Безопасность беспроводных сетей благодаря технологии защиты от вторжений WatchGuard WIPS

Введение

Повсеместное распространение Wi-Fi создало удобные условия для отслеживания, кражи данных и заражения систем ничего не подозревающих пользователей. На момент подготовки этого документа, в YouTube выложены более 300 000 видеороликов, в которых объясняется, как получить доступ к устройствам пользователей через Wi-Fi с помощью простых и одновременно мощных инструментов, легко находимых в интернете. Вполне очевидно, что люба я подобная активность – недопустима в корпоративных сетях Wi-Fi. В этом обзоре рассказано, как решить насущную проблему с помощью технологии защиты от вторжений для беспроводных сетей WatchGuard WIPS. Технология WIPS применима к точкам доступа WatchGuard с возможностью облачного управления с платформой CloudGuard Wi-Fi Cloud.

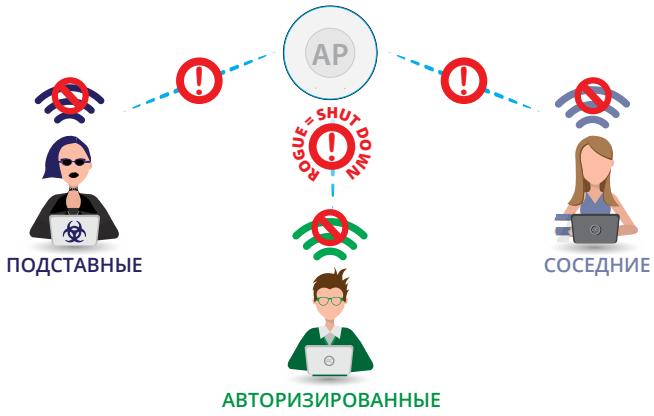
Существующие на рынке решения не выполняют свою задачу

Решения конкурентов в основном ориентированы на обнаружение, а не на предотвращение угроз, из-за риска возможного вмешательства в работу близлежащих сетей Wi-Fi. Также для существующих решений характерно большое количество ложных срабатываний, которые, со временем, полностью игнорируются администраторами, оставляя компании незащищенными. WIPS -технологии конкурентов требуют больших усилий в администрировании и зачастую не обеспечивают надлежащего уровня обнаружения подставных точек доступа. Используя такие решения, компании ошибочно ощущают себя в безопасности, поскольку их сети на самом деле остаются уязвимыми для действий злоумышленников.

В свою очередь, WatchGuard WIPS обеспечивают защиту корпоративного уровня с минимальными затратами на администрирование для Wi-Fi сетей предприятий, требующих соблюдения таких стандартов соответствия, как PCI, HIPAA и Sarbanes Oxley. WatchGuard использует запатентованную технологию Marker Packet для обеспечения наиболее надежной защиты WIPS в отрасли с наименьшим количеством ложных срабатываний, предоставляя полное превосходство в Wi-Fi-пространстве.

Как включить и развернуть защиту WIPS WatchGuard?

WatchGuard WIPS поддерживается всеми точками доступа с возможностью облачного управления при использовании платформы CloudGuard Wi-Fi Cloud с активными лицензиями CloudGuard Wi-Fi Cloud. Развертывание WIPS можно выполнить двумя способами:



1. С использованием выделенных сенсоров WIPS (рекомендуемый)

Этот вариант включает настройку точек доступа с возможностью облачного управления в качестве выделенных сенсоров WIPS. Работая таким образом, точка доступа производит обработку клиентского трафика, проходящего через другие точки, и не используется для подключения клиентов к сети Wi-Fi. Как правило, на каждые 4 точки доступа нужно предусмотреть 1 выделенный сенсор WIPS. Такая модель развертывания обеспечивает наивысший уровень безопасности, благодаря наличию выделенных сенсоров WIPS. Они непрерывно сканируют Wi-Fi-пространство и предотвращают применение злоумышленниками незащищенных интервалов времени, возникающих в режиме использования общего времени вещания точек доступа и системы WIPS.

