Иван ЧЕРНОВ
менеджер по развитию UserGate

Артём ТУРЕНОК
руководитель отдела технических решений АО «ДиалогНаука»

КОНКУРЕНТ ЗАРУБЕЖНЫМ АНАЛОГАМ

КАК ЗАЩИТИТЬ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ С ПОМОЩЬЮ РОССИЙСКОГО МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ

NGFW (Next Generation Firewall) изменили парадигму оперативного контроля внешнего сетевого трафика, предоставив компаниям возможность отсекать пакеты данных из определённых источников, а также анализировать сами передаваемые данные, проверять их на наличие вредоносных сигнатур и ограничивать работу с нежелательными ресурсами. Рассмотрим функции современного межсетевого экрана на примере отечественного представителя систем этого класса UserGate Next Generation Firewall.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ USERGATE NEXT GENERATION FIREWALL

Набор функциональных возможностей UserGate Next Generation Firewall охватывает разнообразные потребности в сфере защиты трафика и фильтрации контента. Гибкие механизмы настройки межсетевого экрана позволяют выстраивать сложные логические схемы обработки данных и в автоматическом режиме реагировать на потенциально опасные или нелегитимные действия. Кратко остановимся на наиболее важных аспектах работы UserGate Next Generation Firewall.

ФИЛЬТРАЦИЯ КОНТЕНТА ПО ПРАВИЛАМ

Фильтрование трафика в UserGate Next Generation Firewall основывается на механизме правил — по сути, политик безопасности, описывающих действия системы при наступлении тех или иных заданных условий. Правила фильтрации могут блокировать или, наоборот, разрешать движение данных в зависимости от их типа, источника, получателя, приложения, категории и других параметров. Правила могут применяться к одному или нескольким пользователям и выполняются последовательно, что даёт возможность строить гибкую систему обеспечения кибербезопасности и осуществлять контроль работы сотрудников.

При помощи правил можно не только создавать белые и чёрные списки ресурсов, но и контролировать множество параметров передаваемых пакетов, например тип используемого браузера, наличие определённых словоформ или типов информации. Правила используются не только для фильтрации контента, но и в других функциональных блоках системы — межсетевом экране, подсистеме ограничения пропускной способности и пр. Пример настройки правил контентной фильтрации представлен на рисунке 1.

АНАЛИЗ ТРАФИКА

Глубокий разбор трафика является ключевой функцией NGFW и основным источником данных для других подсистем. UserGate Next Generation Firewall способен детально исследовать нагрузку каждого передаваемого пакета, на лету определяя потенциально небезопасное содержимое, а также триггеры, по которым активируются заранее заданные правила и сценарии. Помимо обычного трафика, система расшифровывает и защищённые SSL-пакеты (рис. 2), работая с протоколами HTTPS, SMTPS и POP3S. При этом сервер NGFW осуществляет подмену оригинального сертификата на собственный, отдавая на сторону пользователя по-прежнему защищённый контент.

