

Table of Contents

Table of Contents	1
Введение	2
Безопасность сети и защита от сетевых угроз	3
Настройка политик безопасности при помощи сценариев	4
Управление АСУ ТП	5
Работа с внешними системами безопасности	6
Проверка почтового трафика	7
Антивирусная проверка трафика	8
Защита от DOS-атак и сетевого флуда	9
Обнаружение и предотвращение вторжений	10
Межсетевое экранирование	11
Улучшение производительности и надежности интернета	12
Поддержка WCCP	13
Управление пропускной способностью	14
Поддержка нескольких провайдеров	15
FTP поверх HTTP	16
Поддержка кластеризации и отказоустойчивости	17
Управление трафиком и контроль доступа в интернет	18
Поддержка политики BYOD	19
Проксирование приложений	20
Поддержка гостевого портала	21
Аутентификация и авторизация пользователей	22
Маршрутизация трафика и публикация ресурсов	23
Контент-фильтрация и контроль приложений	24
VPN и веб-портал	25
Инспектирование SSL-трафика	26
Инжектирование кода на веб-страницы	27
Блокировка приложений социальных сетей	28
Активация безопасного поиска	29
Выборочная блокировка рекламы	30
Интернет-фильтрация	31
Журналы и отчеты	32
Журналы и отчеты(описание)	33
Другие функции	34
Функция балансировщика нагрузки	35
DNS-фильтрация	36
Типы интерфейсов	37
Использование оповещений	38
Ролевой доступ администраторов к элементам управления UserGate NGFW	39
Алгоритм обработки трафика	40
UserGate NGFW 6 Packet Flow	41
Совместимость с аппаратными платформами	44

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 приоритизировать сценарии для скорейшей реакции на критичные угрозы.

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: 

В новой версии платформы появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП) и управления ей. Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий. Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

Работа с внешними системами безопасности

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

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.

Проверка почтового трафика

Documentation: 

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

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.

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.

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.

Обнаружение и предотвращение вторжений

Version: 7.0.1, 6.1.9, 5.x

Documentation: 

Система обнаружения и предотвращения вторжений (СОВ) 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 различные СОВ-профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила СОВ, определяющие действия для выбранного типа трафика, который будет проверяться модулем СОВ в соответствии с назначенными профилями.

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.

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.

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 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.

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 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.

Поддержка политики BYOD

Documentation: 

Product: UserGate NGFW

Version: 6.1.9

Концепция BYOD (Bring Your Own Device) продолжает набирать популярность, ставя перед системами безопасности новые задачи. UserGate позволяет настроить гибкие политики доступа в сеть для различных групп пользователей и типов устройств, а также ограничить количество устройств, используемых одним пользователем.

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.

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.

Аутентификация и авторизация пользователей

Documentation: 

Product: UserGate NGFW

Version: 6.1.9, 7.0.1

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 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.

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.

Version: 5.x, 6.1.9, 7.0.1

Documentation: 

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

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. NGFW поддерживает работу 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.

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».

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.

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.

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.

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.

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.

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, COV 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.

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.

Типы интерфейсов

Documentation: 

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1

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. Помимо этого, существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

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.

