ПРЕДОТВРАЩЕНИЕ СПУФИНГ-АТАКИ НА ЗАПРОС X-FORWARDED-FOR ПРИ ПОМОЩИ BIG-IP

Питер Сильва (Peter Silva), старший разработчик решений F5 Networks, США

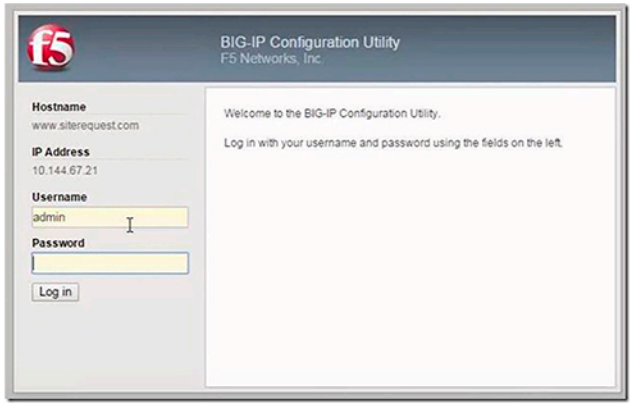
Ранее мы говорили о **Выборочном сжатии на BIG-IP** с использованием политики управления локальным трафиком, а на этой неделе давайте поговорим об использовании рассмотренных ранее решений в сфере безопасности.

Вы можете активировать в BIG-IP политику управления локальным трафиком, предотвращающую подделку запроса x-forwarded-for. Это одно из тех мест, где злоумышленники могут попытаться преодолеть защиту путем фальсификации IP-адреса в заголовке, чтобы обеспечить его прохождение через систему BIG-IP.

Предпосылки:

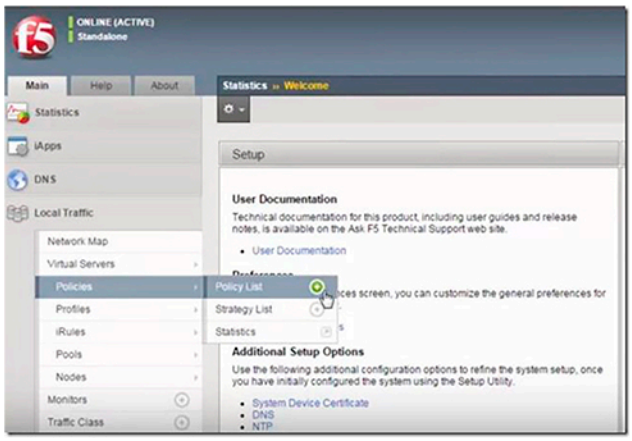
Мы используем BIG-IP v12 и,
У нас уже настроен виртуальный сервер Virtual Server для управления HTTP-трафиком, и за ним закреплен HTTP-профиль.

Итак, заходим в BIG-IP.

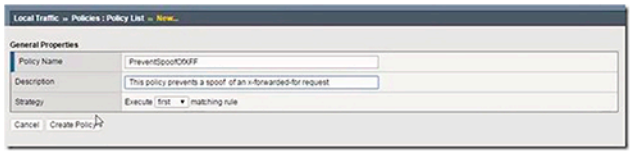


Первое, что нужно сделать, — создать проект политики. В главном меню выберите пункт **Local Traffic > Policies > Policy List** и нажмите на кнопку **Creator +**.

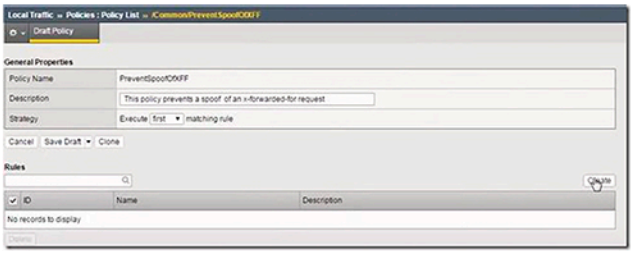
ПРЕДОТВРАЩЕНИЕ СПУФИНГ-АТАКИ НА ЗАПРОС X-FORWARDED-FOR ПРИ ПОМОЩИ BIG-IP



При этом мы перейдем к экрану конфигурации создания политики. Дадим политике уникальное название вроде **PreventSpoofOfXFF** и, хоть это и необязательно, добавим ее описание. Оставим опцию **Strategy** в качестве настройки по умолчанию для правила поиска соответствий Execute **First.** И нажмем на кнопку Create Policy.

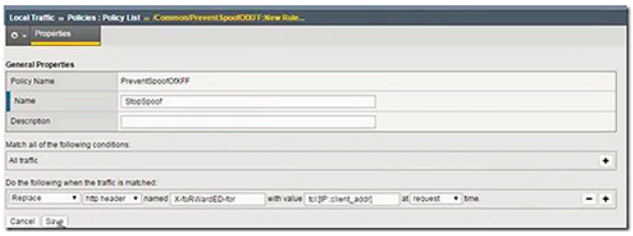


Мы попали на страницу общих свойств проекта политики (General Properties), на которой можно создавать правила. В области **Rules** нажимаем на кнопку **Create**.