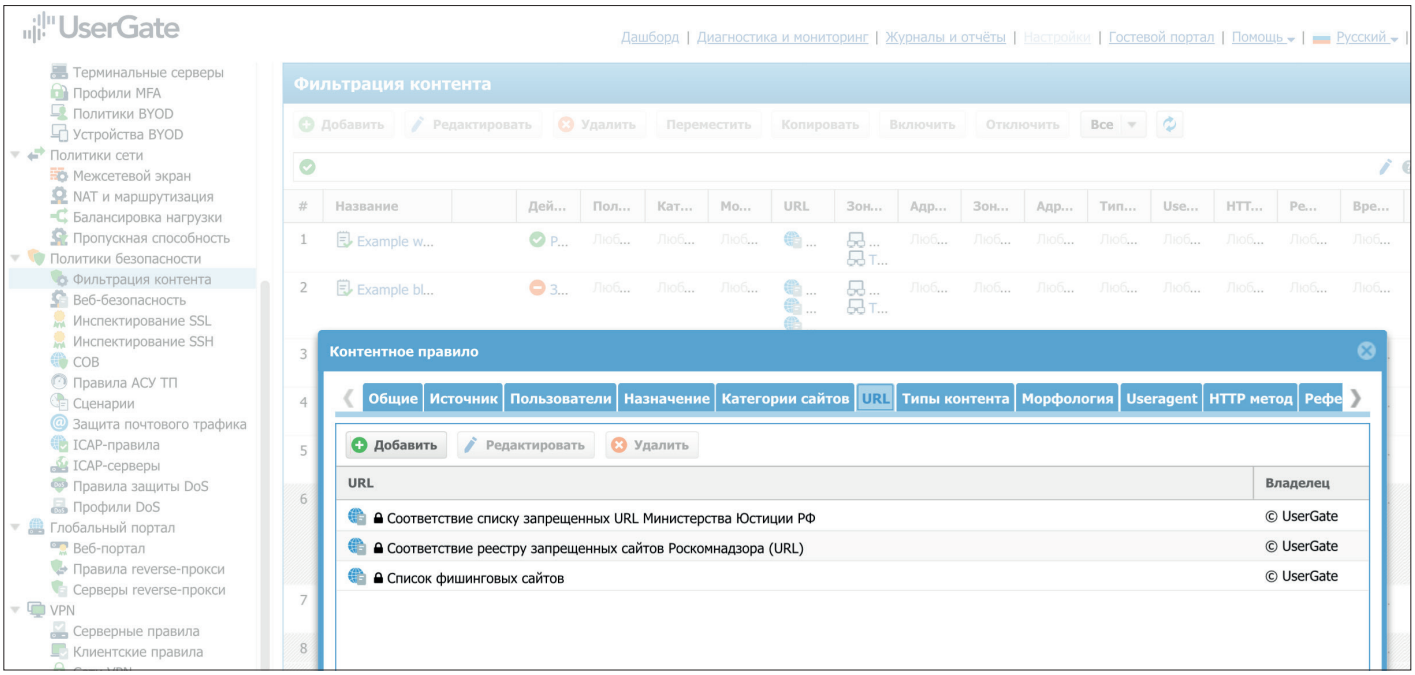

Рисунок 1. Пример настройки правила контентной фильтрации

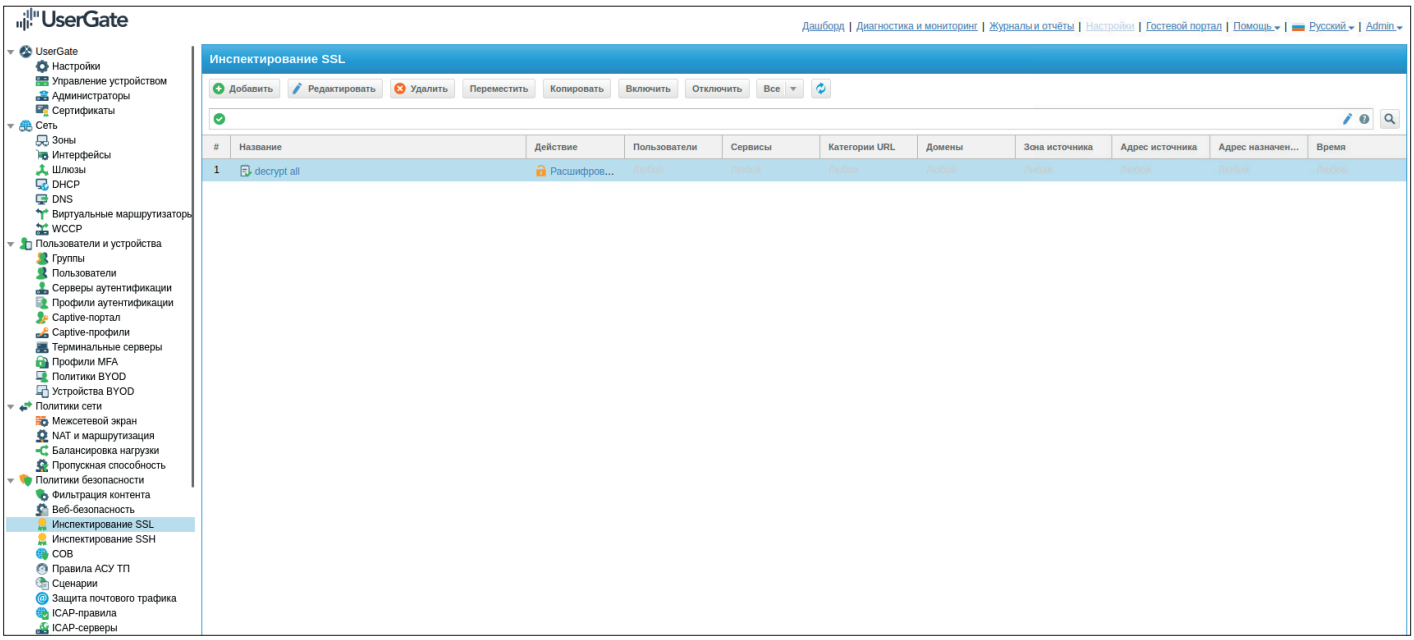

Рисунок 2. Раздел настройки «вскрытия SSL-трафика»

ЗАЩИТА ОТ DOS

Одним из механизмов безопасности в UserGate Next Generation Firewall является функция ограничения числа соединений, открытых одним пользователем. Так же, как и многие другие элементы NGFW, она реализована при помощи механизма правил и сценариев, что позволяет гибко настраивать чувствительность системы в соответствии с особенностями конкретной компании. Ограничение на количество одновременно открытых пользователем сеансов обеспечивает эффективное противостояние возможным DoS-атакам (Denial of Service) через пользовательские или гостевые учётные записи.

КОНТРОЛЬ ИНТЕРНЕТ-ПРИЛОЖЕНИЙ

UserGate Next Generation Firewall работает с приложениями на седьмом уровне сетевого взаимодействия модели OSI. Система идентифицирует более 1000 приложений (рис. 3) и даёт администратору возможность ограничивать их использование. Например, NGFW способен полностью заблокировать работу мессенджеров, торрент-клиентов (рис. 3) и других нежелательных программ. Собственная база обновляемых сигнатур позволяет, помимо этого, защищать локальную сеть от угроз, связанных с теми программами, которые работают с интернетом.