UserGate NGFW 6 Packet Flow

Product: UserGate NGFW

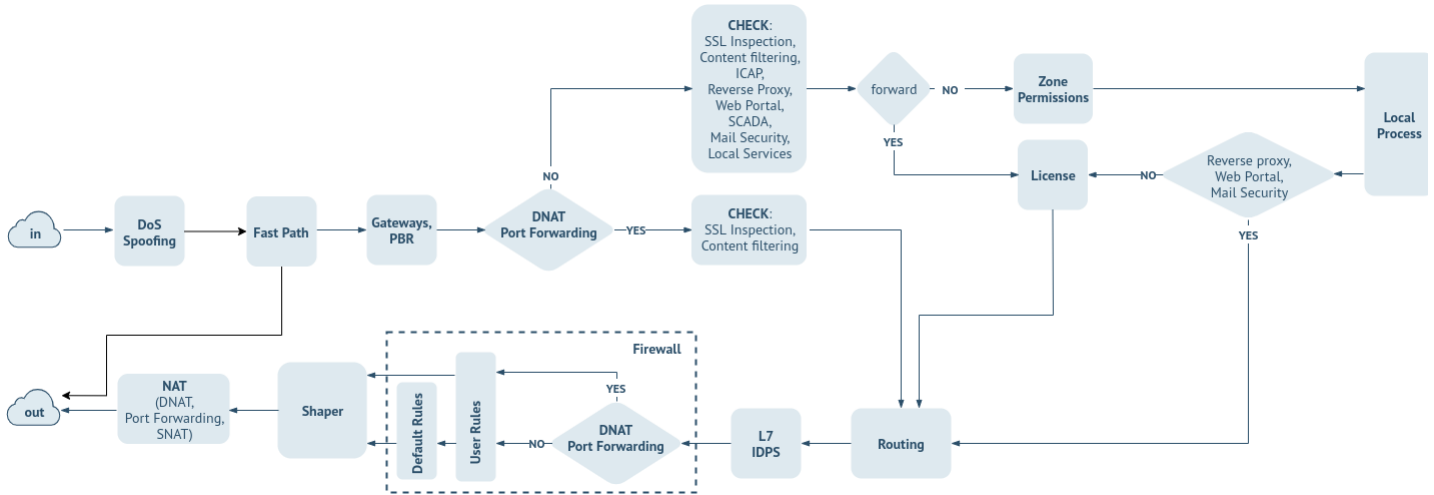
Version: 6.x

Technology: Networking

В данной статье описан алгоритм обработки трафика (packet flow), представленный на схеме ниже. В зависимости от типа трафика и режима работы UserGate, порядок обработки может отличаться. В общем случае рассмотрим:

- Трафик **DNAT** - транзитный трафик; к трафику могут применяться правила инспектирования и, соответственно, фильтрации контента при определённых условиях.
- Transparent Proxy Mode** - работа сервера UserGate в режиме прозрачного прокси-сервера. В этом случае весь трафик является транзитным для UserGate и обрабатывается правилами модуля **Local Process** только в случае их наличия и соответствия условиям.
- Explicit Proxy Mode** - работа сервера UserGate в режиме явного прокси-сервера. В этом случае весь трафик направлен непосредственно на сервер UserGate и всегда обрабатывается правилами модуля **Local Process**.

В общем случае путь прохождения пакета выглядит следующим образом:



Трафик DNAT и Port Forwarding

После поступления на интерфейс UserGate пакет попадает под правила зоны - в блок **DoS, Spoofing**. На этом этапе производится базовая проверка трафика (например, на наличие атак). Уже на этом этапе может произойти отбрасывание пакета, например, по причине детектирования SYN-флуда, наличия аномалий трафика TCP, UDP или ICMP.

Примечание Зона - это логическая среда, объединяющая интерфейсы устройства под едиными для всех правилами.

Примечание Настройка защиты от DoS-атак на зоне является «грубой», т.к. в свойствах зоны настраиваются только параметры защиты зоны от сетевого флуда (порог уведомлений/отбрасывания пакетов, агрегирование) и защита от IP-спуфинга. «Гибкая» настройка - с указанием сервисов и адресов, производится с помощью правил защиты DoS.

Если пакет не был отброшен на предыдущем этапе, то далее он проходит блок **Fast Path**, который позволяет пропустить через все проверки и блоки только первые пакеты сессии. В дальнейшем если пакеты по какой-то причине не требуют проверки и специальной обработки, модуль **FastPath** формирует правило, которое перенаправляет пакет напрямую с входного интерфейса на выходной. При этом с такими пакетами выполняются все необходимые для доставки получателю преобразования (DNAT, PortForwarding и т.д.)

Примечание 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 *Fast Path* выключается автоматически, при записи трафика или при включении журналирования правил межсетевого экрана. Под обработку модуля не попадают фрагментированные пакеты и пакеты предназначенные для L7/IDPS инспектирования.

Примечание Для получения статуса модуля *FastPath* можно использовать команду CLI: *device config -get fastpath*

Отключить функцию можно командой *device config -set fastpath false*

Пакет не попавший под правила **FastPath**, следует дальше и попадает в блок **Gateways, PBR**, в котором помечается (маркируется) для дальнейшего использования в правилах маршрутизации.

Затем в блоке **DNAT, Port Forwarding** происходит обработка и подмена адреса назначения (источника в случае SNAT и порта в случае Port Forwarding), после которой пакет проходит далее, в блок с условным названием **CHECK**. Трафик DNAT и Port Forwarding подчиняется созданным правилам фильтрации межсетевого экрана.

Анализ трафика начинается на этапе установления TCP-соединения с портами назначения 80 и 443. UserGate 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.

Примечание Правила межсетевого экрана, созданные по умолчанию (Default Block), не применяются к трафику DNAT и Port Forwarding.

Обработка трафика DNAT и Port Forwarding проходит следующим образом:

- Проверка соответствия трафика условиям правил фильтрации контента происходит до проверки соответствия правилам межсетевого экрана. Если есть перекрёстные запрещающие правила по зонам, адресам источника/назначения и/или пользователям, то трафик будет заблокирован межсетевым экраном.
- Если есть правила контентной фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.) и настроено SSL инспектирование, то UserGate 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. Случаи возврата пользователю страницы блокировки рассмотрены в разделе [Отображение страницы блокировки](#).

Примечание Результатом блокирующих правил контентной фильтрации является отображение страницы блокировки на пользовательский запрос ресурса. Блокирующие правила межсетевого экрана не возвращают страницу блокировки.

