



ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Выпуски **ТОП-10 Критичных функций безопасности** я начал публиковать начиная с версии [11.6](#) и они были очень популярными.

Как сказал однажды президент нашей компании: «Версия 13 является грандиозным выпуском. Огромным. И она включает лучшие методы по обеспечению безопасности. Я хочу сказать – лучшие в мире. И я обещаю вам, вы будете очень довольны, пользуясь ими».

Вы можете посмотреть официальную информацию о выпуске версии [13.0](#) и [версии 13.1](#). Я объединяю эти версии вместе, называя их просто «версия 13». Она включает множество облачных технологий, контейнеров и функций безопасности. Я просмотрел десятки настроек, обеспечивающих безопасность в этих версиях и выбрал для вас ТОП-10 самых мощных функций

Номер 10: FIPS 140-2 для vCMP в LTM, а также Full-Box FIPS

Флагман среди наших продуктов, Local Traffic Manager (LTM), поддерживает высокий уровень безопасности FIPS 140-2 в различных видах, начиная с версии 4.5. Я осуществлял первую реализацию 15 лет назад. В то время мы невероятно быстро обрабатывали 200 запросов в секунду (TPS).

Сегодня наши карты FIPS 140-2 справляются с десятками тысяч запросов, но в нашей технологии кое-чего не хватало. Наша система vCMP позволяет вам иметь множество виртуальных гостевых устройств TMOS, запущенных внутри более мощного оборудования. Обычно это делается для логического разделения сетей или менеджмента. И даже если основное устройство поддерживает FIPS 140-2 аппаратные ключи, гостевые системы – нет.

Сейчас это изменилось. Версия 13.1, запущенная на 10350v-F, i5820-F и i7820-F платформах (с использованием Cavium NITROX III карт), будет обеспечивать безопасность и обработку трафика SSL/TLS для виртуальных vCMP устройств. Это сделано через крутейший [SR-IOV](#).

Версия 13.1 была представлена одной из тех аккредитованных лабораторий для получения NIST «полнценной FIPS» сертификации. Сертификация уровня 2 (software only) может быть важна на определенных рынках, на которых все ваши устройства должны быть сертифицированы, и получить отказ от претензий является сложной и трудоемкой задачей.



ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Уточнение: управление ключами FIPS с использованием tmsh в LTM

В то время, когда я был начинающим разработчиком, я создал в CLI инструмент, который управлял ключом доступа FIPS 140-2 в TMOS. Правда, я не позаботился о том, чтобы добавить поддержку этой функции в tmsh. После того, как меня выгнали из разработки, следующее поколение высококвалифицированных разработчиков вычистило мой код и включило эту поддержку в tmsh. Это особенно важно для тех заказчиков, которые используют только CLI-доступ для управления TMOS.

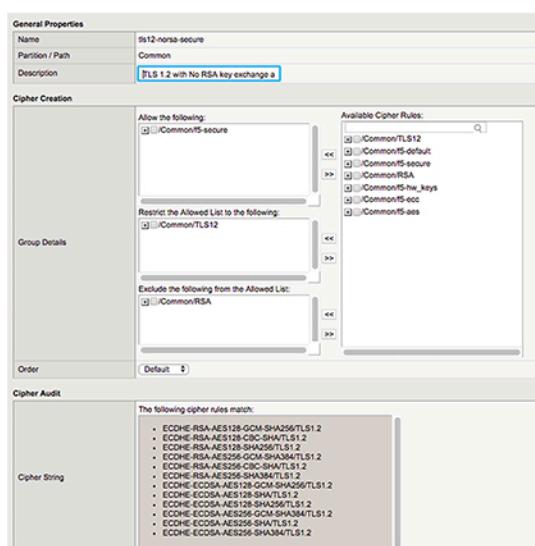
Номер 9: Правила шифров и группы шифров (Cipher Rules и Cipher Groups)

Мы наконец-то сделали списки шифров простыми. Вплоть до 13-й версии они были ужасно неудобными и непонятными. Настолько нелепыми, что я написал 5-ти страничный документ по их использованию в своем TLS-опусе [SSL Everywhere Deployment Guide](#).

