Вопрос:

Как Монитор трафика Уровня 4 блокирует трафик, если это только получает отраженный трафик?

Среда:

Монитор трафика уровня 4 - L4TM, настроенный для блокирования подозрительного трафика

Решение:

Cisco Web Security Appliance (WSA) имеет встроенный сервис Монитора трафика уровня 4 (L4TM), который может заблокировать подозрительные сеансы через все сетевые порты (TCP/UDP 0-65535).

Чтобы быть в состоянии контролировать или заблокировать эти сеансы, трафик должен быть перенаправлен к WSA, любому при помощи TAP (порт Доступа для тестирования) устройство, или путем настройки порта зеркального отражения на сетевых устройствах (Порты SPAN на устройствах Cisco). L4TM встроенный режим еще не поддерживается.

Даже при том, что трафик только отражен (скопированный) от исходных сеансов до устройства, WSA может все еще заблокировать подозрительный трафик или отдыхом сеанса TCP или передачей сообщений "недостижимого узла" ICMP для сеансов UDP.

Для сеансов TCP

Когда WSA L4TM получает пакет к или от сервера, и трафик совпадает с Блочным Действием, L4TM передаст RST TCP (сброс) дейтаграмма клиенту или серверу в зависимости от сценария. Дейтаграмма RST TCP является просто обычным пакетом с набором флага TCP RST к 1.

Получатель RST сначала проверяет его, затем изменяет состояние. Если получатель был в СЛУШАТЬ состоянии, он игнорирует его. Если получатель был в ПОЛУЧЕННОМ ОТ SYN состоянии и ранее был в СЛУШАТЬ состоянии, то получатель возвращается к СЛУШАТЬ состоянию, иначе получатель прерывает соединение и переходит к Закрытому состоянию. Если получатель был в каком-либо другом состоянии, он прерывает соединение и советует пользователю и переходит к Закрытому состоянию.

Существует два случая для рассмотрения (в обоих случаях, пользователи/клиенты находятся позади межсетевого экрана):

Когда подозрительный пакет приходит не из межсетевого экрана к клиенту во внутренней сети, сначала каждый. RST будет передаваться серверу, и в этом случае это доберется до межсетевого экрана, который не будет обычно передавать RST, но это завершит сеанс, поскольку это будет полагать, что RST фактически прибыл от клиента. В этом случае source IP RST будет поддельным IP клиента. Клиент завершит сеанс.

Когда пакет прибывает от клиента во внутреннюю сеть и переходит к внешнему серверу (вне межсетевого экрана), второй случай был бы. RST тогда передается Клиенту, и source IP RST будет поддельным IP сервера.

Для сеансов UDP

Подобное поведение выполнено WSA, когда подозрительный трафик от сеанса UDP, но вместо того, чтобы передать RST TCP, L4TM передаст Сообщения ICMP Host Unreachable (ICMP узел недоступен) (тип ICMP 3 кода 1) или клиенту или серверу. Однако нет IP-спуфинга в этих случаях, поскольку сообщение ICMP сообщает, что хост недостижим, таким образом, это не может передавать пакеты. Source IP в этом случае будет IP WSA.

Эти RST и пакеты ICMP передаются от WSA использование таблицы маршрутизации данных, или через M1, P1 или через P2, в зависимости от развертываний.