Краткий обзор руководства по проектированию технологий межсетевых экранов и систем предотвращения вторжений

Обзор

В данном документе представлено краткое описание *руководства по проектированию технологий межсетевых экранов и систем предотвращения вторжений (IPS)*, а также приведены основные примеры использования этих технологий.

Утвержденные проекты Cisco предоставляют платформу для разработки систем на основе распространенных примеров использования или текущих приоритетов инженерных систем. Они включают в себя широкий набор технологий, функций и приложений для удовлетворения потребностей заказчиков. Инженеры Cisco полностью протестировали и документально оформили все рекомендованные Cisco архитектуры, чтобы обеспечить более быстрое, надежное и полностью предсказуемое развертывание.

В руководстве по проектированию технологий приводятся сведения о развертывании, информация об утвержденных продуктах и программном обеспечении, а также рекомендации по развертыванию межсетевых экранов и IPS. В нем подробно рассматриваются следующие примеры использования:

- применение политики безопасности для сетевого трафика между внутренней сетью, сетями демилитаризованной зоны и Интернетом;
- обеспечение отказоустойчивого доступа к Интернету;
- обнаружение и блокировка внешних атак на интернет-службы в демилитаризованной зоне;
- обнаружение вредоносного трафика во внутренних сетях.

Система безопасности на основе межсетевых экранов — неотъемлемая часть любого развертывания интернет-периметра. Она позволяет защитить информацию, обеспечивая при этом безопасность и надежность сетей, а также применение политик для поддержания производительности труда персонала. Там, где применяются отраслевые правила, межсетевые экраны играют решающую роль в соблюдении организацией установленных нормативов. Нормативные требования зависят от страны и отрасли. В данном документе не рассматриваются конкретные требования.

Круг вопросов

В *руководстве по проектированию технологий межсетевых экранов и систем предотвращения вторжений* рассматриваются службы обеспечения безопасности интернет-периметра — межсетевой экран и система предотвращения вторжений (IPS), защищающие корпоративный шлюз доступа к Интернету. Отказоустойчивость обеспечивается различными вариантами маршрутизации и подключения к сетям поставщиков услуг Интернета. В этом руководстве описывается создание и использование сегментов демилитаризованной зоны с интернет-сервисами, например для присутствия в Интернете. В руководстве по системе IPS рассматривается встроенное развертывание интернет-периметра и развертывание системы обнаружения вторжений на внутреннем уровне распределения, называемое также развертыванием *для контроля всех сетевых пакетов*.

Это руководство охватывает следующие технологии и продукты:

- межсетевые экраны нового поколения Cisco ASA серии 5500-X для защиты интернет-периметра и предотвращения вторжений;
- датчики Cisco IPS серии 4300 для предотвращения вторжений во внутреннюю сеть[1];
- демилитаризованная зона и средства коммутации вне локальной сети;
- интеграция указанных выше компонентов с инфраструктурой коммутации локальной сети.

Интернет-сервисы стали сегодня важной составляющей повседневной работы многих организаций. Обеспечение безопасного доступа к Интернету с предотвращением проникновения вредоносного контента в сеть организации необходимо для поддержания производительности труда персонала. Помимо клиентского доступа к Интернету, почти всем организациям требуется присутствие в глобальной сети для предоставления партнерам и клиентам информации о себе. Размещенная в Интернете корпоративная информация подвержена риску в результате атаки на общедоступные службы. Чтобы организация могла эффективно использовать ресурсы Интернета, необходимо найти решения для всех этих проблем.

Примеры использования технологии

Интернет-периметр — это точки подключения сети организации к Интернету. Он представляет собой границу между общедоступным Интернетом и частными ресурсами, расположенными в сети организации. Программные черви, вирусы и несанкционированный доступ из бот-сетей создают существенные угрозы работе сети, ее доступности и безопасности данных. Кроме того, подключение организации к Интернету может привести к снижению производительности труда персонала и утечке конфиденциальной информации.

Действующие через Интернет злоумышленники представляют угрозу для сетевых инфраструктур и информационных ресурсов организации. Большинство подключенных к Интернету сетей подвержены постоянным угрозам со стороны программных червей, вирусов и целенаправленных атак. Организации должны бдительно защищать свои сети, пользовательские данные и информацию о заказчиках. Кроме того, большинство сетевых адресов необходимо преобразовывать в адреса, по которым осуществляется маршрутизация в Интернете, и эту функцию целесообразно выполнять с помощью межсетевого экрана.

Средства обеспечения сетевой безопасности на межсетевом экране должны гарантировать защиту информационных ресурсов организации от перехвата и фальсификации и предотвращать нарушение безопасности узлов программными червями, вирусами и бот-сетями, потребляющими ресурсы. Кроме того, политика межсетевого экрана должна устанавливать оптимальный баланс между безопасностью и доступом к интернет-приложениям и не препятствовать получению данных от бизнес-партнеров по VPN-соединениям экстрасети.