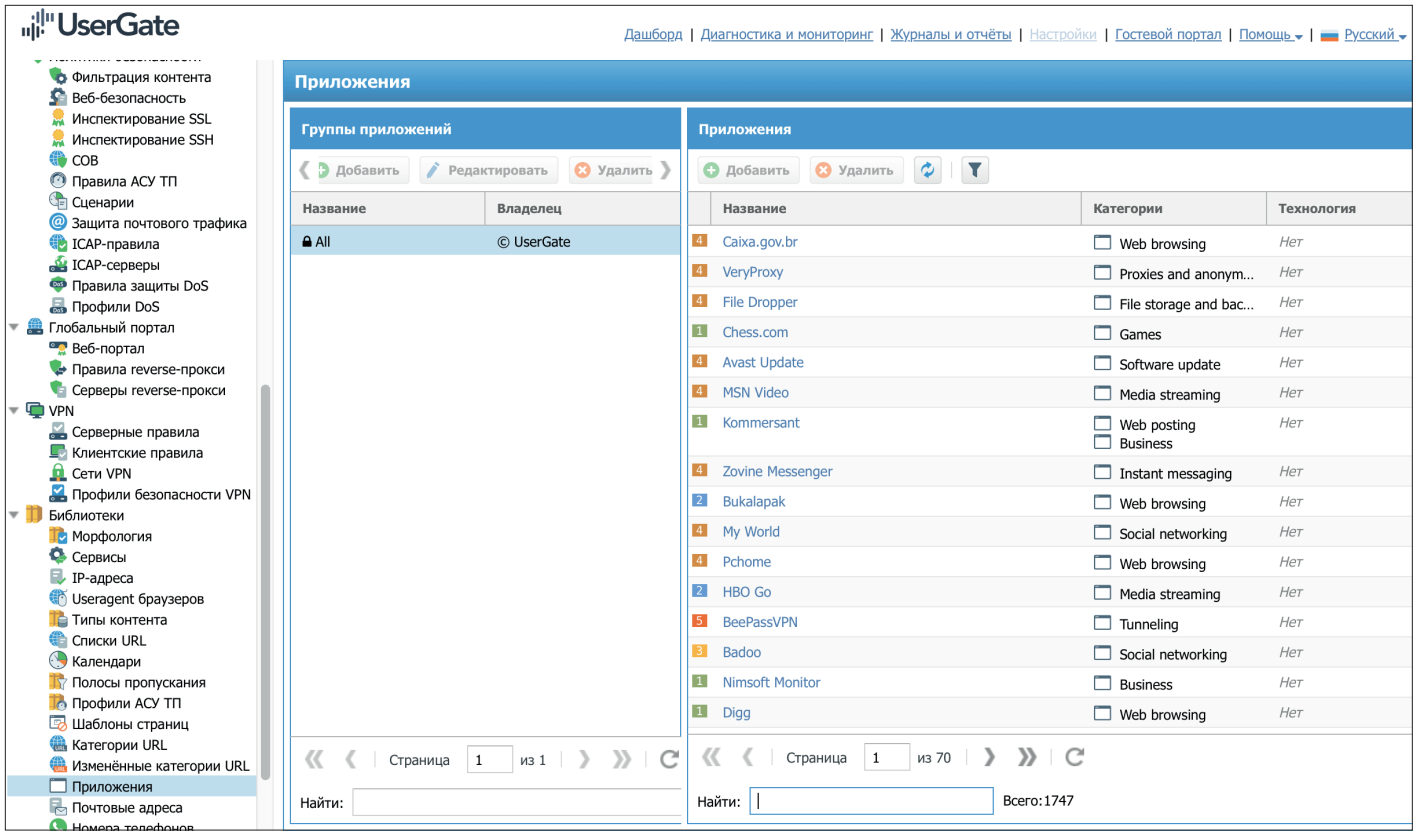

Рисунок 3. Список доступных приложений

АНТИВИРУС

В состав UserGate Next Generation Firewall входит потоковый антивирус, который может проверять внешний трафик на наличие вредоносных программ. Анализ ведётся при помощи собственной базы сигнатур, что обеспечивает достаточную надёжность и блокировку основных угроз до того, как данные пересекут контур безопасности. С другой стороны, использование лёгкого сигнатурного антивирусного ядра минимально нагружает систему, что даёт возможность при необходимости проверять весь трафик полностью. Антивирусная защита использует механизм правил безопасности NGFW.

РЕАГИРОВАНИЕ

В UserGate Next Generation Firewall встроена система предотвращения вторжений, которая способна в настоящем времени реагировать на атаки киберпреступников, эксплуатирующих известные уязвимости. UserGate Next Generation Firewall даёт администратору возможность создавать различные наборы сигнатур для защиты различных сервисов, а также формировать на базе универсального механизма правил собственные сценарии для каждого типа трафика. Это позволяет не только формировать реакции на кибератаки, но и контролировать вредоносную активность внутри сети.

СОБСТВЕННАЯ ОС

В основе UserGate Next Generation Firewall лежит оригинальная операционная система UGOS, оптимизированная для задач быстрой и эффективной обработки трафика. Платформа создана на базе дистрибутива Linux и не использует готовых комплексных модулей: все подсистемы безопасности разработаны программистами UserGate и не содержат стороннего кода. С одной стороны, это позволяет быстро адаптировать её под требования заказчика, а с другой — существенно снижает вероятность атак на систему с использованием общеизвестных уязвимостей.

ВАРИАНТЫ ПОСТАВКИ

UserGate Next Generation Firewall может поставляться как в виде виртуального межсетевого экрана, развёрнутого на одном из гипервизоров (VMware, Hyper-V, Xen, KVM, OpenStack, VirtualBox, отечественные разработки), так и в виде программно-аппаратного комплекса, созданного UserGate. Производитель предлагает несколько вариантов исполнения таких NGFW, предназначенных для организаций разного масштаба — от компаний сегмента СМБ до крупных предприятий и дата-центров.

ВЫВОДЫ

UserGate Next Generation Firewall занимает передовые позиции в секторе NGFW российского рынка информационной безопасности и может конкурировать с ведущими зарубежными аналогами. Компетенции компании UserGate в сфере анализа сетевого трафика позволили ей создать зрелый продукт, способный стать существенным препятствием для кибератак, универсальным инструментом первой необходимости, который сможет обезопасить компанию от большого числа инцидентов даже при частичной недоступности других инструментов информационной безопасности.