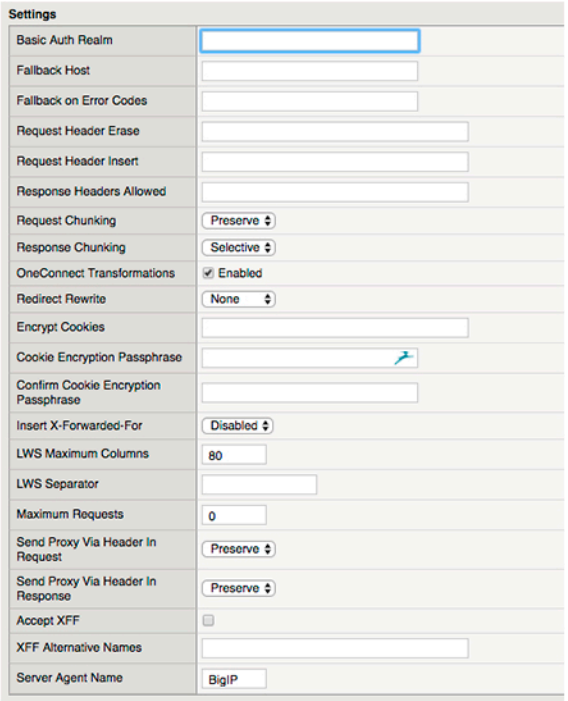
ЧТО ТАКОЕ HTTP. ЧАСТЬ V. ОСНОВНЫЕ НАСТРОЙКИ ПРОФИЛЯ HTTP

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

В первых четырех частях этой серии статей, посвященных HTTP, мы заложили фундамент, необходимый для понимания дальнейшего материала. В этой статье мы рассмотрим базовые настройки профиля HTTP в BIG-IP. Прежде чем перейти к настройкам HTTP, предлагаю коротко обсудить характер профиля. В BIG-IP каждое приложение обслуживается одним или несколькими виртуальными серверами. Там существуют сотни различных настроек для конфигурирования разных протоколов, используемых для обслуживания приложений. Поочередная регулировка каждой настройки для каждого приложения по отдельности не только отнимает много времени, но и влечет за собой риск чисто человеческих ошибок. Профиль позволяет администратору конфигурировать протокол с множеством специфических настроек, а затем применять их к одному или нескольким виртуальным серверам. Кроме того, профили могут быть выстроены иерархически, позволяя создавать дочерние профили с возможностью тонкой регулировки индивидуальных настроек на основе базового родительского профиля. Встроенные профили можно изменять, но делать это не рекомендуется. Лучше создать дочерний профиль на основе встроенного и изменять уже его.

Настройки, которым посвящена сегодняшняя статья, показаны на приведенном ниже снимке экрана. Речь пойдет о TMOS версии 12.1 HF1. HTTP-профиль менялся от версии к версии путем добавления и исключения различных наборов функций, поэтому не волнуйтесь, если у вас он выглядит иначе. В HTTP-профиле есть несколько режимов прокси, но мы сосредоточимся на рассмотрении режима reverse proxy.



Поле Basic Auth Realm

Эта область определяет объем защиты ресурсов на корневом сервере. Области — это своего рода разделы, где каждый может завести собственные схемы аутентификации.

Если аутентификация нужна, сервер должен ответить на запрос статусом 401 и заголовком WWW-Authenticate. Если присвоить этому полю значение testrealm, то возвращаемый клиенту заголовок будет иметь значение Basic realm="testrealm". Со стороны клиента при получении такого ответа во всплывающем окне браузера появится сообщение вроде «Введите имя пользователя и пароль для:», хотя некоторые браузеры не указывают область в этом сообщении.

Поля Fallback

В профиле два поля резервного режима могут использоваться для обработки пула ресурсов вашего сервера в неблагоприятных условиях. Поле Fallback on Error Codes позволяет вам указать коды статуса в списке, разделенном пробелами, который обеспечит перенаправление на резервный хост (Fallback Host) при наличии в ответе сервера любого из указанных здесь кодов. Это может пригодиться для сокрытия проблем с бэкендом ради улучшения взаимодействия с пользователем, а также — для предотвращения утечек информации о базовом сервере. Сам по себе резервный хост используется в отсутствие свободных узлов, на которые можно было бы направить запросы. Когда такое происходит, клиент в ответном сообщении получает статус 302 (временное перенаправление) с указанием хоста.

