Содержание

Вопрос

Как вы блокируете неизвестные приложения на Cisco Web Security Appliance?

Примечание: Эта статья Базы Знаний ссылается на программное обеспечение, которое не поддерживается Cisco. Информация предоставлена как любезность для вашего удобства. Для дальнейшей поддержки свяжитесь с поставщиком программного обеспечения.

1. Первая защита должна использовать строки "Клиента User Agent" для блокирования таких приложений. Так как мы не знаем все user-agent для них приложение, необходимо будет искать их на ссылках ниже.
   Мы можем добавить "User-Agent" при ***веб-Менеджере безопасности > Политика доступа > Протоколы и*** столбец ***Клиентов User Agent*** <для требуемой политики доступа>.-> Добавляют строку агента пользователя под ***'Блочными Пользовательскими Клиентами User Agent':*** (один на линию).

2. Если Средства управления за видимостью приложения (AVC) включены *(В соответствии с> Security GUI Сервисы> веб-Репутация и Антивирус)*, то мы можем блокировать доступ на основе типов приложения как Прокси, Общий файл, интернет-утилиты. Мы можем сделать это под ***веб-*** *столбцом* ***Security Manager> Access Policies> 'Applications'*** *<для требуемой политики доступа>*.
3. Если Клиент User Agent не существует, можно попытаться добавить тип MIME (Пример*:* разрядные приложения потоков).
   Мы можем добавить типы "MIME" *под* ***веб-*** ***Security Manager> Web Access Policies> Objects*** *<для требуемой политики доступа>*.---> Добавляют в типе объекта/mime в **'Блочном Пользовательском** разделе**' Типов MIME** как application/x-bittorrent (один на линию).

4. Гарантируйте, что категории как Предотвращение Фильтра, Незаконная деятельность заблокирована в политике доступа. Если некоторые приложения используют известные URL или IP-адреса для их соединений, то мы можем заблокировать их связанные предопределенные категории URL или настроить их в заблокированной пользовательской категории URL с помощью их IP-адреса, FQDN или regex, совпадающего с доменами. Мы можем сделать это *под* ***веб-*** столбцом ***Security Manager> Access Policies> "URL Categories"***.
5. Некоторые приложения могут использовать метод ПОДКЛЮЧЕНИЯ HTTP для соединения с другими портами. Только позвольте известные порты или определенные порты, необходимые в вашей среде в доменах конфигурации портов ПОДКЛЮЧЕНИЯ HTTP.
   ПОДКЛЮЧЕНИЕ HTTP может быть настроено *при* ***веб-Менеджере***

безопасности > Политика доступа > Протоколы и *столбец* ***Клиентов User Agent*** *<для требуемой политики доступа>.*-> Добавляют разрешенные порты под **'портами ПОДКЛЮЧЕНИЯ HTTP':**

6. Для приложений, где вы только знаете о IP - адресах назначения, к которым обращаются, можно использовать функцию Монитора трафика L4 для блокирования доступа для заинтересованного IP-адреса. Мы можем добавить целевой IPs *при* ***веб-Менеджере безопасности > Монитор трафика L4 > Дополнительные Подозреваемые Вредоносные Адреса.***

Если вы не знаете, какой 'Клиент User Agent' или 'Тип Mime' используются определенными приложениями, то можно сделать любой из следующих для обнаружения этой информации:

- Выполните захват пакета с WireShark (Эфирным) на машине клиента и фильтре для протокола 'http'.
- Выполните перехват на WSA (под "Поддержкой и Справкой"> "Захват пакета"), фильтруемый на IP-адресе клиента.

Список клиентов User Agent:
==========
http://www.user-agents.org/

Список типов MIME:
==========
http://www.webmaster-toolkit.com/mime-types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx