройки в соответствии с требованиями пользователей.
- **Поддержка нескольких механизмов обмена информацией** между задействованными клиентами.
- **Поддержка прямых запросов и запросов по требованию между клиентами,** общающимися через сервер XMPP.
- **Поддержка передачи файлов вне диапазона и прямые коммуникации** между задействованными клиентами.
- **Двусторонняя связь,** благодаря которой отменяется необходимость в туннелировании межсетевого экрана или открытия нового подключения в каждом направлении между клиентом и сервером.
- **Масштабируемость** с поддержкой развертываний в кластерном режиме с несколькими адресатами, одновременно принимающими сообщения, и маршрутизацией сообщений, а также с передачей между равноправными узлами.
- **Простое развертывание** благодаря упрощенной структуре XMPP узлов для обнаружения присутствия, доступности и сервисных возможностей других задействованных в системе узлов.

Для упрощения интеграции с разными партнерскими платформами pxGrid задает инфраструктурный протокол, который скрывает нюансы протокола уровня данных XMPP и обеспечивает расширение моделей обмена информацией с использованием простых и интуитивно понятных API-интерфейсов. Узлы pxGrid подключаются к сети pxGrid с помощью протокола pxGrid, который использует транспортный протокол XMPP

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

и предоставляет протокол уровня приложений, который использует расширения XML и XMPP. Партнеры, которые предоставляют платформы для решения pxGrid, могут расширить инфраструктурную модель протокола pxGrid и задать модели и схемы конкретно для каждой возможности. Кроме того, они также могут обеспечить четкое разделение инфраструктуры и возможностей, которые должны быть реализованы в этой инфраструктуре.

Обеспечение безопасного обмена информацией

pxGrid обеспечивает безопасный обмен информацией между узлами в сети pxGrid тремя способами. Во-первых, для получения или отправки информации в сети pxGrid для каждой платформе помимо простой защиты с помощью имени пользователя и пароля используется надежная инфраструктура открытых ключей (PKI) и аутентификация на основе сертификатов.

Во-вторых, pxGrid предоставляет структуру подробной авторизации, чтобы контролировать, что каждая подключенная платформа может делать в сети и чего она делать не может. Например, операторы могут определять, какие конкретные темы платформы можно публиковать, какие получать, разрешать отдельным узлам подписываться на темы, но не публиковать их (и наоборот) или указывать, что определенные платформы могут делать пакетные загрузки, тогда как другие нет.

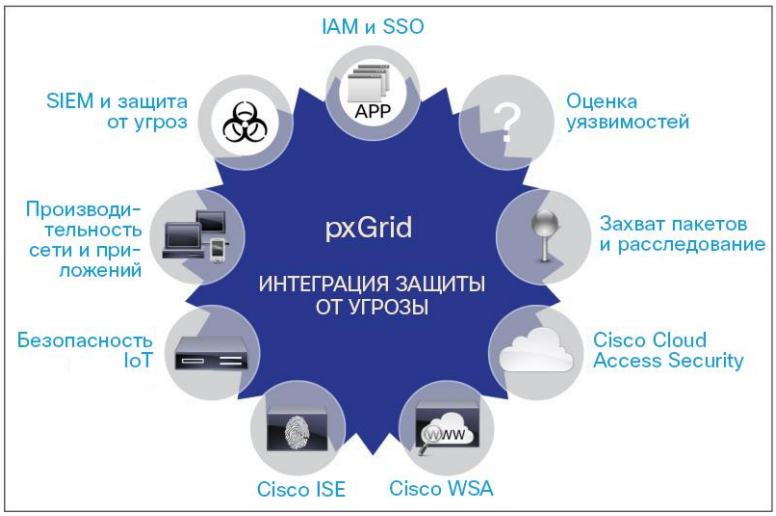
И, наконец, все данные, которые циркулируют в сети pxGrid, зашифрованы. Все коммуникации всегда идут по частным каналам и защищены от перехвата атакой через посредника. Работая вместе, эти инструменты обеспечивают большую безопасность и контроль межплатформенных коммуникаций, чем обычные API-интерфейсы.

Экосистема pxGrid в действии

pxGrid может предоставить эффективную структуру для обеспечения межплатформенных коммуникаций в ИТ-средах с большей безопасностью и масштабируемостью, чем это было возможно сделать на предприятиях когда-либо прежде. Однако вся ценность решения будет реализована, только если платформы смогут воспользоваться всеми его преимуществами. Что же можно делать с помощью pxGrid уже сегодня? Многое.

Все большее число поставщиков ИТ-решений и решений по безопасности уже встраивают поддержку pxGrid в свои решения. В настоящее время экосистема партнеров включает поставщиков лучших в отрасли решений для SIEM и защиты и угроз, ускорения работы сетей и приложений, облачной безопасности и безопасности IoT и многих других (см. рис. 9).

Рисунок 9. Экосистема партнеров pxGrid



В настоящее время партнеры используют решение pxGrid в следующих целях.

