Содержание

Вопрос:

Как делает Cisco Web Security Appliance Трафик Skype маркера (WSA)?

Среда: Cisco WSA, Skype

Skype является составляющей собственность сетью (VoIP) интернет-телефонии. Skype прежде всего действует в качестве одноранговой программы, таким образом он непосредственно не связывается с центральным сервером для работы. Skype может быть особенно трудно заблокировать, поскольку он попытается соединиться многими другими способами.

Skype соединяется в следующем порядке предпочтения:

1. Прямые пакеты UDP к другим узлам с помощью номеров случайного порта
2. Прямые пакеты TCP к другим узлам с помощью номеров случайного порта
3. Прямые пакеты TCP к другим узлам с помощью порта 80 и/или порта 443
4. Туннелируемые пакеты через веб - прокси с помощью HTTP СОЕДИНЯЮТСЯ с портом 443

Когда развернуто в явном прокси - окружении, методы 1-3 никогда не будут передаваться Cisco WSA. Для блокирования Skype он должен сначала быть заблокирован от другого местоположения в сети. Шаги 1-3 Skype могут быть заблокированы с помощью:

- Межсетевой экран: Используйте NBAR для блокирования версии 1 Skype. Дополнительные сведения доступны в http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Cisco IPS (ASA): Cisco ASA может потенциально обнаружить и заблокировать Skype через подписи.

Когда Skype переключается на использование явного прокси, Skype сознательно не предоставляет клиентской подробной информации в Запросе соединения HTTP (никакая строка user-agent ни один). Это мешает дифференцироваться между Skype и допустимым Запросом соединения. Skype будет всегда соединяться с портом 443, и адресом назначения (DA) всегда является IP-адрес.

Пример:

СОЕДИНИТЕСЬ 10.129.88.111:443 HTTP/1.0
Прокси - подключение: поддержка активности

Следующая Политика доступа заблокирует любые Запросы соединения через WSA, который совпадает с IP-адресами и портом 443. Это будет совпадать со всем трафиком Skype. Однако программы не-Skype, пытающиеся туннелировать к IP-адресу на порту 443,

будут заблокированы также.

Блокирование Skype - Явная среда с отключенным Прокси HTTPS

Создайте пользовательскую категорию URL для соответствия с IP и трафиком порта 443:

1. Перейдите "Менеджеру безопасности"-> "Пользовательские Категории URL"->, "Добавляет Пользовательская Категория".
2. Заполните "Название категории" и расширьтесь "Усовершенствованный".
3. Используйте" [0-9] + \. [0-9] + \. [0-9] + \. [0-9] +" в окне Regular Expression.

Заставьте эту категорию запрещать в Политике доступа:

1. Перейдите "веб-Менеджеру безопасности"-> "Политика доступа".
2. Щелкните по ссылке под столбцом "URL Categories" для соответствующей группы политик.
3. В "Пользовательском разделе" фильтрации Категории URL выберите "Block" для новой категории Skype.
4. Отправьте и передайте изменения

Примечание: Если сервис proxy HTTPS отключен, явные Запросы соединения могут только быть заблокированы!

Когда расшифровка HTTPS WSA включена, трафик Skype может, скорее всего, сломаться, потому что это не чисто Трафик HTTPS (несмотря на использование ПОДКЛЮЧЕНИЯ и порта 443). Это приведет к 502 ошибкам, генерируемым WSA, и соединение будет отброшено. Любой реальный веб - трафик HTTPS к IP-адресу продолжит работать (невзирая на то, что он будет дешифрован на WSA).

Блокирование Skype - Явный / прозрачная среда с включенным Прокси HTTPS

Создайте пользовательскую категорию для соответствия с IP и трафиком порта 443:

1. Перейдите "Менеджеру безопасности"-> "Пользовательские Категории URL"->, "Добавляет Пользовательская Категория".
2. Заполните "Название категории" и расширьтесь "Усовершенствованный".
3. Используйте" [0-9] + \. [0-9] + \. [0-9] + \. [0-9] +" в окне Regular Expression.

Заставьте эту категорию дешифровать в Политике расшифровки:

1. Перейдите "веб-Менеджеру безопасности"-> "Политика расшифровки".
2. Щелкните по ссылке под столбцом "URL Categories" для соответствующей группы политик.
3. В "Пользовательском разделе" фильтрации Категории URL выберите "Decrypt" для новой категории Skype.
4. Отправьте и передайте изменения.

Примечание: Так как трафик Skype передается IP, это рассмотрят как часть "Некатегоризированных URL". Тот же эффект как выше произойдет в зависимости от того, должно ли действие дешифровать или passthrough.