2. С использованием общего времени вещания точек доступа и системы WIPS

Все точки доступа с возможностью облачного управления могут быть настроены на использование общего времени вещания (в процентах) для обработки клиентского трафика и WIPS-сканирования. В этом режиме одна точка доступа действует одновременно как стандартная точка, и как сенсор WIPS. Вместе с тем, функция пакетной инъекции через Wi-Fi становится недоступной.

Про WatchGuard

WatchGuard – это почти миллион интегрированных многофункциональных систем управления угрозами по всему миру. Характерные «красные коробки» WatchGuard – это самые умные, быстрые и продвинутые устройства защиты в отрасли, в которых все механизмы сканирования работают с недоступной прочим вендорам производительностью. Штаб-квартира WatchGuard расположена в Сиэтле (США). Компания имеет офисы в Северной Америке, Европе, Азиатско-Тихоокеанском регионе и Латинской Америке.

Больше информации: www.watchguard.com, www.watchguard.com/secplicity (блог об информационной безопасности)

Сравнительная характеристика вариантов развертывания WIPS

Сканирование выделенными сенсорами	Сканирование в фоновом режиме (с общим временем вещания)
Время вещания используется для двухдиапазонного циклического сканирования (каждый канал сканируется в течение 100 мс с интервалом в 5 секунд)	Время вещания является общим для работы точек доступа с двухдиапазонным сканированием в фоновом режиме (ненагруженный трафиком канал сканируется в течение 100 мс с интервалом в 2 минуты)
Моментальное обнаружение угроз на всех каналах	Обнаружение угроз в ненагруженном трафиком канале может занять время (по-прежнему лучшие показатели в отрасли для обнаружения подставных точек доступа, поскольку инъекции Marker Packets™ осуществляются во время посещения канала)
Предотвращение угроз через Wi-Fi и через проводные сети. Обеспечивает блокировку всех видов угроз	Предотвращение угроз только через проводные сети (блокировка подставных точек доступа с помощью tarpitting)
Основное применение: для компаний с высокими требованиями к безопасности/соответствию (финансовые и государственные учреждения, объекты здравоохранения и образования, ИТ-компании и т.д.)	Основное применение: для соблюдения требований стандарта PCI для розничной торговли

Принцип работы WIPS WatchGuard

Инъекция пакетов по проводной сети

В WIPS используется технология инъекции пакетов Marker Packets в проводную сеть системы точек доступа с WIPS-сенсорами. Эти пакеты передаются в Wi-Fi-пространство точками доступа, подключенными к контролируемой проводной сети, и, далее, принимаются WIPS-сенсорами по Wi-Fi. Точки доступа могут находиться в подсетях или быть подключенными к магистральному порту управляемого коммутатора нескольких подсетей.

Преимущества такого метода:

- Не требует непосредственного взаимодействия с коммутаторами сети.
- Не требует создания изначальных или дополнительных конфигураций для успешной работы.
- Позволяет быстро обнаруживать подсоединение новых точек доступа, независимо от размера сети, поскольку работает одновременно в каждой локальной подсети.
- Ничтожно малый объем трафика, создаваемый в результате инъекции пакетов (менее 0,1% от пропускной способности LAN-порта).
- Отсутствие ложных срабатываний благодаря точному разграничению внешних и подставных точек доступа.

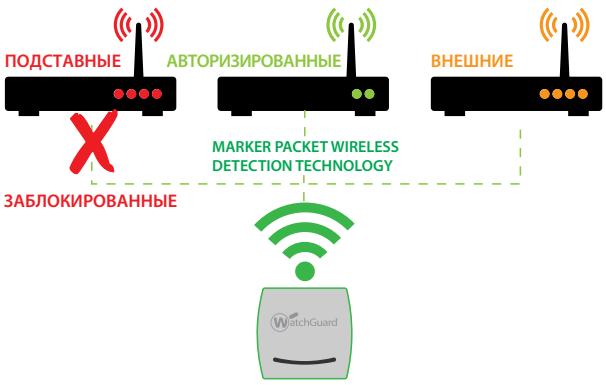
Инъекция пакетов по Wi-Fi

При обнаружении WIPS-сенсором клиента, связанного с точкой доступа, он отправляет пакеты с уникальным идентификатором (Marker Packets) по Wi-Fi на потенциальную подставную точку доступа, адресованные на IP-адрес известного узла проводной сети. Эти пакеты совмещаются с пакетами соединения клиента с потенциальной подставной точкой доступа. Если какой-либо из этих пакетов принимается целевым узлом, точка доступа считается подключенной к контролируемой проводной сети.