Версия 13 предоставляет поддержку конфигурирования Cipher Rules и Cipher Groups, расположенную в модуле меню LTM. Cipher Groups используют Cipher Rules для выбора правильного шифра, описанного в выбранном Cipher Rule. Cipher Rules состоят из набора различных комбинаций шифров. Опции конфигурации для набора шифров включают в себя: Разрешенные наборы шифров, Ограничения для списка разрешенных шифров, явное Исключение для набора шифров. Каждая из этих настроек определяется путем добавления Cipher Rules в соответствующую категорию. Профили Clientssl и Serverssl были расширены возможностью выбора между вводом строки шифров (существующая функция) и между выбором группы шифров (Cipher Group) во время конфигурирования опции **Cipher**.

ECDHE+AES-GCM:ECDHE+AES:ECDHE+3DES:DHE+AES-GCM:DHE+AES:DHE+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:-MD5:-SSLv3:-RC4

Вместо этого вы можете собрать логические подгруппы шифров, затем объединить их в большие группы. И после — использовать эти группы в каждом профиле clientssl и serverssl.





ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

По правде говоря, мы сделали это несколько лет назад, однако не включали данный функционал, ввиду ограниченности ресурсов разработки.

Номер 8: глобальная VLAN SYN-flood защита в LTM

SYN-flood — неприятное явление, от которого очень трудно избавиться.

Даже простейшая LTM-конфигурация имеет как минимум два VLAN: один для внешнего трафика (неотфильтрованного) и один — для внутреннего трафика (в теории, чистого). SYN-flood приходит снаружи и направлен на виртуальный сервер, настроенный на вашем внешнем VLAN.

До версии 13 LTM активирует SYN-flood защиту для виртуального сервера, который подвергается атаке. И это хорошо работает. Версия 13 сделала шаг вперед: после того, как SYN-flood атака определена, включается защита всех виртуальных серверов на этом VLAN. Мы добавили это изменение по двум причинам.

Во-первых, если атакующий нападает на один из ваших виртуальных серверов, он очень быстро может переключиться на другие, поэтому имеет смысл защищать их все. Во-вторых, более эффективно использовать FPGA для обработки всего VLAN, чем выборочно для одного виртуального сервера.

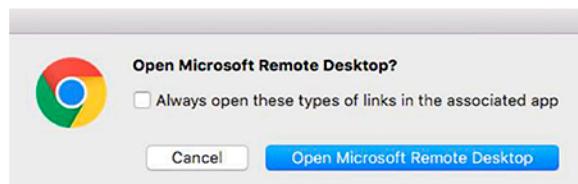
Номер 7: Простые RDP-туннели для Linux и Mac OS в модуле APM

Access Policy Manager (APM) — это один из наших наиболее популярных продуктов. APM дает возможность пользователям работать с Single SignOn и SSL/VPN. В версии 13 также не забыли про APM.

Вы хотите, чтобы ваши пользователи хорошо к вам относились? Они начнут это делать, когда исследуют номер 7 из ТОП-10 списка, которым является: Простой клиентский RDP, запущенный на Linux и Mac.

Single SignOn WebTop в APM давно поддерживал Remote Desktop Protocol (RDP) от компании Microsoft. Обычно, RDP требует ввода имени пользователя и пароля, что в свою очередь разрушает концепцию SSO WebTop, не так ли? До версии 13, механизм аутентификации работал через ActiveX в IE на Windows. Но в других браузерах или других ОС (Linux, Mac) возникали сложности.

В некоторых операционных системах мы должны запускать Java or ActiveX для получения беспарольного запуска RDP-клиента. Это просто ужасно, поэтому мы поработали над тем, чтобы добиться беспарольного запуска, используя только естественные (non-Java) запросы.





ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

В версии 13.1 APM получил эту возможность, работая для Linux и Mac OS. На моем Mac Book Pro я вижу это сообщение после того, как кликаю на иконку RDP WebTop. После этого RDP запускается и работает без запроса пароля. И это — замечательно! Очевидно, что, поставив галочку в чек-бокс, вы больше никогда не увидите этого сообщения.

Уточнение #2: JSON Web Token в APM

Вообще-то, эта функция немного выделяется из ТОП-10 списка. Но она остается важной, потому назовем это уточнением.

OAuth и объединенный вход являются критичными технологиями для современной инфраструктуры. APM демонстрирует поддержку OAuth 2.0 с новыми улучшениями JSON Web Token.

Структура OAuth 2.0 в APM теперь поддерживает аутентификацию без отслеживания состояния. Сервер OAuth может верифицировать входящий JSON Web Token и осуществлять проверку доступа, основываясь на содержании токена, без подключения к серверу авторизации. Эта крутая функция безопасности имеет три варианта:

Защита ресурсов компании с помощью stateless-аутентификации с использованием токенов JWT.

Использование F5 как OAuth в качестве клиента и сервера обработки.

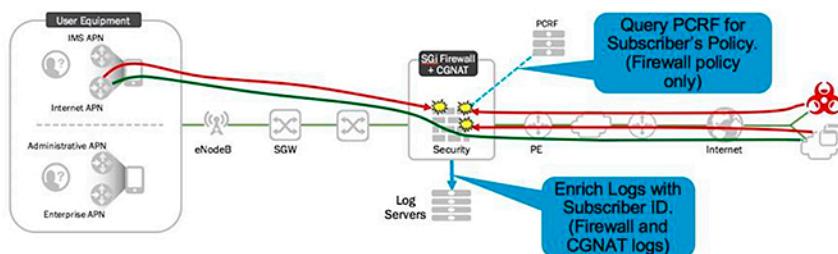
Использование F5 как OAuth в качестве клиента и сервера обработки через ROPC Grant.

Насколько это круто? Если вы хотите побольше узнать о поддержке JSON Web Token в APM, позвольте мне отправить вас к [документации](#).

Номер 6: Файрвол с идентификацией абонентов

Модуль Advanced Firewall Manager (AFM) в F5 пользуется успехом у всех хороших провайдеров.

В предыдущих версиях абоненты и группы абонентов могли быть включены в политики AFM. Эта возможность была изначально разработана для сценариев, не гарантировавших безопасность, однако сейчас мы тесно объединили ее с нашим firewall и обеспечили скачок производительности.





ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Версия 13.1 превращает AFM в настоящий файрвол с идентификацией абонентов.

AFM встраивает определение абонентов в данные TMOS и в уровень управления. Файрвол может динамически создавать базу данных абонентов, идентифицируя их по MS-ISDN, IMSI, MAC и информации с RADIUS сервера или базы DHCP snooping и запросить PCRF через Gx-интерфейс для получения политики безопасности. После чего эта определенная политика применяется для абонента или группы. И определяет абонентов или группы абонентов в обе политики безопасности и репортинга.

Ниже перечислены основные пункты для сервис-провайдеров:

- Добавление в логи Subscriber-ID (ID абонента) для файрвола и CGNAT (NAPT и PVA логи).
- Определение абонентов и динамическое применение политик.
- PCRF-интеграция, использующая Gx-интерфейс.

Использование для защиты от IoT ботнетов

Файрвол с идентификацией пользователя очень хорошо подходит для IoT архитектуры. Политика безопасности, привязанная к устройству, которая может контролировать IP и URL каждого типа устройства — это очень круто! Запретите все остальные устройства, чтобы защититься от IoT ботнетов.

Номер 5: Поведенческий DOS для DNS

Мы очень гордимся нашей поведенческой DoS-защитой. Даже само название BaDOS звучит круто. Если вы не знали, это — автоматическая защита от DDoS-атак. ASM модуль использует его для L7 DOS, о чем мы напишем ниже. AFM модуль использует поведенческий анализ для защиты от DoS-атак на уровне сети. BaDOS использует всеми любимую технологию — машинное обучение (machine-learning) — для анализа поведения трафика между клиентами и серверами приложений и после автоматически устанавливает пороговые значения для трафика на L7 (HTTP) и L3-4.

Например, в случае DoS-атаки со стороны ботнета, каждый запрос может быть полностью легитимным, но множество запросов сразу могут замедлить или завалить сервер. Поведенческий DoS может снизить воздействие DoS-атаки путем снижения объема трафика и сохранения работоспособности сервера. Поведенческий анализ DOS в модуле AFM непрерывно отслеживает состояние сервера (по наличию определенных ответов от него), чтобы в реальном времени обеспечить взаимосвязь, подтверждать состояния сервера, атаки и реакции на них. Каждое последующее аномальное срабатывание подвергается анализу, и система реагирует на них уменьшением трафика или блокировкой, если это необходимо.

Поведенческий DoS-анализ работает по таким этапам:



ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

- изучение типичного поведения нормального трафика;
- обнаружение атаки в текущих условиях (по доступности сервера);
- обнаружение поведенческой аномалии (кто и что стало причиной перегруженности?);
- уменьшение воздействия атаки путем замедления подозрительных клиентов;
- улучшение своих настроек на основе опыта.

Вы устанавливаете уровень смягчения последствий атаки, который ранжируется от «no mitigation» (только изучение) до «aggressive protection» (проактивная DoS-защита). Система может быстро определить DoS-атаку, характеризовать проблемный трафик и смягчить атаку. Модуль AFM в версии 13 расширил действие BaDOS и на DNS-защиту.

И эта функция в AFM позволяет включить его в ТОП-10. А теперь мы переходим к самому интересному на вершине рейтинга!

Номер 4: Иерархические политики по защите приложений (Application Security Policies)

Наш модуль ASM является лучшим в мире Web Application Firewall (WAF). Он включает в себя множество новых и улучшенных функций безопасности, добавленных в версии 13.

Номером 4 нашего списка являются многоуровневые политики Application Security. Политики Application Security в версии 13 теперь могут наслаждаться близким контактом со своим родителем. Но политики могут быть наследниками своих родителей.

Такое наследование политики дает возможность осуществить быстрое создание и обучение. Администраторы могут:

Изменять родительскую политику, одновременно распространяя эти изменения на все наследующие политики.

Внедрять определенные параметры безопасности, задавая их как обязательные для наследования (mandatory) и родительской политике.

Разрешать редактору application security принимать или отклонять параметры безопасности.



ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Иерархическая структура политик не дает возможности пользователю обойти настройку родительской политики, но позволяет упростить развертывание и применение политик. Когда родительская политика помечает функцию, как опциональную, каждая дочерняя политика имеет возможность принять настройку.

В действительности, это довольно здорово и потенциально может упростить несколько реальных задач заказчиков, которые возникают с ростом количества приложений и связанных с ними политик.

Номер 3: Полный поведенческий анализ DOS на L7 (модуль ASM)

Версия 13 развернула полную BaDOS-защиту. В предыдущей 12 версии BaDOS был ограничен двумя виртуальными сервисами. Тринадцатая версия является первой, в которой поведенческий анализ DOS реально развернулся во всех направлениях, никакой другой продукт в сфере защиты приложений не делает ничего подобного. Команда разработчиков сказала мне, что эта возможность обязательно должна быть в ТОП-3, в противном случае они перестанут со мной здороваться.

