

Table of Contents

Table of Contents	1
Введение	2
Безопасность сети и защита от сетевых угроз	3
Межсетевое экранирование	4
Обнаружение и предотвращение вторжений	5
Защита от DOS-атак и сетевого флуда	6
Антивирусная проверка трафика	7
Проверка почтового трафика	8
Управление трафиком АСУ ТП	9
Работа с внешними системами безопасности	10
Настройка политик безопасности при помощи сценариев	11
Улучшение производительности и надежности интернета	12
Поддержка кластеризации и отказоустойчивости	13
FTP поверх HTTP	14
Поддержка нескольких провайдеров	15
Управление пропускной способностью	16
Поддержка WCCP	17
Управление трафиком и контроль доступа в интернет	18
Маршрутизация трафика и публикация ресурсов	19
Аутентификация и авторизация пользователей	20
Поддержка гостевого портала	21
Проксирование приложений	22
Перенаправление трафика на вышестоящий прокси-сервер	23
Журналы и отчеты	24
Журналы и отчеты(описание)	25
Контент-фильтрация и контроль приложений	26
Интернет-фильтрация	27
Выборочная блокировка рекламы	28
Активация безопасного поиска	29
Блокировка приложений социальных сетей	30
Инжектирование кода на веб-страницы	31
Инспектирование SSL-трафика	32
VPN и веб-портал	33
Другие функции	34
Функция балансировщика нагрузки	35
DNS-фильтрация	36
Использование оповещений	37
Ролевой доступ администраторов к элементам управления UserGate NGFW	38
Типы интерфейсов	39
Алгоритм обработки трафика	40
UserGate NGFW 7 Packet Flow	41
Совместимость с аппаратными платформами	52
Совместимость версий UserGate NGFW с аппаратными платформами	53

Межсетевое экранирование

Documentation: 

Version: 5.x, 6.1.9, 7.x, 7.0.1

Product: NGFW

Межсетевой экран нового поколения UserGate NGFW фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

Обнаружение и предотвращение вторжений

Version: 7.1.0

Product: NGFW

Documentation: 

Система обнаружения и предотвращения вторжений (COB) позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление отчетов.

Администратор может создавать собственные сигнатуры COB для защиты определенных сервисов и включать их в профили COB наряду с сигнатурами, поставляемыми UserGate. Профили COB интегрируются в правила межсетевого экрана. При срабатывании сигнатур такого профиля будет произведено действие, настроенное в сигнатурах и произведена соответствующая запись в [Журнале COB](#).

Защита от DOS-атак и сетевого флуда

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

NGFW позволяет задать параметры защиты каждой зоны сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP), указав порог уведомления - количество запросов с одного IP-адреса, после которого происходит запись в журнал - и порог отбрасывания пакетов - количество запросов, после которого пакеты отбрасываются с соответствующей записью в журнале.

Возможно настроить исключения, например, для зон, использующих IP-телефонию и поэтому отправляющих большое количество UDP-пакетов.

Антивирусная проверка трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

Потоковый антивирус UserGate позволяет обеспечить антивирусную проверку трафика без ущерба для производительности и быстродействия сети. Модуль использует обширную базу сигнатур.

Проверка почтового трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

NGFW способен обрабатывать транзитный почтовый трафик (SMTP(S), POP3(S)), анализируя его источник, а также содержание письма и вложений, что гарантирует надежную защиту от спама, pharming- и phishing- атак. NGFW также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

Управление трафиком АСУ ТП

Technology: SCADA

Version: 7.x

Product: NGFW

Documentation: ☒

В новой версии платформы администратор может контролировать прохождение трафика автоматизированных систем управления технологическими процессами (АСУ ТП) через NGFW с помощью профилей COB и приложений. В библиотеке сигнатур, предоставляемых компанией UserGate, имеется набор сигнатур, которые идентифицируют известные уязвимости протоколов АСУ ТП по CVE/BDU.

Работа с внешними системами безопасности

Documentation: ☒

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Имеется возможность передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. Администратор может указать, какой трафик требуется передавать на ICAP, а также настроить работу с фермами серверов.

Настройка политик безопасности при помощи сценариев

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☒

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря автоматизации безопасности при помощи механизма сценариев (SOAR — Security Orchestration, Automation and Response).

Эта концепция находится на пике популярности и позволяет администратору создавать сценарии (запускаемые по плану или при обнаружении атаки), где прописываются автоматические действия в ответ на те или иные события. Такой подход обеспечивает гибкую настройку политик безопасности, сокращает участие человека благодаря автоматизации повторяющихся задач, а также дает возможность приоритезировать сценарии для скорейшей реакции на критичные угрозы.

Улучшение производительности и надежности интернета

Поддержка кластеризации и отказоустойчивости

Documentation: 

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

UserGate NGFW поддерживает 2 типа кластеров: кластер конфигурации, позволяющий задать единые настройки узлам в рамках кластера, и кластер отказоустойчивости, призванный обеспечить бесперебойную работу сети. Кластер отказоустойчивости может работать в двух режимах: Актив-Актив и Актив-Пассив. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

FTP поверх HTTP

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Модуль FTP поверх HTTP позволяет обращаться к содержимому FTP-сервера из браузера пользователя.