Уникальное отличие – автоматическая классификация точек доступа

Одновременно самый простой и удобный способ классификации точек доступа заключается в обнаружении сетевых подключений. Этот тип автоматической классификации не требует малонадежных или неуправляемых классификационных подписей на основе SSID, названия компании-поставщика, уровня мощности, настройки шифрования или канала. Все, что необходимо в этом случае — это надежное сетевое подключение и доступ к желаемым VLAN.

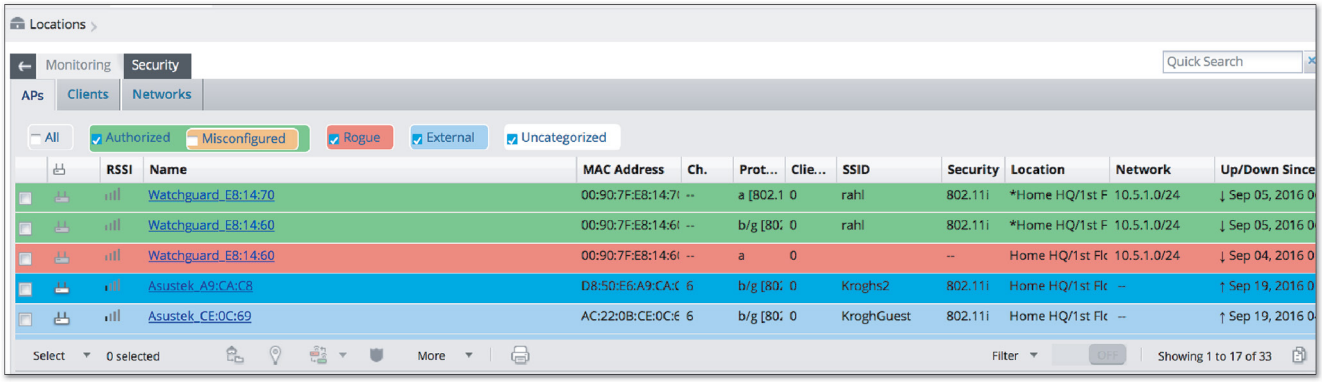
WIPS WatchGuard — единственная система на рынке, обеспечивающая автоматическую классификацию точек доступа по подключению к сети, благодаря использованию уникальной технологии Marker Packet, которая точно определяет наличие подключения к сети любых типов точек доступа.



Автоматическая классификация точек доступа позволяет разделить их на 3 категории:

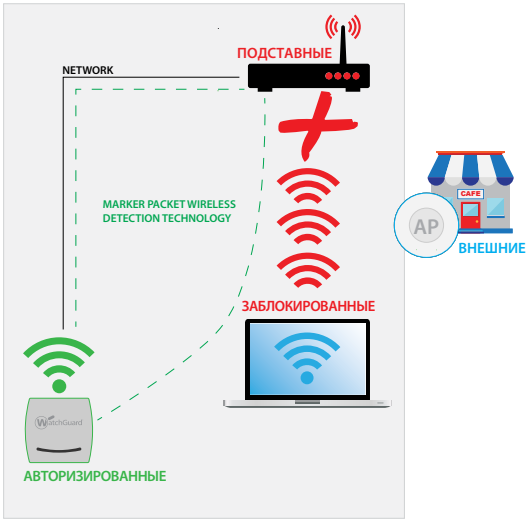
- **Авторизованные** – точки доступа в проводной сети под управлением администратора.
- **Внешние** – неуправляемые точки доступа в близлежащем Wi-Fi-пространстве, которые не подключены к контролируемой проводной сети.
- **Подставные** – неавторизованные точки доступа, созданные в проводной сети без ведома администратора.