[1] Обратите внимание, что после публикации этого руководства корпорация Cisco добавила в свой портфель дополнительные средства IPS, в частности систему предотвращения вторжений, интегрированную с межсетевыми экранами нового поколения, и систему предотвращения вторжений нового поколения Sourcefire.

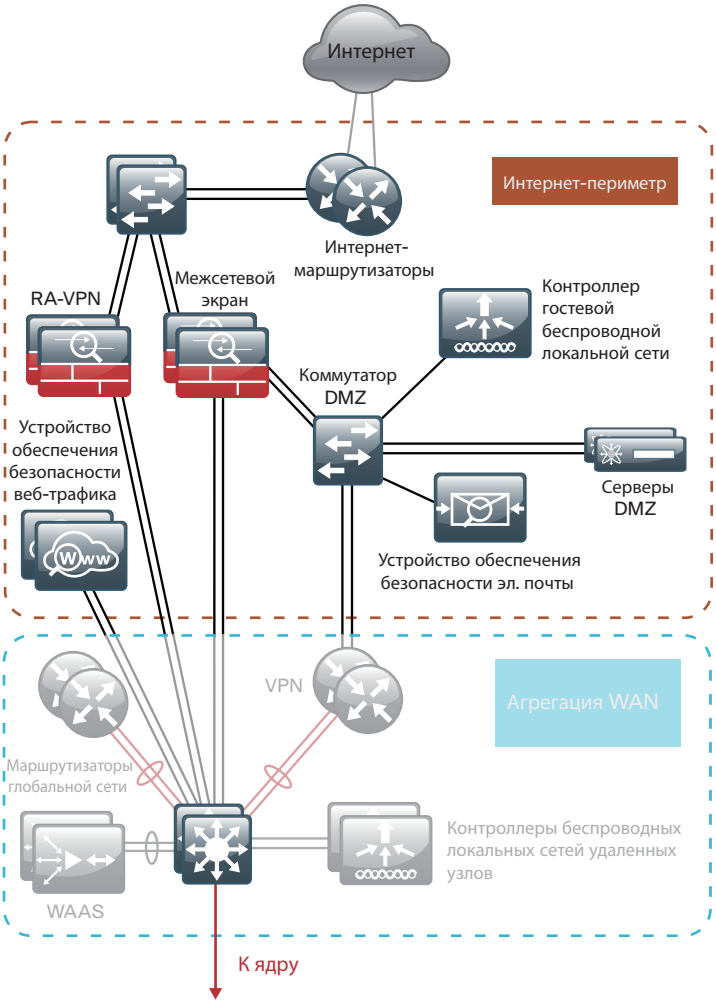
Сценарии использования

Пример использования: применение политики безопасности для сетевого трафика между внутренней сетью, сетями демилитаризованной зоны и Интернетом

Сети головного офиса и удаленных площадок считаются внутренними зонами, а Интернет – внешней зоной. Сети демилитаризованной зоны, настраиваемые для других услуг на интернет-периметре, находятся между внутренней и внешней зонами.

В данном руководстве по проектированию рассматривается использование следующих возможностей обеспечения безопасности.

- **Скрытие адресов внутренней сети с помощью преобразования сетевых адресов (NAT).** Большинство организаций используют частные адреса (согласно документу RFC 1918), по которым маршрутизация в Интернете невозможна. Поэтому межсетевой экран должен преобразовывать частные адреса во внешние, по которым осуществляется маршрутизация в Интернете.
- **Разрешение доступа из внутренней сети к Интернету**. Из внутренней зоны весь трафик (за исключением отдельных, явно запрещенных категорий) направляется в Интернет. Межсетевой экран проверяет каждый сеанс и неявно разрешает поступление соответствующего обратного трафика во внутреннюю зону.
- **Разрешение доступа из внутренней сети к сетям демилитаризованной зоны.** Из внутренней зоны весь трафик (за исключением отдельных, явно запрещенных категорий) направляется в сети демилитаризованной зоны. Межсетевой экран проверяет каждый сеанс и неявно разрешает поступление соответствующего обратного трафика во внутреннюю зону.



- **Разрешение доступа из Интернета к сетям демилитаризованной зоны**. Из Интернета в сети демилитаризованной зоны направляется трафик только определенных, явно разрешенных типов. Межсетевой экран проверяет каждый сеанс и неявно разрешает поступление соответствующего обратного трафика в Интернет.
- **Блокировка остального трафика.** Трафик всех других типов неявно блокируется.

Пример использования: обеспечение отказоустойчивого доступа к Интернету

Хорошо спроектированная сеть интернет-периметра должна быть устойчива к наиболее часто возникающим типам отказов. На одной площадке такую устойчивость можно обеспечить с помощью пары межсетевых экранов, использующих статическую маршрутизацию в Интернет по умолчанию.

В данном руководстве по проектированию рассматривается использование следующих сетевых возможностей.

- В случае отказа оборудования осуществляется переключение с сохранением состояния между активным и резервным устройствами отказоустойчивой пары межсетевых экранов.
- Автоматическое перенаправление интернет-трафика с канала основного поставщика услуг Интернета на канал резервного поставщика с использованием мониторинга активных датчиков, имитирующих пользовательский трафик в Интернет.