BaDOS включает следующий уникальный функционал:

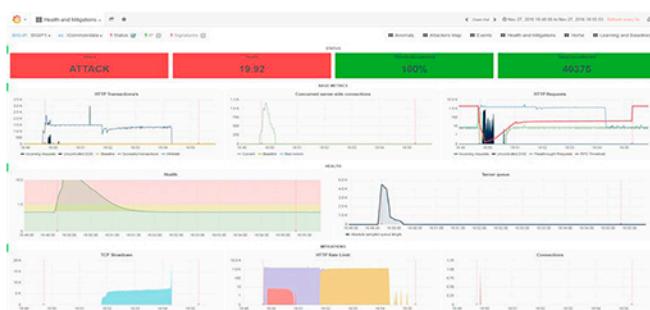
Автоматическое определение и противодействие L7 DoS-атакам с использованием непрерывного отслеживания состояния сервиса, поведенческий анализ, включающий 600 различных метрик и алгоритмы машинного обучения

Нет необходимости во вмешательстве пользователя: не нужно настраивать пороговые значения (thresholds), ни переопределять их, за счет **авто-настройки и адаптивных изменений**

Автоматическая генерация сигнатур атак с помощью алгоритмов машинного обучения, которая объединяет аномальное количество атакующих запросов в небольшое количество правил

Избежание ложных срабатываний (false-positive) для отсутствия влияния сгенерированных сигнатур на легитимный трафик

На картинке показано применение машинного обучения и регулярное обновление статистической информации (собранное во время обычной работы). Увеличение на графиках – DoS-атака.





ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Номер 2: [ASM] CAPTCHA, ловушки и отражение атак

В версии 13 механизм противодействия brute-force атакам также был значительно улучшен. Он стал быстрее, проще и эффективнее. Многие из этих улучшений построены на идеи «ID устройства». ASM определяет характерные признаки каждого устройства, которое подключается к приложению и приписывает их к уникальному ID устройства. Таким образом, ASM может заблокировать brute-force атаку от конкретного устройства без блокировки целого IP-адреса, что может случайно заблокировать всех пользователей, сидящих за NAT и proxy.

Существует три различных параметра, по которым ASM идентифицирует устройство:

- IP-адрес источника
- Имя пользователя
- ID устройства

Анализируя эти параметры, ASM может точно детектировать атаки. Для примера, в версии 13 ASM может предотвращать распределенную brute-force атаку на логин, в которой атакующие используют ботнет для распределения попыток залогиниться (чтобы обойти использование одного адреса источника).

Так как brute-force атака была обнаружена (распределенная или нет), ASM может использовать CAPTCHA. ASM будет делать это всегда и атакующий будет пытаться обойти ее, передавая CAPTCHA-изображения группе людей, которые вводят ответ. Это смешленый ход и некоторые зарабатывают на этом.

Итак, вот и №2 среди мощных функций безопасности, представленных в версии 13.

ASM может определять такие группы и выдавать этим пользователям специальные страницы-ловушки (honeypots).



ТОП-10 МОЩНЫХ ФУНКЦИЙ БЕЗОПАСНОСТИ В BIG-IP 13

Если ASM увидит множество ответов на CAPTCHA, объединенных одним именем пользователя и приходящим с одного адреса, но не использующих ID устройства, то это, вероятнее всего, CAPTCHA-ферма. ASM может отбрасывать такой трафик или отправлять в ответ фальшивый ответ об ошибке логина. Вы можете использовать стандартный код honeypot-страницы или загрузить собственный HTML, чтобы затруднить атакующему определение фальшивой страницы.

Определение CAPTCHA-ферм с защитой с помощью honeypots — это реально круто! В нашей внутренней документации это описано как «honeypot and drop».

Номер 1: [ASM] Защита от использования скомпрометированных данных для входа

Вы готовы к самой крутой фишке из ТОП 10 самых мощных функций безопасности в версии 13? Одна из моих самых любимых функций по защите — это **защита от Credential Stuffing!**

Возвращаясь к проблеме **credential stuffing**: атакующие приобретают скомпрометированные данные username/login в даркнете, и после пробуют их на разных сайтах. Так как пользователи меняют свои пароли не очень часто, то такие атаки оказываются очень успешными.



Группа компаний БАКОТЕК – официальный дистрибутор 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