Поддержка нескольких провайдеров

Documentation: 

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

При подключении системы к нескольким провайдерам UserGate NGFW позволяет настроить для каждого из них свой шлюз для обеспечения доступа к интернету. Администратор также может настроить балансировку трафика между провайдерами, указав вес каждого шлюза, или указать один из шлюзов как основной с переключением на других провайдеров в случае недоступности основного шлюза.

Управление пропускной способностью

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Правила управления пропускной способностью служат для ограничения канала для определенных пользователей, хостов, сервисов или приложений.

Поддержка WCCP

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Поддержка протокола WCCP позволяет использовать NGFW в инфраструктуре с WCCP-серверами, например, маршрутизаторами Cisco.

Маршрутизация трафика и публикация ресурсов

Documentation: ☒

Product: NGFW

Version: 6.1.9, 7.0.1, 7.1.0

NGFW позволяет использовать как статическую, так и динамическую маршрутизацию. Динамическая маршрутизация осуществляется по протоколам OSPF и BGP, что позволяет использовать NGFW в сложной маршрутизируемой сети предприятия.

Администратор может создавать в системе правила NAT (для предоставления пользователям доступа в интернет), а также правила безопасной публикации внутренних ресурсов в интернет с использованием reverse-прокси для HTTP/HTTPS и DNAT для других протоколов.

Аутентификация и авторизация пользователей

Documentation: ☒

Product: NGFW

Version: 7.x

Платформа поддерживает различные механизмы аутентификации пользователей: Captive-портал, Kerberos, NTLM, при этом учетные записи могут поступать из различных источников — LDAP, Active directory, FreeIPA, TACACS+, RADIUS, SAML IDP. Аутентификация SAML IDP, Kerberos или NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory на устройстве UserGate. В Captive-портале также возможна аутентификация пользователей посредством сертификатов, использующих инфраструктуру открытых ключей (PKI).

Благодаря функциональности UserID возможна прозрачная аутентификация пользователей на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Active Directory, syslog и сообщения RADIUS accounting. Для этого агент UserID осуществляет запросы посредством протокола WMI на серверы AD, в сценарии с syslog осуществляет прослушивание порта syslog и сбор информации, которую присылают серверы syslog, а в сценарии с RADIUS-серверами принимает сообщения RADIUS accounting от серверов NAS. Далее информация фильтруется по событиям входа/выхода пользователей. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя отправляются на все устройства UserGate, указанные в Профиле редистрибуции источника и производится вход пользователя на NGFW.

Администратор может настроить правила безопасности, ширину канала, правила межсетевого экранирования, контентной фильтрации и контроля приложений для отдельных пользователей, групп пользователей, а также всех известных или неизвестных пользователей. Дополнительно к этому продукт поддерживает применение правил безопасности к пользователям терминальных служб с помощью специальных агентов (Terminal Services Agents), а также использование агента авторизации для Windows-платформ.

Для обеспечения большей безопасности учетных записей рекомендуется использовать мультифакторную аутентификацию с помощью токенов TOTP (Time-based One Time Password Algorithm), SMS или электронной почты.

Поддержка гостевого портала

Documentation: ☒

Product: NGFW

Version: 6.1.9, 7.0.1, 7.1.0

NGFW позволяет предоставлять пользователям временный доступ к сети, что актуально, например, для публичных Wi-Fi сетей. Профили могут быть как созданы администратором, так и зарегистрированы самими пользователями с подтверждением через email или SMS. Платформа позволяет указывать отдельные настройки безопасности для временных пользователей.

Проксирование приложений

Documentation: ☒

Product: NGFW

Version: 6.1.9, 7.0.1, 7.1.0

Для пользователей, работающих с ОС Windows, можно настроить прокси-агент, позволяющий использовать возможности прокси приложениям, не умеющим работать с прокси-серверами. Прокси-агент также может быть использован для предоставления таким приложениям доступа в интернет в случаях, когда NGFW не является шлюзом по умолчанию.

Перенаправление трафика на вышестоящий прокси-сервер

Documentation: ☒

Product: NGFW

Version: 7.1.0

С помощью функциональности Upstream proxy UserGate NGFW позволяет перенаправлять пользовательский трафик на вышестоящий прокси-сервер, благодаря чему возможно создание каскадной иерархии, когда трафик с одного прокси-сервера передается на следующий в цепочке прокси-серверов. Подобное каскадирование обычно используется для обеспечения конфиденциальности коммуникаций или для организации доступа к контенту с региональными ограничениями. Также благодаря технологии каскадирования упрощается встраивание новых региональных офисов в существующую иерархию глобальной сети компании.