В противном случае 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.

Далее пакет попадет в блок **L7, IDPS**, в котором проверяются используемые приложения, а также работает система обнаружения и предотвращения вторжений.

В блоке **Firewall** пакеты обрабатываются только в случае наличия правил, созданных администратором. Затем пакет проходит через блок **Shaper** (настройка пропускной способности), попадает в блок **NAT** (настройка правил NAT, DNAT, Policy-based routing, Port Forwarding и Network Mapping) и передаётся на выходной интерфейс.

Режим Explicit Proxy

Поступая на интерфейс, пакет проходит проверку соответствия правилам зоны в блоке **DoS, Spoofing**. Далее пакет обрабатывается в блоке **Gateways, PBR**, в котором помечается (маркируется) для дальнейшего использования в правилах маршрутизации.

Затем пакет без изменений проходит в блок с условным названием **CHECK**.

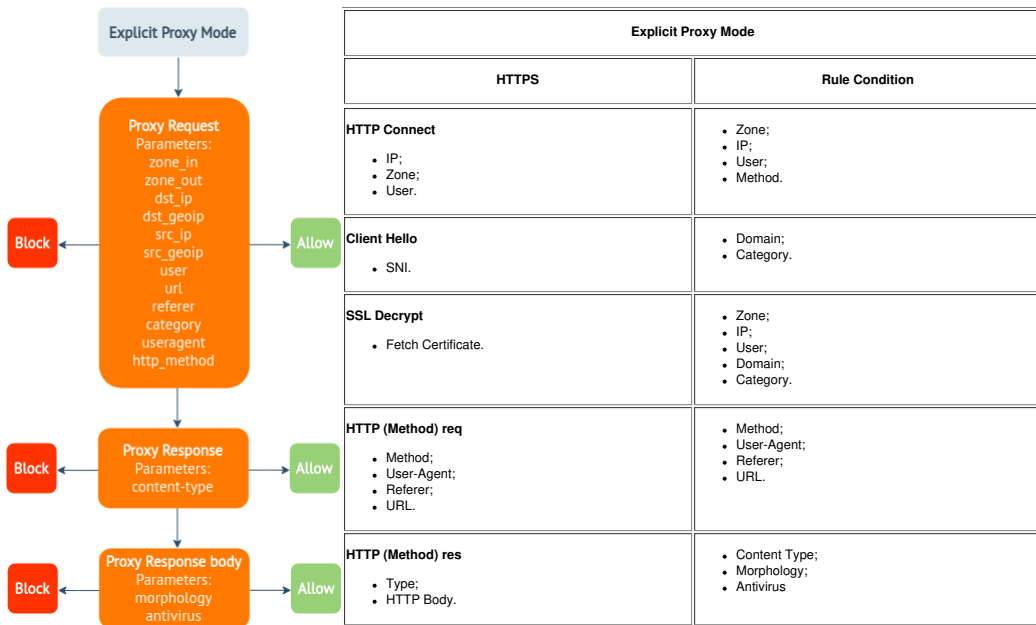
В блоке **CHECK** весь трафик будет проходить проверку соответствия условиям правил инспектирования, контентной фильтрации, а также принадлежности сервисам ICAP, reverse-прокси, веб-портала, АСУ ТП и защиты почтового трафика. Проверка осуществляется путём поэтапного анализа трафика в соответствии с параметрами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

В случае работы в режиме **Explicit Proxy** в момент запроса клиентом внешнего ресурса формируется 2 TCP-сессии:

- Первая сессия: КЛИЕНТ - USERGATE - обращение от клиента происходит непосредственно к UserGate и начинается с HTTP Connect.
- Вторая сессия: USERGATE - КОНЕЧНЫЙ СЕРВЕР - при этом трафик от UserGate 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 UserGate режиме Explicit Proxy необходимо на зоне разрешить сервис HTTP(s)-прокси, иначе пакет будет отброшен.

Далее представлен алгоритм сопоставления трафика политикам UserGate при работе в режиме **Explicit Proxy**. Сопоставление происходит в блоке **CHECK**.



При работе в **Explicit Proxy Mode**, первое сообщение, которое UserGate получает от клиента - **HTTP Connect**, из которого можно извлечь информацию о зонах, адресах источника/назначения, пользователя. Если по таким параметрам, блокировка не происходит, то следующий пакет, который ожидает UserGate - 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 UserGate 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**); трафик сервисов reverse-прокси, веб-портала и защиты почтового трафика не проходит блок **License**, а сразу переходят в блок **Routing**, где происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов.

Далее пакет попадет в блоки **L7, IDPS** (проверка используемых приложений, также работает система обнаружения и предотвращения вторжений), **Firewall, Shaper** (настройка пропускной способности), **NAT** (настройка правил NAT, DNAT, Policy-based routing, Port Forwarding и Network Mapping) и передаётся на выходной интерфейс.