Поля Header Insertions, Erasures, & Allowances

Профиль поддерживает ограниченную функциональность добавления, удаления и очистки. Можно выбрать один заголовок для добавления в запросы и один заголовок для удаления из них. При добавлении и удалении одного и того же заголовка следует помнить об очередности этих действий. Не знаю, зачем вам может это понадобиться, но я провел тесты и увидел, что, похоже, заголовки HSTS и X-Forwarded-For добавляются первыми; если любой из них указан в поле Request Header Erase, то они будут удалены, а если их указать в поле Request Header Insert, то они будут вновь вставлены по пути к серверу.

Что касается ответов, то здесь можно составить список допустимых заголовков, разделенный пробелами: в этом случае заголовки, не указанные в списке, будут удаляться перед возвращением ответа клиенту. Если ни один из этих вариантов не соответствует вашим потребностям, то можно перейти к настройкам локальных политик обработки трафика или iRules, которым будет посвящена девятая статья из этой серии.

Поле Chunking

Поля деления запросов и ответов на фрагменты помогают справиться со сжатием. Последнему будет посвящена восьмая статья из этой серии. Эти поля позволяют указать BIG-IP порядок обработки разделенного на фрагменты контента, поступающего от клиентов и серверов, в соответствии с отметками в заголовке Transfer-Encoding. В приведенной ниже таблице показано, каким образом настройки профиля воздействуют на фрагментированные и нефрагментированные данные в ответах и запросах.

Setting	Content State	Action on Request	Action on Response
Preserve	Chunked	processes chunked content, sends to server unchanged	processes chunked content, sends to client unchanged
	Unchunked	processes content, sends to server unchanged	processes content, sends to client unchanged
Selective	Chunked	unchunks HTTP content, processes it, re-adds the chunk headers, sends updated content to server	unchunks HTTP content, processes it, re-adds the chunk headers, sends updated content to client
	Unchunked	processes HTTP content, sends to server unchanged	processes HTTP content, sends to server unchanged
Rechunk	Chunked	unchunks HTTP content, processes it, re-adds the chunk headers, sends updated content to server	unchunks HTTP content, processes it, re-adds the chunk headers, sends updated content to client
	Unchunked	processes HTTP content, adds transfer encoding headers and chunk headers to the response, sends the chunked request to the server	processes HTTP content, adds transfer encoding headers and chunk headers to the response, sends the chunked request to the client

Поле OneConnect Transformations

Мы рассмотрим OneConnect в седьмой части, но, в принципе, в случае разрешения преобразований и наличия профиля OneConnect, система получает возможность менять непостоянное соединение со стороны клиента на постоянное со стороны сервера. Если же эта функция подключена БЕЗ профиля OneConnect (этот вариант задан по умолчанию), то ничего не произойдет.

Поле Redirect Rewrites

Разгрузка SSL — это очень популярный компонент в BIG-IP. Трафик от клиента на BIG-IP, как правило, защищен SSL, а трафик с BIG-IP на сервер часто бывает незащищенным. Некоторые серверы либо не настроены, либо — просто не в состоянии обрабатывать возвращаемые защищенные URL, если сервер передает незащищенный контент. Существуют разные способы решения этой проблемы, но именно эта настройка может обеспечить перезапись всех URL или URL, соответствующих запросу, из http:// в https://. Перенаправления на IP-адреса узла можно настроить таким образом, чтобы перезапись осуществлялась вместо этого на адрес виртуального сервера. По умолчанию, эта настройка не выполняет перезапись перенаправлений. Для каждой опции перезаписи предусмотрены следующие действия:

None: указывает, что система не переписывает URI в любых HTTP-ответах с перенаправлением.

All: указывает, что система переписывает URI во всех HTTP-ответах с перенаправлением.

Matching: указывает, что система переписывает URI в любых HTTP-ответах с перенаправлением, совпадающих с URI запроса.

Nodes: указывает, что если URI содержит IP-адрес узла вместо имени хоста, то система заменяет его на адрес виртуального сервера.

Обратите внимание, что здесь переписывается не контент. Изменяется лишь заголовок Location в перенаправлении.

Поля Cookie Encryption

Эта функция безопасности позволяет вам принять незашифрованный куки-файл в ответе сервера, зашифровать его 192-битным ключом по алгоритму AES, а затем закодировать его при помощи b64 перед отправкой ответа клиенту. В списке, разделяемом пробелами, можно указать целый ряд куки-файлов. Все это можно сделать и при помощи iRules для всех куки-файлов без указания их имен.