Журналы и отчеты(описание)

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Платформа позволяет осуществлять мониторинг работы системы в режиме реального времени при помощи журналов событий, веб-доступа, СОВ и трафика. Для удобства анализа администратор может настроить автоматический экспорт журналов на сервера SSH, FTP и Syslog. С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Интернет-фильтрация

Documentation: ☒

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Использование модуля интернет-фильтрации обеспечивает административный контроль за использованием интернета, загружаемыми данными. Модуль обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

Для анализа безопасности сайтов, запрашиваемых пользователями, используются репутационные сервисы, типы контента (фото, видео, тексты и др.), специальные морфологические словари, предоставляемые UserGate, а также черные и белые списки URL и Useragent, с помощью которых администратор может запретить или разрешить работу с определенным типом браузеров. NGFW предоставляет возможность создавать собственные черные и белые списки, словари, типы контента, морфологические словари и Useragent, применяя их как правила к пользователям и группам пользователей.

Выборочная блокировка рекламы

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☒

Даже безопасные сайты могут содержать нежелательные изображения на баннерах, содержимое которых не зависит от владельца ресурса. UserGate NGFW решает эту проблему, блокируя баннеры и защищая пользователей от негативного контента.

Активация безопасного поиска

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☒

NGFW позволяет принудительно активировать функцию безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. Такая защита позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту. Также можно заблокировать поисковые системы, в которых не реализована функция безопасного поиска.

Блокировка приложений социальных сетей

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Documentation: ☒

NGFW дает возможность блокировки игр и других приложений для наиболее популярных социальных сетей, таких, как Facebook, VK, Одноклассники. Администраторы могут разрешать использование социальных сетей в целом, при этом контролируя и ограничивая непродуктивные действия.

Инжектирование кода на веб-страницы

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователями. Эта возможность может быть использована для получения различных метрик, сокрытия некоторых элементов веб-страниц, а также показа рекламы или другой информации.

Инспектирование SSL-трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

UserGate NGFW позволяет фильтровать не только обычный, но и зашифрованный трафик (протоколы HTTPS, SMTPS, POP3S), дешифруя их при помощи технологии MITM (Man In The Middle) и подписывая доверенным корневым сертификатом с последующим шифрованием после анализа. Система позволяет настроить выборочную проверку трафика, например, не расшифровывать ресурсы категории «Финансы».

VPN и веб-портал

Version: 7.1.0

Product: NGFW

Documentation: 

VPN (Virtual Private Network) служит для того, чтобы настраивать виртуальные логические сети поверх других сетей, например, интернет. UserGate NGFW поддерживает два типа VPN-сетей: Remote Access VPN (модель клиент-сервер) и Site-to-Site VPN (модель сервер-сервер).

Для создания защищенных туннелей используются протоколы L2TP/IPsec или IKEv2/IPsec. UserGate имеет собственный VPN клиент UserGate Client, также поддерживается работа со стандартными клиентами большинства популярных операционных систем: Windows, Linux, Mac OS X, iOS, Android и других.

Веб-портал (SSL VPN) позволяет предоставить безопасный доступ сотрудникам компании к внутренним веб-ресурсам, серверам SSH и серверам терминальных служб без необходимости установки специального клиента VPN, используя только протокол HTTPS.

Другие функции

Функция балансировщика нагрузки

Documentation: 

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

NGFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена для внутренних серверов, публикуемых в интернет (DNAT или reverse-прокси), внутренних серверов без публикации.

DNS-фильтрация

Documentation: 

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

NGFW позволяет осуществлять настройку работы с DNS-серверами, а также настраивать сервис DNS-прокси, позволяющий перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Платформа также позволяет подключить фильтрацию DNS-запросов пользователей.

Использование оповещений

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

UserGate NGFW поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается как управление с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps).

Помимо этого, система позволяет создавать профили оповещений, уведомляющие пользователей об определенных событиях по протоколам SMTP (email) и SMPP (SMS).

Ролевой доступ администраторов к элементам управления UserGate NGFW

Documentation: ☒

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

По умолчанию в системе существует один суперадминистратор, который может создавать учетные записи других администраторов и выдавать им права на просмотр и изменение различных разделов.

Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Типы интерфейсов

Documentation: 

Product: NGFW

Version: 7.1.x

UserGate NGFW позволяет добавлять и настраивать тегированные VLAN-интерфейсы, а также объединять ряд физических интерфейсов в один логический агрегированный интерфейс (бонд) с использованием протокола LACP (link aggregation control protocol) для повышения пропускной способности или для отказоустойчивости канала.

Существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании. Если мост создается в ПАК NGFW, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить два интерфейса в байпас-мост. Подробнее читайте в разделе [Настройка интерфейсов](#).

Алгоритм обработки трафика

UserGate NGFW 7 Packet Flow

Documentation: ☒

Product: NGFW

Version: 7.1.x

В данной статье представлен обобщённый высокоуровневый алгоритм обработки трафика (packet flow), реализованный в UserGate NGFW версии 7.1.x.

Пакеты трафика проходят три основные стадии обработки:

1. Стадия предварительной обработки входящего трафика (Ingress).
2. Стадия обработки политиками сети и политиками безопасности (Policy processing).
3. Стадия завершающей обработки исходящего трафика (Egress).

На стадии предварительной обработки трафик подвергается базовым проверкам от DoS-атак и IP-спуфинга, маркируется для дальнейшей обработки, при необходимости происходит распаковка и дешифрация пакетов IPsec VPN, подмена адресов и портов назначения.

