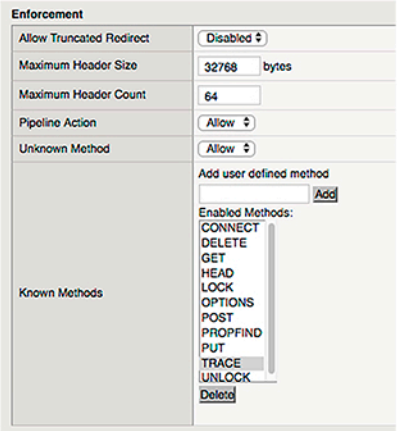
ЧТО ТАКОЕ HTTP. ЧАСТЬ VI. НАСТРОЙКИ АКТИВАЦИИ ПРОФИЛЯ HTTP

Джейсон Рамм (Jason Rahm), архитектор решений, F5 Networks, США

В статье из серии «Что такое HTTP» мы рассмотрели основные настройки HTTP-профиля. В этот раз мы поговорим о параметрах активации профиля (profile enforcement), имеющихся в настройках профиля. И, как и в прошлый раз, мы будем обсуждать только опции профиля для режима reverse proxy.
В TMOS версии 12.1 используются следующие параметры активации (приведены значения по умолчанию).



Поле Allow Truncated Redirect

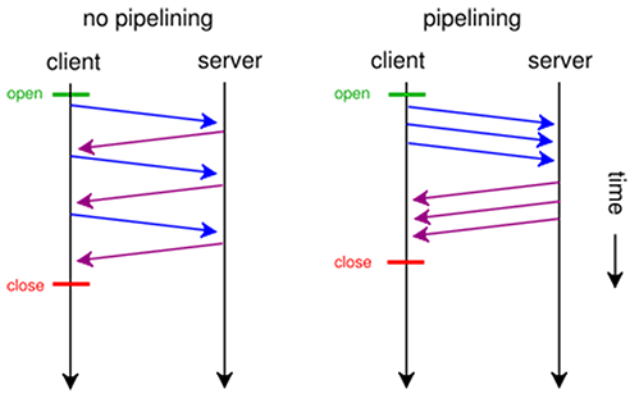
Это — обычный переключатель, позволяющий выбирать, каким образом BIG-IP будет обрабатывать перенаправления, не закрытые символом возврата каретки CRLF. По умолчанию, перенаправление будет отключено.

Поля Maximum Header Size & Count

Спецификация HTTP не устанавливает максимальный размер заголовка, который в данном случае является не размером одного заголовка, а размером строки запроса и всех заголовков вместе взятых, причем разные сервера устанавливают соответствующие максимальные параметры по-разному. Значение по умолчанию в BIG-IP составляет 32k, тогда как в Apache — 8k, в nginx, в зависимости от версии — от 4k до 8k, в IIS — 8k-16k, а вTomcat — 8k-48k. Поэтому, если вы настраиваете фронтенд к любому из этих серверов, кроме Tomcat, на выделенной виртуальной машине, установленное по умолчанию значение можно существенно уменьшить, и это никак не отразится на серверах. Здесь, однако, могут возникнуть различия в поведении. Большинство серверов возвращают код статуса 4xx: я видел, в частности, 400 404 и 413. Как можно не любить стандарты? BIG-IP просто перезапустит TCP-соединение. Размеры отдельных заголовков можно ограничить в iRules: такая возможность предусмотрена в различных правилах, разработанных для противодействия уязвимостям нулевого дня до установки патчей для сервера приложений.
Счетчик max header count — это действительно просто. Пока запрос менее 65, все в порядке.

Поле Pipeline Action

Поле Pipeline action — это еще один простой переключатель, позволяющий принимать или отклонять новые запросы от клиентов, если на их предыдущий запрос еще не поступил ответ. Что же такое конвейерный режим? Представьте себе телефонный разговор: вы задаете вопрос или делаете замечание, а ваш собеседник отвечает на него. Именно это происходит в системе без конвейерного режима. А теперь представьте себе публичные дебаты: первый участник излагает свой вопрос из десяти частей. Как правило, он делает это в один присест. А уж после того, как он сделает все свои заявления или задаст все свои вопросы, второй участник по порядку ответит на них. Так все происходит в системе с конвейерным режимом. Настройка конвейерного режима позволяет ведущему дебатов вмешаться — либо позволить первому участнику делать новые заявления и задавать новые вопросы до того, как ответит второй участник, либо лишить его такой возможности. Лори Маквитти представила в своей статье о рисках безопасности, присущих конвейерному режиму, неплохую схему функционирования конвейерного режима (см. ниже).