Автоматическая классификация точек доступа в WIPS WatchGuard



Преимущества WatchGuard WIPS:

- Активное предотвращение, а не только обнаружение угроз.
- Технология Marker Packet.
- Точная классификация устройств с минимальным на рынке количеством ложных срабатываний.
- Обнаружение, определение и предотвращение доступа через NAT-защищенные, зашифрованные и виртуальные точки доступа.
- Обнаружение и блокировка неавторизованных клиентов.
- Автоматическое реагирование без ущерба для работы соседних сетей.
- Предотвращение угроз по нескольким каналам с помощью одного сенсора.
- Блокировка различных типов DoS-атак по 802.11.
- Реализация политик беспроводной связи для каждого отдельного местоположения VLAN, SSID.
- Поддержка Multi-VLAN (до 100 VLAN на один сенсор).
- Работа системы не основана на использовании таблиц CAM или SNMP.
- Список отслеживания мобильных устройств.
- Режим автономного датчика (беспрерывная защита).
- Удаленный захват сетевых пакетов (R-PCAP) с любого сенсора.
- Наиболее точное определение местоположения с использованием одного сенсора.
- Возможность управления тысячами сенсоров с одной консоли.
- Автоматизированные отчеты о безопасности и соответствии.
- Простота использования и развертывания, а также — низкая совокупная стоимость обладания и администрирования.
- Превышает требования DoD 8100.2 WIDS.
- Беспрерывное соблюдение политики «no Wi-Fi» в проводных VLAN сетях.



5 недостатков конкурирующих решений WIPS

Все системы WIPS сильно различны и, чтобы проиллюстрировать это, следует рассмотреть 5 основных недостатков, встречающихся в большинстве конкурирующих решений WIPS:

1. Обнаружение подставных точек доступа в конкурирующих WIPS

Подставная точка доступа может быть определена как любая неавторизованная и подключенная к контролируемой сети. Подставные точки доступа представляют угрозу, поскольку они позволяютосуществлятьнесанкционированныйбеспроводнойдоступ к частной сети. Неавторизованные точки доступа могут появляться в сети в результате непреднамеренных действий сотрудников или же – в результате вредоносных действий инсайдеров. Многие конкурирующие решения WIPS используют неполноценный метод обнаружения подставных точек доступа в локальной сети, суть которого заключается в объявлении любой точки доступа вне списка авторизованных – в качестве неавторизованной.

Про WatchGuard

WatchGuard – это почти миллион интегрированных многофункциональных систем управления угрозами по всему миру. Характерные «красные коробки» WatchGuard – это самые умные, быстрые и продвинутые устройства защиты в отрасли, в которых все механизмы сканирования работают с недоступной прочим вендорам производительностью. Штаб-квартира WatchGuard расположена в Сиэтле (США). Компания имеет офисы в Северной Америке, Европе, Азиатско-Тихоокеанском регионе и Латинской Америке.

Больше информации: www.watchguard.com, www.watchguard.com/secplicity (блог об информационной безопасности)

В таком подходе существует ряд недостатков:

- **Ложные срабатывания:** предупреждения безопасности выдаются даже в случае появления в Wi-Fi-пространстве неавторизованной точки доступа, не имеющей подключения к контролируемой проводной сети (то есть, не представляющей угрозы безопасности).
- **Необходимость ручного вмешательства:** системный администратор должен самостоятельно изучить неавторизованные точки доступа и решить, какие из них действительно являются подставными точками доступа, а какие – просто внешними точками доступа соседней сети.
- **Отсутствие возможности мгновенного автоматического реагирования:** поскольку случайное или массовое блокирование точек доступа соседних сетей является крайне нежелательным методом, мгновенная и автоматическая блокировка подставных точек доступа невозможна при таком подходе.