На стадии обработки политиками в зависимости от сценариев обработки трафика и наличия соответствующих правил происходит инспектирование трафика, фильтрация контента, проверка потоковым антивирусом, обработка правилами межсетевого экрана, COV и фильтрации приложений (L7).

На стадии завершающей обработки исходящий трафик обрабатывается правилами управления пропускной способности, подмены исходящих адресов (SNAT), при необходимости происходит инкапсуляция и шифрование IPsec VPN и передача пакетов в выходной интерфейс.

В общем случае путь прохождения пакетов через UserGate NGFW можно представить с помощью следующей функциональной диаграммы:

Диаграмма описывает обобщённый путь прохождения пакетов через NGFW. При этом пакеты могут не подвергаться обработке или изменениям во всех функциональных блоках, представленных на диаграмме. Это зависит от типа пакета, настроек функциональности NGFW и сценариев прохождения трафика.

Далее будут рассмотрены следующие сценарии обработки трафика в UserGate NGFW:

- Транзит трафика без фильтрации контента.
- Прозрачный прокси с фильтрацией контента.
- Явный прокси.
- Трафик DNAT/порт-форвардинг.
- Трафик через reverse-прокси.
- Публикация ресурсов через веб-портал.

Транзит трафика без фильтрации контента

Путь прохождения пакетов транзитного трафика без фильтрации контента на функциональной диаграмме обозначен с помощью цветовой маркировки:

Стадия предварительной обработки входящего трафика (Ingress)

Пакеты, пришедшие на входной интерфейс NGFW, попадают под действие правил зоны — в блок **DoS, Spoofing**. Если в настройках зоны включены соответствующие параметры, на этом этапе производится базовая проверка трафика на наличие DoS-атак или выявление аномалий трафика по выставленным порогам уведомлений/отбрасывания пакетов и правилам агрегирования, также в этом блоке проверяются условия защиты от IP-спуфинга. Уже на этом этапе может произойти отбрасывание пакета при срабатывании условий защиты.

Примечание Настройка защиты от DoS-атак в свойствах зоны является грубой. Более гибкая настройка с указанием сервисов и адресов производится с помощью правил защиты DoS.

Прошедшие далее пакеты помечаются (маркируются) для последующей обработки правилами политик сети и политик безопасности.

Если входящие пакеты определяются как пакеты, относящиеся к VPN туннелю, совпадающему с настройками на NGFW, производится их распаковка и расшифровка в условном блоке **IPsec VPN decryption**. В случае возникновения ошибок при расшифровке пакеты отбрасываются.

В блоке **NAT** происходит проверка наличия правил подмены IP-адресов и портов. При отсутствии правил с совпавшими условиями пакеты проходят блок без изменений.

В условном блоке **User auth** производится аутентификация пользователей со статусом Unknown.

Стадия обработки политиками сети и политиками безопасности (Policy processing)

В блоке с условным названием **Check** происходит проверка трафика на предмет соответствия условиям политик безопасности. Если трафик не попадает под условия правил инспектирования, контентной фильтрации, принадлежности сервисам ICAP и защиты почтового трафика, созданных на NGFW, то пакеты проходят дальше в блок лицензирования, откуда попадают в блок **Routing**, где происходит проверка всех записей подключённых сетей, проверка доступности шлюзов, проверка записей (статических и динамических) виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка транзитного трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, данные начинают анализироваться сигнатурами профилей безопасности COB и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COB не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Стадия завершающей обработки исходящего трафика (Egress)

В блоке **Shaper** происходит настройка пропускной способности исходящего трафика при наличии соответствующих правил.

В блоке **NAT** при наличии соответствующего совпавшего правила происходит обработка пакета и подмена адреса источника в исходящем пакете (SNAT).

При наличии соответствующих правил исходящие пакеты инкапсулируются и шифруются в условном блоке **IPsec VPN encryption**.

Далее пакеты передаются на выходной интерфейс.

Функция быстрой обработки сетевых пакетов

В UserGate NGFW реализована функция быстрой обработки сетевых пакетов (**FastPath**). Принцип такой обработки прост: если сессия уже установлена и остальные пакеты сессии по какой-то причине не требуют проверки и специальной обработки, то их можно сразу перенаправлять со входного интерфейса в выходной, выполнив необходимые соответствующие преобразования (DNAT, Port forwarding итд.).

Функция FastPath активирована по умолчанию. Сброс правил модуля осуществляется одновременно со сбросом сессий в межсетевом экране. Для этого на странице **Политики сети** → **Межсетевой экран** доступна кнопка **Принудительно применить**.

Функция FastPath выключается автоматически при записи трафика. Под обработку модуля не попадают фрагментированные пакеты и пакеты, предназначенные для COV/L7 инспектирования.

Статус функции можно проверить с помощью команды CLI:

```
Admin@nodename# show settings fastpath
```

```
enabled    : on
```

Отключить функцию можно командой:

```
Admin@nodename# set settings fastpath enabled
```

```
+ on      Enable
```

```
+ off     Disable
```

Прозрачный прокси с фильтрацией контента

Режим прозрачного прокси применяется к транзитному трафику, проходящему через NGFW. В режиме прозрачного прокси NGFW является посредником между клиентом и конечным сервером, выполняющим обработку и перехват трафика в соответствии с настроенными политиками безопасности.