Заголовок X-Forwarded-For

Заголовок X-Forwarded-For стал стандартом де-факто для передачи IP-адресов клиентов на серверы в тех случаях, когда сервер не видит истинный путь IP. Это характерно для трансляции сетевых адресов между клиентами и сервером. По умолчанию, поле Insert является неактивным, но если его сделать активным, то IP-адрес пакетов, принимаемых BIG-IP со стороны клиента, будет вставлен в заголовок X-Forwarded-For и отправлен на сервер. Поскольку X-Forwarded-For — это стандарт де-факто, это значит, что на самом деле стандарта не существует: некоторые прокси вставляют дополнительный заголовок, тогда как другие — просто присоединяют его к заголовку. Поля Accept XFF и XFF Alternate Names используются для статистики системного уровня и определения ее достоверности. Более подробную информацию об этом (особенно к ASM) можно найти в публикации solution K12264.

Подключение опции X-Forwarded-For в HTTP-профиле не очищает существующие заголовки X-Forwarded-For, уже присутствующие в запросе клиента. Если в запросе уже есть два заголовка, то BIG-IP, если он настроен для добавления, просто вставит третий. В этом можно легко убедиться при помощи утилиты curl:

```
curl -H "X-Forwarded-For: 172.16.31.2" -H "X-Forwarded-For: 172.16.31.3" http://www.test.local/
```

А вот то, что показал мне wireshark на моем тестовом сервере Ubuntu до и после активации вставки заголовка XFF в профиле:

```
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.102.62\r\n
    User-Agent: curl/7.54.0\r\n
    Accept: */*\r\n
    X-Forwarded-For: 172.16.31.2\r\n
    X-Forwarded-For: 172.16.31.3\r\n
    \r\n
```

```
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.102.62\r\n
    User-Agent: curl/7.54.0\r\n
    Accept: */*\r\n
    X-Forwarded-For: 172.16.31.2\r\n
    X-Forwarded-For: 172.16.31.3\r\n
    X-Forwarded-For: 192.168.102.1\r\n
    \r\n
```

Если вам нужно передать на сервер только один заголовок X-Forwarded-For, то для этого лучше применить iRule.

Поля Linear White Space

Для работы с линейным пробелом предусмотрены два поля: максимальное количество столбцов max columns (по умолчанию: 80) и разделитель separator (по умолчанию: \r\n). Линейное белое пространство — это любое количество пробелов, символов табуляции, новых строк, за которыми идет, как минимум, один пробел или символ табуляции. Вот выдержка из RFC2616:

«CRLF допускается в определении TEXT только как часть продолжения поля заголовка. При этом предполагается, что, перед интерпретацией значения TEXT, сложенный LWS будет заменен на одиночный пробел SP»

У меня ни разу не возникало причин для изменения этих настроек. Вы же можете проверить наличие линейного пробела в заголовке при помощи команды HTTP::header lws. Вот в этой ветке неплохо рассказано о том, что такое линейное пустое пространство.

Поле Max Requests

Здесь почти все — само собой разумеется. Нулевое значение, установленное по умолчанию, не ограничивает количество HTTP-запросов на одно соединение, но изменение этого значения ограничивает количество клиентских запросов по каждому соединению на указанное значение.

Поля Via Header

Независимо от того, идет ли речь о запросе или об ответе, эта настройка управляет тем, как BIG-IP обрабатывает заголовок Via. Как и при трассировке IP-пакетов, в заголовок Via дописывается каждый промежуточный сервер по пути следования, поэтому, когда сообщение поступает по назначению, становится известной трассировка HTTP (а не IP) (причем, если все прокси HTTP/1.1 должны это делать, то прокси HTTP/1.0 могут заголовок Via не дописывать). При обновлении заголовка, прокси должен указать имя (или псевдоним) своего хоста и версию HTTP предыдущего сервера в цепочке. Каждый прокси дописывает информацию в заголовок последовательно. Ниже приведен пример заголовка Via с портала разработчиков Mozilla.

```
Via: 1.1 vegur
Via: HTTP/1.1 GWA
Via: 1.0 fred, 1.1 p.example.net
```

В этом поле для запросов и ответов можно выбрать настройки, позволяющие сохранять, удалять или дописывать заголовок Via.

Поле Server Agent Name

Здесь указывается значение, которое BIG-IP вносит в заголовок Сервера при формировании ответов. При настройках по умолчанию, BIG-IP позволяет получать сведения об инфраструктуре, поэтому во многих реализациях эту настройку меняют. Заголовок Server в трафике ответа аналогичен заголовку User Agent в трафике клиента.

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 (эта статья)

Что такое HTTP. Часть VI. Настройки активации профиля HTTP

Что такое HTTP. Часть VII. OneConnect

Что такое HTTP. Часть VIII. Сжатие и кэширование

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

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