- Ускорение реагирования на угрозы за счет интеграции своих решений SIEM и защиты от угроз с модулем Identity Services Engine.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

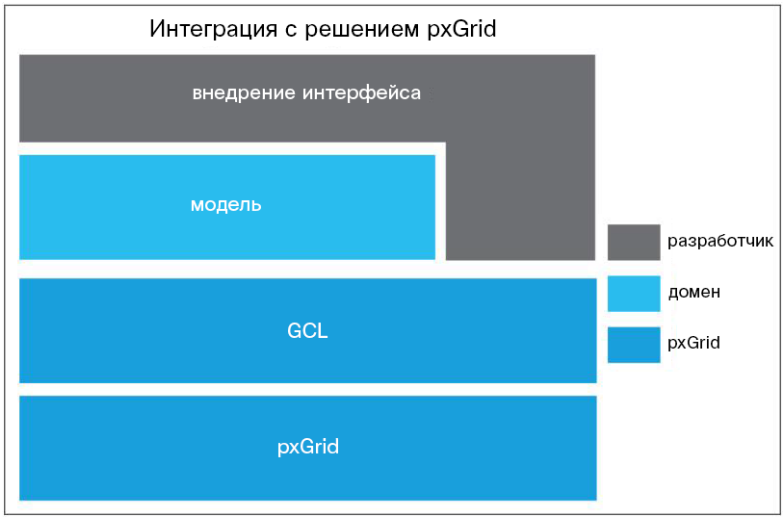
- Получение более подробных оценок сетевых уязвимостей с использованием информации об идентификаторе пользователя и его авторизации, способе доступа, оценке состояния безопасности и других контекстных данных.
- Упрощение сложных процессов IAM для обеспечения единого входа для нескольких облачных приложений.
- Присвоение привилегий для пользователей и сетей для мониторинга событий и аналитики и обеспечения облачной безопасности.
- И многое другое.

Интеграция с решением pxGrid

Cisco облегчает своим партнерам задачу интеграции их решений с pxGrid и получение преимуществ от двусторонней связи с другими платформами безопасности для предоставления их заказчикам новых возможностей для бизнеса. Мы предоставляем полный технический обзор и обучение по работе в среде Cisco DevNet, а также полный набор разработчика ПО (SDK) со всеми необходимыми библиотеками клиентов Java и C для разработчиков, чтобы они могли интегрировать свои узлы с сервером pxGrid. Этот набор включает полную тестовую среду, а также весь необходимый инструментарий для быстрой интеграции с pxGrid и начала публикации или подписки на темы и выполнения соответствующих действий.

На рис. 10 схематично представлена взаимосвязь между pxGrid, библиотекой GCL, моделью для конкретного домена и пользовательским кодом, написанным разработчиком. Эта модель, как мы уже упоминали ранее, состоит из сущностей и интерфейсов, общих для данного домена (например, безопасности). «Внедрение интерфейса» означает, как узел будет вести себя при внедрении конкретной функциональности. Разработчик расширяет интерфейсы этой модели и использует существующие классы в библиотеке GCL для внедрения этой функциональности.

Рисунок 10. Интеграция с решением pxGrid



Набор разработчика ПО можно загрузить по ссылке http://cisco.com/go/pxgrid. В состав набора входят:

- Технический обзор решения pxGrid, учебное пособие по работе с решением, руководство по конфигурации и тестированию и другая полезная документация.
- Библиотека GCL на языке Java и C, которую можно интегрировать с платформой, подключенной к pxGrid.
- Виртуальная машина Identity Services Engine и документацию по настройке, которую можно использовать как контроллер xGrid для тестирования внедрения клиентов pxGrid.
- Информация о получении доступа к размещенной в облаке тестовой среде pxGrid для тестирования вашей интеграции, в случае если вы решили не устанавливать локальный тестовый экземпляр.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация Cisco.

- Пример результатов тестового сеанса pxGrid, чтобы проверить способность системы получать данные pxGrid.
- Эмулятор сеанса RADIUS для создания данных сеанса подключения пользователя и устройства в реальном времени для тестирования систем, интегрированных с pxGrid.

Заключение

По мере того как сетевые угрозы становятся все сложнее и их все труднее обнаружить, для эффективного реагирования на угрозы все более важную роль начинает играть скорость. Недостаточно просто использовать разнообразные решения сетевой безопасности все вместе в одной среде или стараться объединить в своей работе вместе все многочисленные API-интерфейсы для разных платформ.

Cisco pxGrid предоставляет структуру для ускорения и автоматизации сложных процессов безопасности в современной среде. Любая платформа безопасности может обмениваться информацией с любой другой системой в среде в реальном времени с высокой степенью масштабируемости и с полным контролем, независимо от API-интерфейсов для конкретных платформ. Для поставщиков решений безопасности pxGrid предоставляет структуру, которую просто внедрить, чтобы увеличить возможности своих решений и обеспечить еще больше преимуществ для своих заказчиков.

Дополнительная информация

Для получения более подробной информации о решении Cisco pxGrid, а также загрузки набора разработчика ПО и начала использования решения прямо сегодня перейдите по ссылке http://www.cisco.com/go/pxgrid.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820, факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460, факс: +998 (71) 140 4465

© 2015 Cisco и (или) ее дочерние компании. Все права защищены. Cisco, логотип Cisco и Cisco Systems являются зарегистрированными товарными знаками или товарными знаками Cisco и (или) ее дочерних компаний в США и некоторых других странах. Все прочие товарные знаки, упомянутые в этом документе или на сайте, являются собственностью соответствующих владельцев. Использование слова «партнер» не означает наличия партнерских отношений компании Cisco с какой-либо другой компанией. (1002R)