В случае использования режима прозрачного прокси NGFW по умолчанию будет анализировать TCP-пакеты, отправляемые по портам 80 (HTTP) и 443 (HTTPS).

При наличии правил защиты почтового трафика NGFW также будет анализировать TCP-пакеты по портам, указанным в правилах защиты почтового трафика. Это могут быть как стандартные порты 110 (POP3) / 995 (POP3S) / 25 (SMTP) / 465 (SMTPS), так и выбранные администратором порты, добавленные в настройки используемых в правилах сервисов.

Путь прохождения пакетов в режиме прозрачного прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:

Стадия предварительной обработки входящего трафика (Ingress)

Путь прохождения пакетов в стадии предварительной обработки в целом аналогичен пути, описанному [ранее](#).

Стадия обработки политиками сети и политиками безопасности (Policy processing)

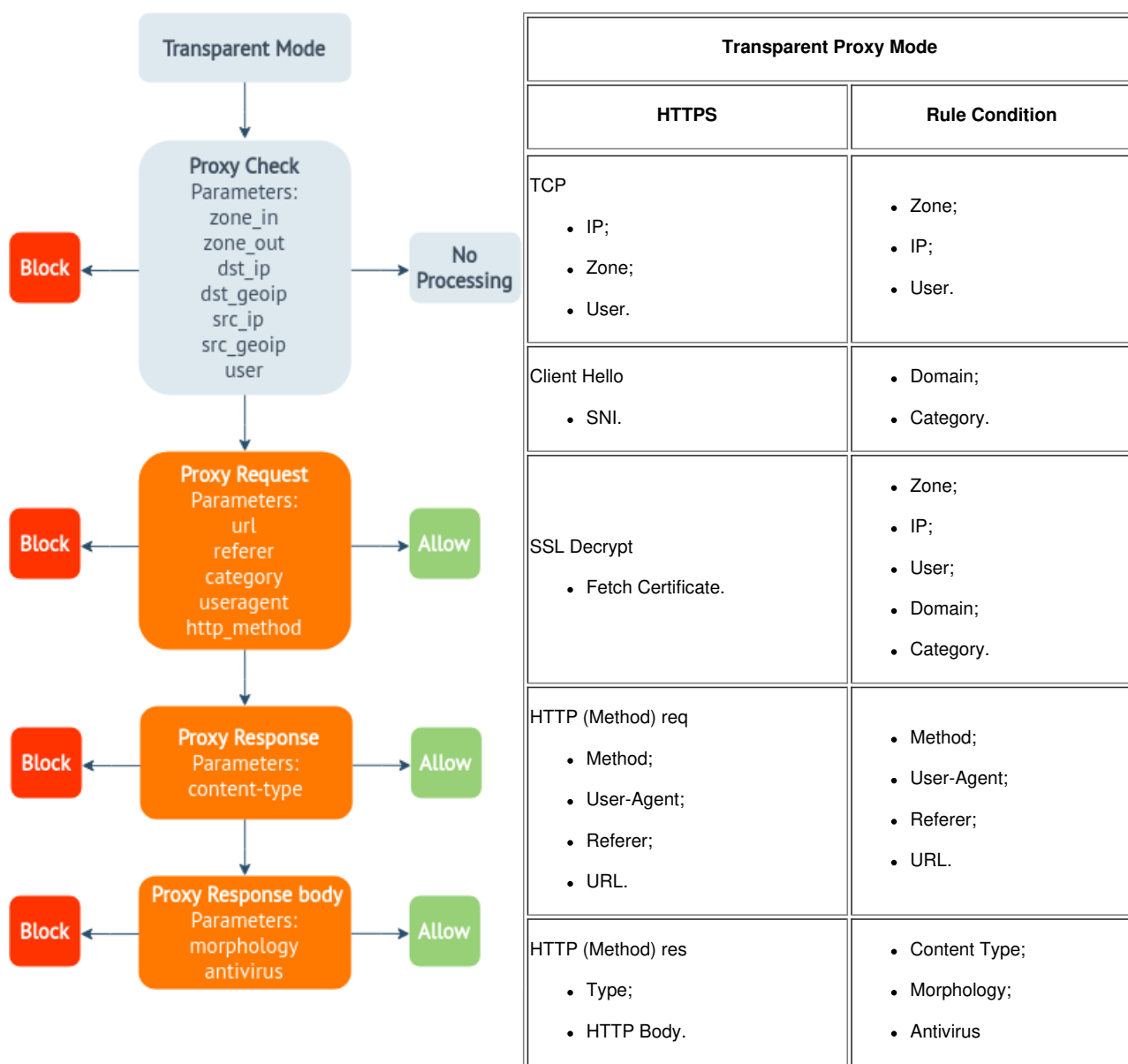
В режиме прозрачного прокси из всего потока в обработку модулем **Local Process** попадает только трафик, удовлетворяющий условиям политик, настроенных на NGFW.