2. Определение точек доступа на основе подписей

Многие конкурирующие WIPS пытаются классифицировать точки доступа на основе пользовательских классификационных подписей. Для их определения может использоваться множество параметров точек доступа, включая SSID, название компании-поставщика, уровень мощности, настройки шифрования или каналов. Наличие подключения точки доступа к сети может даже не являться фактором в правилах классификации. Этот подход имеет несколько недостатков:

- **Обслуживание подписей:** значительные трудозатраты при создании классификационных подписей. Их необходимо регулярно обновлять, например, в случае смены SSID в настройках WLAN известной точки доступа соседской сети.
- **Необходимость постоянного ручного вмешательства:** конфигурации новых точек доступа, появляющихся в сети, могут не точно соответствовать заданным подписям, что вызывает необходимость определения типа точки вручную.
- **Пропущенные угрозы:** этот подход часто пропускает настоящие угрозы. Например, в случае использования классификационной подписи «SSID = freewifi AND signal strength = Low» подставная точка доступа с низкой мощностью передачи и SSID «freewifi» будет опознана как нормальная точка доступа соседней сети.

3. Поиск по таблице MAC-адресов

Этот метод сравнивает MAC-адреса видимых беспроводных устройств с MAC-адресами, зарегистрированными портами коммутаторов контролируемой проводной сети. Если через Wi-Fi и по проводной сети обнаруживается общий MAC-адрес, то устройство с этим MAC-адресом определяется как подключенное к контролируемой проводной сети.

При наличии точки доступа, работающей в режиме моста, определение ее принадлежности возможно только после подключения клиента. После подключения, MAC-адрес клиента регистрируется портом коммутатора, к которому подключена эта точка доступа. Сбор MAC-адресов, зарегистрированных портами управляемых коммутаторов в сети, выполняется путем опроса CAM-таблиц каждого коммутатора по протоколу SNMP.

Однако это связано с несколькими недостатками:

- Метод можно определить как интрузивный по отношению к инфраструктуре коммутаторов. Для возможности опроса таблиц MAC-адресов коммутаторов требуется занесение информации о коммутаторах в систему WIPS. Возможны проблемы совместимости с коммутаторами от разных поставщиков.
- Опрос таблиц MAC-адресов всех управляемых коммутаторов в сети является трудоемкой задачей, особенно для крупных сетей с сотнями коммутаторов. Таким образом, обнаружение сетевых подключений в крупных сетях при таком подходе может происходить через раз и зависеть от фактора случайности.
- MAC-адрес клиента исчезает из таблицы MAC-адресов при переходе клиента в неактивное состояние, поэтому данный метод может давать успешный результат только в случае, если клиент непосредственно подключен к подставной точке доступа во время опроса таблицы MAC-адресов (обычно происходящего через заданный интервал времени).

4. Пассивная корреляция MAC-адресов

Этот подход пытается преодолеть недостатки поиска с использованием таблицы MAC-адресов. В этом подходе WIPS-сенсор пассивно прослушивает проводной интерфейс для обнаружения активных MAC-адресов подсети. MAC-адреса, обнаруженные таким образом, используются для корреляции MAC-адресов проводной/беспроводной сети. Однако даже этот подход имеет недостаток, который заключается в том, что точки доступа, не подключенные к контролируемой сети (например, точки доступа соседней сети) могут быть ошибочно определены как подключенные. Это может произойти, когда клиенты переключаются между точками доступа.

5. Отслеживание по Wi-Fi

В этом подходе, при обнаружении WIPS-сенсором точки доступа, производится подключение к ней по Wi-Fi. Затем WIPS-сенсор пингует или отправляет пакет на известный узел проводной сети через потенциальную подставную точку доступа, чтобы попытаться определить, подключена ли она к контролируемой проводной сети. Использование активного подключения к точкам доступа имеет ограничения, поскольку, для создания соединений уровней L2 и L3 между точками доступа, требуется достаточно много времени (до 5 секунд). В течение этого времени WIPS-сенсор занят каналом точки доступа и не может выполнять функцию сканирования. Таким образом, при наличии большого количества потенциальных подставных точек доступа, видимых WIPS-сенсором, подключение ко всем точкам будет выполняться в течение довольно длительного времени, что приведет к большой задержке в обнаружении новых соединений. Кроме того, этот метод не позволяет обнаружить подставные точки доступа с нестандартными настройками, например, с измененным списком MAC-адресов авторизованных клиентов в Wi-Fi интерфейсе, что может помешать WIPS-сенсору активно связываться с потенциальной подставной точкой доступа.