Пример использования: обнаружение и блокировка внешних атак на интернет-службы в демилитаризованной зоне

Мониторинг и блокировка сетевых атак с помощью IPS повышает надежность и эффективность присутствия организации в глобальной сети, а также поддерживает доступность ее ресурсов для партнеров и клиентов.

В данном руководстве по проектированию рассматривается использование следующих возможностей обеспечения безопасности.

- **Обнаружение и отражение сетевых атак.** Система IPS выполняет глубокий анализ пакетов сетевого трафика для сопоставления с известными сигнатурами атак и блокировки вредоносного трафика.
- **Фильтры на основе репутации.** Система IPS определяет, связан ли источник атаки с известными опасными группами.
- **Защита от совершенно новых атак.** Система IPS распознает нормальное поведение сети и оповещает оператора при обнаружении аномальных действий.

Пример использования: обнаружение вредоносного трафика во внутренних сетях

Мониторинг и обнаружение программных червей, вирусов и другого вредоносного ПО с помощью системы IPS, используемой для обнаружения вторжений, имеют большое значение для поддержания эффективной работы сети.

В данном руководстве по проектированию рассматривается использование следующих возможностей обеспечения безопасности.

- **Обнаружение сетевых атак и оповещение о них.** Система IPS выполняет глубокий анализ пакетов сетевого трафика для сопоставления с известными сигнатурами атак и блокировки вредоносного трафика.
- **Фильтры на основе репутации.** Система IPS определяет, связан ли источник атаки с известными опасными группами.
- **Защита от совершенно новых атак.** Система IPS распознает нормальное поведение сети и оповещает оператора при обнаружении аномальных действий.

Обзор архитектуры

Руководство по проектированию межсетевых экранов и систем предотвращения вторжений является компонентом более крупного проекта создания интернет-периметра, в котором используется модульная структура для разделения интернет-периметра на функциональные блоки по услугам. Применяя модульное проектирование, организация может развертывать сервисы в соответствии с требованиями.

Ниже перечислены функциональные блоки, входящие в проект интернет-периметра.

- **Межсетевой экран.** Управляет доступом к разным сегментам интернет-периметра извне и изнутри, а также предоставляет ряд других сервисов, в частности преобразование сетевых адресов (NAT) и создание демилитаризованной зоны.
- **Предотвращение вторжений.** Проверяет трафик, проходящий через интернет-периметр, и обнаруживает злонамеренное поведение.
- **VPN удаленного доступа.** Обеспечивает безопасный постоянный доступ к ресурсам независимо от места и времени подключения пользователя.
- **Безопасность электронной почты**. Обеспечивает фильтрацию спама и вредоносного ПО для управления рисками, связанными с электронной почтой.
- **Безопасность веб-трафика**. Осуществляет контроль допустимости использования, управляя растущими рисками, связанными с просмотром веб-сайтов пользователями.

Варианты модульной структуры в основном различаются масштабом, производительностью и устойчивостью. Каждый модуль проекта интернет-периметра создается независимо от других, поэтому можно комбинировать разные компоненты для обеспечения оптимального соответствия потребностям бизнеса.

Щелкните здесь, чтобы открыть полное 106-страничное *руководство по проектированию технологий межсетевых экранов и систем предотвращения вторжений* на английском языке.

Документы по теме

В *руководстве по проектированию VPN удаленного доступа* и *руководстве по проектированию средств удаленного мобильного доступа* рассматривается выделение сетевых ресурсов для предоставления услуг удаленного доступа. Развертывание включает в себя внедрение доступа через VPN в качестве компонента межсетевых экранов интернет-периметра, а также обеспечение возможности реализации сервисов VPN удаленного доступа на отдельных выделенных устройствах.

В *руководстве по проектированию системы безопасности веб-трафика с помощью Cisco WSA* рассматривается развертывание устройства Cisco Web Security Appliance для клиентов, имеющих доступ к Интернету. Это устройство защищает от вредоносных программ и вирусов, а также осуществляет контроль допустимости использования, предоставляя доступ только к разрешенным сайтам.

В *руководстве по проектированию системы безопасности облачных сервисов от интернет-угроз с помощью Cisco ASA* рассматривается развертывание решения Cisco Cloud Web Security для клиентов, имеющих доступ к Интернету. Это устройство защищает от вредоносных программ и вирусов, а также осуществляет контроль допустимости использования, предоставляя доступ только к разрешенным сайтам.

В *руководстве по проектированию системы защиты электронной почты с помощью Cisco ESA* рассматривается развертывание устройства Cisco Email Security Appliance для обеспечения безопасности корпоративной системы электронной почты. Цель развертывания такого устройства – проверка входящих сообщений на наличие спама и вредоносного контента. В этом руководстве также рассматривается добавление к межсетевому экрану Интернета демилитаризованной зоны электронной почты для повышения общей безопасности.

C07-730895-00 02/14