Перехват трафика модулем Local Process осуществляется на финальной стадии установления TCP-соединения, т.е. на последнем этапе «трёхстороннего рукопожатия» (three-way handshake).

Изначально, на этапе установления TCP-соединения, пакеты доходят до межсетевого экрана и проверяются правилами политик сети. При наличии блокирующего пользовательского правила, под которое попадают эти пакеты, они будут отброшены и TCP-соединение не будет установлено. В случае отсутствия разрешающих пользовательских правил все пакеты будут отброшены правилом межсетевого экрана Default Block, созданным по умолчанию.

Если трафик не был заблокирован правилами межсетевого экрана на этапе установления TCP-соединения, то происходит проверка соответствия условиям правил контентной фильтрации.

Проверка соответствия условиям правил инспектирования, контентной фильтрации осуществляется путём поэтапного анализа трафика в соответствии с параметрами алгоритма блока **CHECK**:



- Если трафик попадает под какое-либо правило контентной фильтрации, то происходит проверка соответствия условиям правила, запрещающим трафик по зонам, адресам источников/назначений и/или пользователям. В случае соответствия NGFW заблокирует данное соединение и отобразит страницу блокировки.
- В случае отсутствия блокирующих правил контентной фильтрации по зонам, адресам источников/назначений или пользователям NGFW проверяет наличие правил фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.). Если таких правил нет, то блок Proxy Check пропускает трафик дальше без обработки. Если такие правила есть, блок Proxy Check пропускает трафик без обработки, но продолжает его отслеживать до установления TLS-сессии.
- После получения сообщения **Client Hello**, содержащего SNI, доступна фильтрация по доменам и категориям сайтов.
- Если настроено инспектирование SSL, то на этом же этапе происходит проверка сертификата (корректность сертификата, срок действия и т.д.). Настройка правил инспектирования доступна по зонам, адресам, пользователям, категориям URL, доменам.
- Если на данном этапе блокировка не произошла, то далее NGFW получает от пользователя **HTTP Request** (GET, PUT и т.д.), из которого можно получить информацию о реферере, URL, Useragent браузера, методе HTTP. Соответственно, эти же параметры могут быть использованы в качестве параметров фильтрации при настройке политик. На этом этапе доступна работа с URL. Поэтому, если трафик не расшифровывается, то доступна только фильтрация по доменным именам.
- При получении ответа от сервера (**HTTP Response**) доступна информация о типе контента (содержится в заголовке **HTTP Response**) и тело сообщения. Соответственно, на данном этапе доступна фильтрация по типу контента, проверка морфологии, а также работает потоковый антивирус UserGate.

Если после проверки соответствия политикам NGFW трафик не был заблокирован, то он будет передан в блоки **License** (лицензирование трафика), **Routing** (проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов).

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COB и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COB не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать

сигнатурами профиля.

Примечание Т.к. в режиме прозрачного прокси из всего потока в обработку попадает только трафик, удовлетворяющий условиям политик, настроенных на NGFW, то этот режим является более производительным при большом потоке веб-трафика по отношению к режиму явного прокси.

Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Явный прокси

В режиме явного прокси весь трафик направлен на NGFW. На стороне клиента в веб-браузере или в других приложениях в явном виде указывается адрес и порт прокси-сервера NGFW (порт 8090 по умолчанию).

В момент запроса клиентом внешнего ресурса формируется две TCP-сессии:

- Первая сессия: КЛИЕНТ — NGFW. Обращение от клиента происходит непосредственно к NGFW и начинается с HTTP Connect.
- Вторая сессия: NGFW — КОНЕЧНЫЙ СЕРВЕР. При этом трафик от NGFW до сервера является транзитным для блока **Firewall** (если настроено запрещающее правило по IP-адресу назначения, т.е. указан адрес конечного сервера, то трафик будет заблокирован).

Примечание Для использования NGFW в режиме явного прокси необходимо в настройках доступа зоны разрешить сервис HTTP(s)-прокси, иначе пакет будет отброшен.