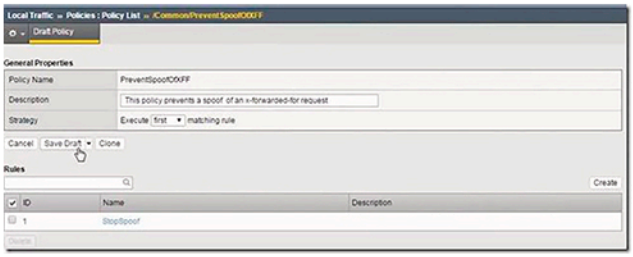


Присваиваем правилу уникальное имя вроде **StopSpoof**, а первое условие, которое необходимо настроить, заключается в сопоставлении всего HTTP-трафика со стратегией поиска соответствий. Это значит, что мы можем воспользоваться настройкой по умолчанию **All Traffic**. Теперь скажем политике, что мы собираемся делать в случае выполнения условия **All Traffic**. Новое действие заключается в замене **Replace заголовка http** под названием **X-forwarded-for** на значение tcl:[IP::client_addr] (для возврата IP-адреса клиента) во время запроса **request**. Сохраняемся, нажав **Save**.

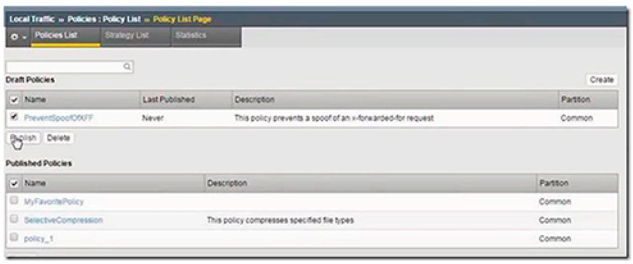
ПРЕДОТВРАЩЕНИЕ СПУФИНГ-АТАКИ НА ЗАПРОС X-FORWARDED-FOR ПРИ ПОМОЩИ BIG-IP



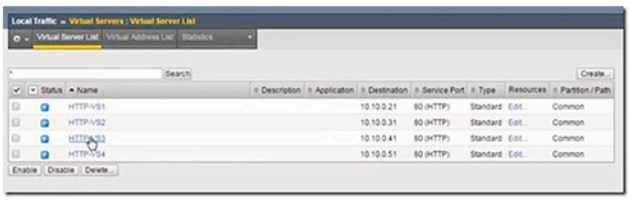
И сохраняем проект политики.



Затем ставим галочку возле проекта политики и нажимаем на **Publish**.

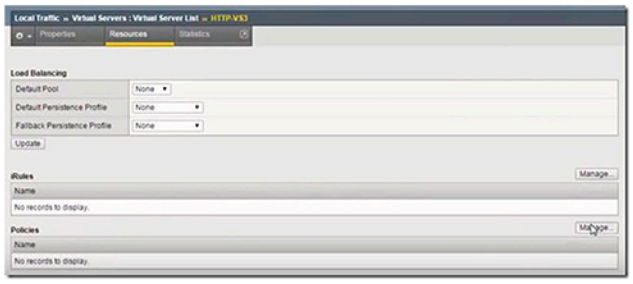


Теперь мы можем связать опубликованную политику с виртуальным сервером, которым мы пользуемся для управления HTTP-трафиком. В главном меню выбираем пункт Local Traffic > Virtual Servers > Virtual Server List и нажимаем на имя виртуального сервера, который нужно связать с этой политикой.

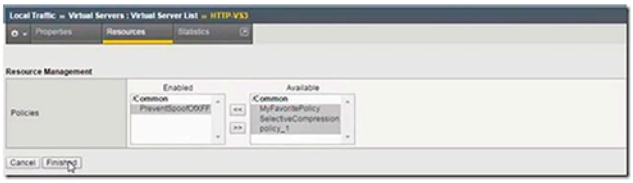


В меню выбираем пункт **Resources** и в области Policies нажимаем на кнопку **Manage**.

ПРЕДОТВРАЩЕНИЕ СПУФИНГ-АТАКИ НА ЗАПРОС X-FORWARDED-FOR ПРИ ПОМОЩИ BIG-IP



Переносим **PreventSpoofOfXFF** в список **Enabled** и заканчиваем работу нажатием на **Finished**.



Теперь виртуальный сервер, на котором работает политика управления локальным трафиком **PreventSpoofOfXFF** не пропустит HTTP-трафик, пытающийся подделать запрос x-forwarded-for.

Поздравляю! Вы легко и просто внесли дополнительное правило защиты в свою политику управления локальным трафиком! Благодаря нашей команде технических публикаций весь этот процесс можно увидеть в полном демонстрационном видеоролике.

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