Поля управления методами

Эти настройки помогают избавиться от ранее неизвестных векторов атаки. Если ваше приложение — это простое приложение GET/POST, то нет никакой нужды разрешать что-либо еще. Запрещая неизвестные методы и исключая все прочие методы, кроме GET и POST из набора разрешенных методов, вы можете снизить свою уязвимость к угрозам, к которым сервер МОЖЕТ оказаться уязвимым. Аккуратное управление этими настройками означает, что у вас налажена хорошая коммуникация со своей командой прикладных программ, поэтому при разработке прикладных программ не будет случаев внедрения новых методов без корректировки профиля.

Бонусные функции!

Хоть это и не настройки активации профиля, но обсуждение этих функций позволяет завершить рассмотрение настроек reverse proxy в HTTP-профиле, поэтому я и решил написать о них здесь.

sFlow

sFlow это масштабируемая технология выборки пакетов, позволяющая вам наблюдать за закономерностями трафика для управления производительностью, поиска неисправностей, выставления счетов в целях безопасности. В HTTP-профиле предусмотрены две настройки: интервал опроса (polling interval) и частота выборки (sampling rate). Интервал опроса — это максимальный интервал между опросами, а частота выборки — доля выбираемых пакетов в общем числе пакетов в выборке. Таким образом, для установленного по умолчанию значения в 10 секунд и 1024 пакета, за десять секунд будет выполнено два опроса, для которых система случайным образом выберет один образец из 1024 пакетов. При этом, и частоту выборки, и интервал опроса можно либо указать здесь, в настройках профиля, либо принять значение, установленное по умолчанию: в этом случае будут унаследованы настройки HTTP, сделанные в меню System->sFlow->Global Settings.

Поле HTTP Strict Transport Security

Заголовок Strict Transport Security — это заголовок безопасности, требующий от браузера передавать каждый запрос на соответствующий домен через SSL, даже если в ответе с сервера для URL указан протокол HTTP, а не HTTPS. HSTS — одна из тех настроек, которые возникли как iRule (простое добавление заголовка для ответов клиента), а затем вошли в состав продукта. HSTS подключается проставлением галочки в поле Mode. Настройка Maximum Age устанавливается в секундах; ее значение по умолчанию соответствует шести месяцам. Если флажок Include Subdomains активен, то браузер получит указание использовать ту же настройку для поддоменов, а это — не всегда желательно.

Включение поддоменов может оказаться опасным! Допустим, вы собираетесь подключить HSTS для домена test.local, так как на нем подключен активный SSL. Но при этом вы забыли, что у вас еще есть сайт suckstobeyou.test.local, работающий только по HTTP. Если вы поставили флажок Include Subdomains, то ни один клиент, обращающийся к домену test.local не сможет попасть в этот поддомен до тех пор, пока не уберет эту настройку в своем браузере или не пройдет время, соответствующее максимальному возрасту запроса (по умолчанию — 6 месяцев), что на практике изолирует ваши домены! Будьте осторожны!

Читайте также:

Что такое HTTP? Часть I

Что такое HTTP. Часть II. Базовые протоколы

Что такое HTTP. Часть III. Терминология

Что такое HTTP. Часть IV. Клиенты, серверы и прокси

Что такое HTTP. Часть V. Основные настройки профиля HTTP

Что такое HTTP. Часть VI. Настройки активации профиля HTTP (эта статья)

Что такое HTTP. Часть VII. OneConnect

Что такое HTTP. Часть VIII. Сжатие и кэширование

Что такое HTTP. Часть IX. Политики и правила iRules.

Ожидайте продолжение:

Что такое HTTP. Часть X. Безопасность приложений.

Что такое HTTP. Часть XI. 2.0 и дальше.

Группа компаний БАКОТЕК – официальный дистрибьютор F5 Networks в Украине, Азербайджане, Республике Беларусь, Грузии, Армении и Молдове.
bakotech.com, f5@bakotech.com, +38 044 273 33 33.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle,
WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. 0113