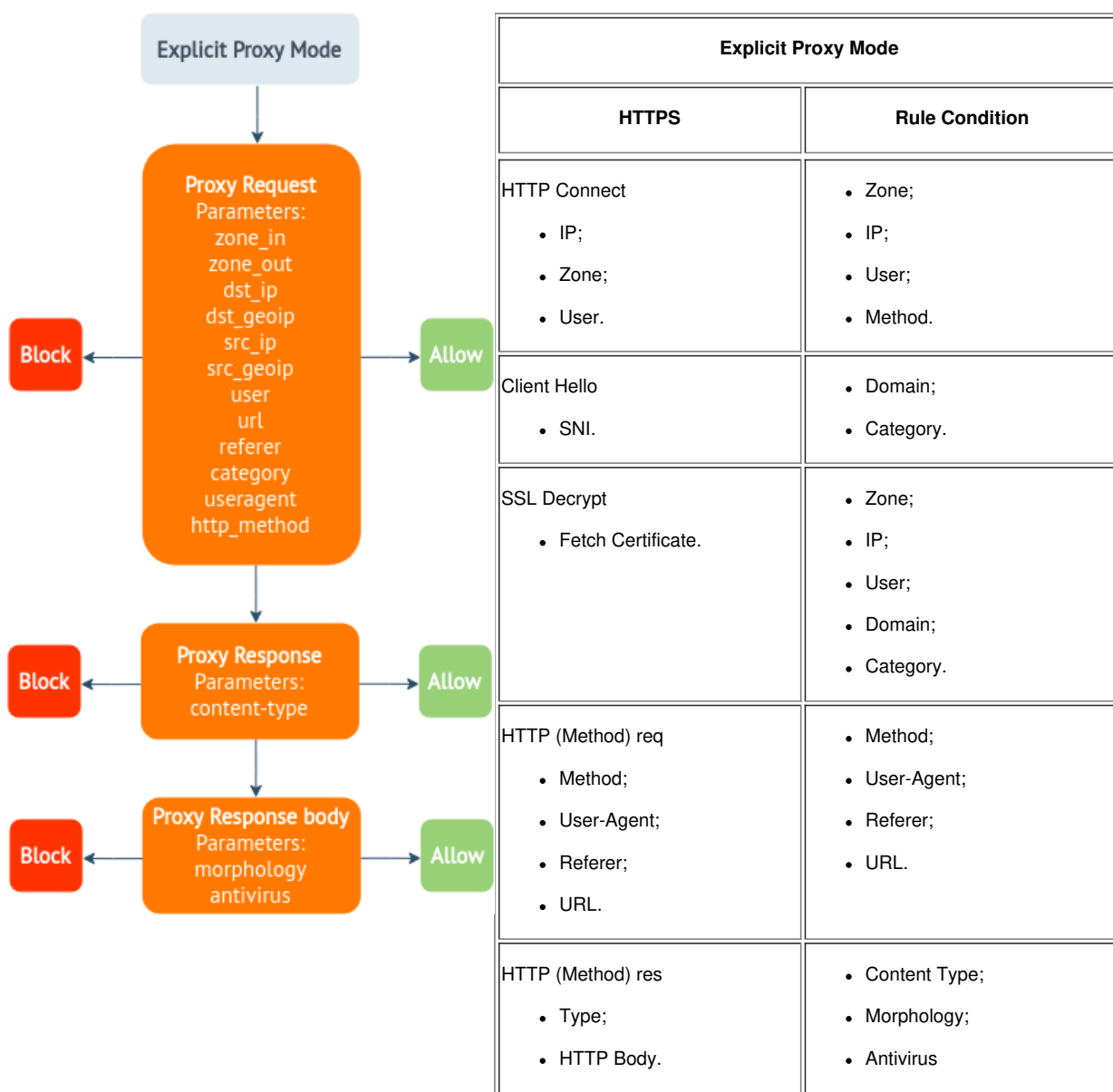
Путь прохождения пакетов в режиме явного прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:

Стадия предварительной обработки входящего трафика (Ingress)

Путь прохождения пакетов в стадии предварительной обработки в целом аналогичен пути, описанному [ранее](#).

Стадия обработки политиками сети и политиками безопасности (Policy processing)

В блоке **CHECK** весь трафик будет проходить проверку соответствия условиям правил инспектирования, контентной фильтрации, а также принадлежности сервисам ICAP, reverse-прокси, веб-портала, АСУ ТП и защиты почтового трафика. Проверка осуществляется путём поэтапного анализа трафика в соответствии с параметрами алгоритма блока **CHECK**:



- В режиме явного прокси первое сообщение, которое NGFW получает от клиента — **HTTP Connect**, из которого можно извлечь информацию о зонах, адресах источника/назначения, пользователе.
- Если по таким параметрам, блокировка не происходит, то следующий пакет, который ожидает NGFW — это пакет **Client Hello**, с которым становится доступна идентификация по имени сервера (SNI). На основании SNI доступна фильтрация по доменам и категориям сайтов.
- Если настроено инспектирование SSL, то на этом же этапе происходит проверка сертификата (корректность сертификата, срок действия и т.д.). Настройка правил инспектирования доступна по зонам, адресам, пользователям, категориям URL, доменам.
- Если на данном этапе блокировка не произошла, то далее NGFW получает от пользователя **HTTP Request** (GET, PUT и т.д.), из которого можно получить информацию о реферере, URL, Useragent браузера, методе HTTP. Соответственно, эти же параметры могут быть использованы в качестве параметров фильтрации при настройке политик. На этом этапе доступна работа с URL. Поэтому, если трафик не расшифровывается, то доступна только фильтрация по доменным именам.
- При получении ответа от сервера (**HTTP Response**) доступна информация о типе контента (содержится в заголовке **HTTP Response**) и тело сообщения. Соответственно, на данном этапе доступна фильтрация по типу контента, проверка морфологии, а также работает потоковый антивирус UserGate.

После обработки в блоке **CHECK** трафик будет направлен в блок лицензирования трафика (**License**). В блоке **Routing** происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COB и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COB не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Трафик DNAT/порт-форвардинг

Трафик DNAT/порт-форвардинг является транзитным и подчиняется созданным правилам фильтрации межсетевого экрана, к нему могут применяться правила инспектирования и, соответственно, фильтрации контента при определённых условиях.

Путь прохождения пакетов трафика DNAT на функциональной диаграмме обозначен с помощью цветовой маркировки:

Стадия предварительной обработки входящего трафика (Ingress)

Пакеты, пришедшие на входной интерфейс NGFW, попадают под действие правил зоны — в блок **DoS, Spoofing**. Если в настройках зоны включены соответствующие параметры, на этом этапе производится базовая проверка трафика на наличие DoS-атак или выявление аномалий трафика по выставленным порогам уведомлений/отбрасывания пакетов и правилам агрегирования, также в этом блоке проверяются условия защиты от IP-спуфинга. Уже на этом этапе может произойти отбрасывание пакета при срабатывании условий защиты.

Прошедшие далее пакеты помечаются (маркируются) для последующей обработки правилами политик сети и политик безопасности.

Если входящие пакеты определяются как пакеты, относящиеся к VPN туннелю, совпадающему с настройками на NGFW, производится их распаковка и расшифровка в условном блоке **IPsec VPN decryption**. В случае возникновения ошибок при расшифровке пакеты отбрасываются.

В блоке **NAT** при совпадении условий соответствующего правила происходит подмена адреса назначения (порта — в случае порт-форвардинга).

В условном блоке **User auth** производится аутентификация пользователей со статусом Unknown.

Стадия обработки политиками сети и политиками безопасности (Policy processing)

Анализ трафика начинается на этапе установления TCP-соединения с портами назначения 80 и 443. NGFW анализирует весь TCP-трафик, но его перехват осуществляет на финальной стадии установления надёжного TCP-соединения, т.е. на последнем этапе «трёхстороннего рукопожатия» (three-way handshake). Таким образом, первые пакеты пройдут путь до блока **Firewall** и будут отброшены в случае наличия запрещающего правила, под условия которого подходят эти пакеты. Правила межсетевого экрана, созданные по умолчанию (Default block), не применяются к трафику DNAT и порт-форвардинг.

Обработка трафика DNAT и порт-форвардинг проходит следующим образом:

- Проверяется соответствие трафика условиям правил фильтрации контента по зонам, адресам источника/назначения и/или пользователям.
- Если есть правила контентной фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.) и настроено SSL инспектирование, то NGFW ожидает установки TLS-сессии, после чего производит проверку соответствия.

В случае соответствия условиям блокирующего правила контентной фильтрации трафик будет заблокирован, а пользователю вернётся страница блокировки. Блокирующие правила межсетевого экрана не возвращают страницу блокировки.

В случае, если нет соответствия условиям блокирующих правил, трафик будет перенаправлен в блок **Routing**. В блоке **Routing** происходит проверка всех записей подключённых сетей, проверка доступности шлюзов, проверка записей (статических и динамических) виртуальных маршрутизаторов.

В блоке **Firewall** пакеты обрабатываются только в случае наличия правил, созданных администратором. Правилами по умолчанию (Default block) DNAT-трафик не обрабатывается.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COV и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COV не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Публикация ресурсов через reverse-прокси

С помощью правил reverse-прокси производится публикация серверов по протоколам HTTP/HTTPS.

Путь прохождения пакетов в режиме reverse-прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:

Обработка пакетов в целом аналогична режиму прозрачного прокси, но перехват включается сразу же при обращении к публикуемому серверу (без дополнительного анализа tcp-трафика для перехвата).

После сопоставления трафика политикам NGFW в блоке **CHECK** пакеты перенаправляются для обработки в блок **Local process** через блок **Zone Permission**. Для работы сервиса reverse-прокси в настройках доступа зоны необходимо разрешить сервис **Reverse-прокси**, иначе пакеты будут отброшены.

Трафик сервиса reverse-прокси не анализируется в блоке **License**, а сразу переходят в блок **Routing**, где происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COV и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COV не совпало ни одной сигнатуры, трафик передаётся дальше

без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Публикация ресурсов через веб-портал

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удалённых или мобильных пользователей, используя при этом только протокол HTTPS.

Путь прохождения пакетов в режиме веб-портала на функциональной диаграмме обозначен с помощью цветовой маркировки:

Обработка пакетов аналогична режиму прозрачного прокси, но перехват включается сразу же при обращении к веб-порталу (без дополнительного анализа tcp-трафика для перехвата).

После сопоставления трафика политикам NGFW в блоке **CHECK** пакеты перенаправляются для обработки в блок **Local process** через блок **Zone Permission**. Для работы сервиса веб-портала в настройках доступа зоны необходимо разрешить сервис **Веб-портал**, иначе пакеты будут отброшены.

Трафик сервиса веб-портала не анализируется в блоке **License**, а сразу переходит в блок **Routing**, где происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов. Далее трафик передаётся на выходной интерфейс.

Совместимость с аппаратными платформами

Совместимость версий UserGate NGFW с аппаратными платформами

Product: NGFW

Version: 7.x

В таблице представлена матрица совместимости версий UserGate NGFW с моделями аппаратных платформ.

Важно! Доступность тех или иных версий продукта зависит от используемой аппаратной платформы. Перед обновлением обязательно сверьтесь с матрицей совместимости для вашего устройства.

[illegible]