Режим Transparent Proxy

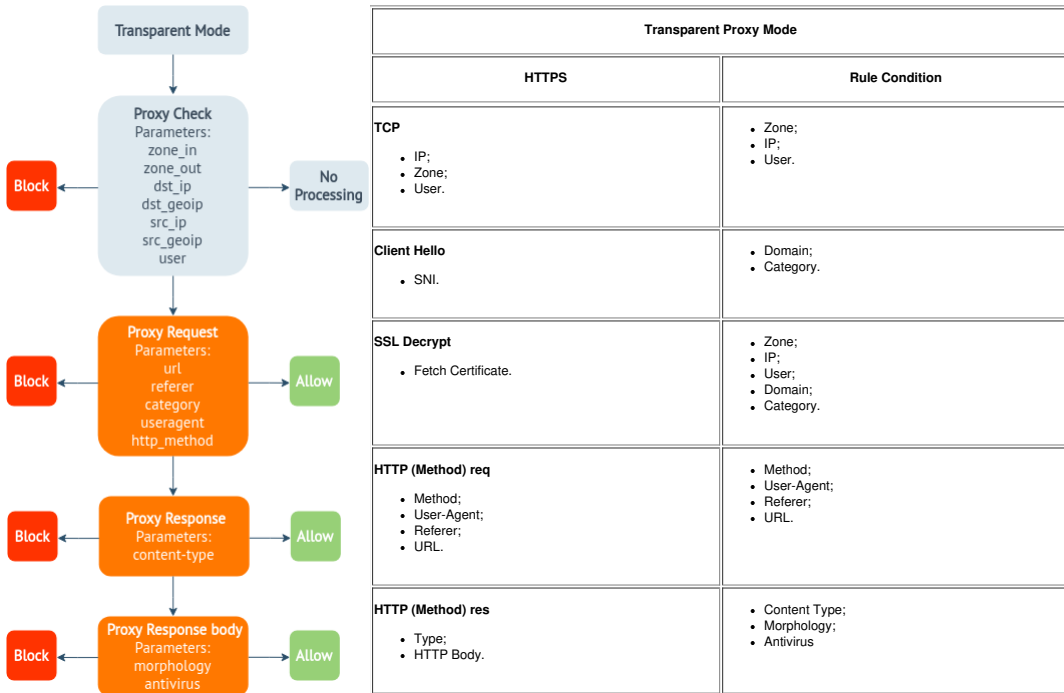
Поступая на интерфейс, пакет проходит проверку соответствия правилам зоны в блоке **DoS, Spoofing**. Далее пакет обрабатывается в блоке **Gateways, PBR**, в котором помечается (маркируется) для дальнейшего использования в правилах маршрутизации.

Затем пакет без изменений проходит в блок с условным названием **CHECK**.

В режиме **Transparent Proxy** UserGate является посредником между клиентом и конечным сервером, выполняющим обработку и перехват трафика в соответствии с настроенными на UserGate политиками.

В случае использования **Transparent Proxy Mode**, по умолчанию, UserGate будет анализировать TCP-пакеты, отправляемые по портам 80 и 443.

В **Transparent Proxy Mode** обработка в блоке **CHECK** происходит по следующей схеме:



UserGate анализирует весь TCP-трафик, но его перехват модулем **Local Process** осуществляется на финальной стадии установления надёжного TCP-соединения, т.е. на последнем этапе «трёхстороннего рукопожатия» (three-way handshake).

Примечание В случае отсутствия разрешающих клиентских правил все пакеты будут отброшены правилом межсетевого экрана Default Block, созданным по умолчанию.

- Если трафик не соответствует условиям правил инспектирования, контентной фильтрации, принадлежности сервисам ICAP и защиты почтового трафика, созданных на UserGate, то он будет перенаправлен в блоки **License, Routing** и далее.
- Если трафик не был заблокирован клиентскими правилами межсетевого экрана, то происходит проверка соответствия условиям правил контентной фильтрации, запрещающих трафик по зонам, адресам источников/назначений и/или пользователям. В случае соответствия UserGate блокирует данное соединение и отобразит страницу блокировки.
- В случае отсутствия блокирующих правил контентной фильтрации по зонам, адресам источников/назначений или пользователям UserGate проверяет наличие правил фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.). Если правил нет, то блок **CHECK** пропускает трафик дальше без обработки; если такие правила есть - блок **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 UserGate 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 UserGate трафик не был заблокирован, то он будет передан в блоки **License** (лицензирование трафика), **Routing** (проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов), **L7, IDPS** (проверка используемых приложений, также работает система обнаружения и предотвращения вторжений), **Firewall, Shaper** (настройка пропускной способности), **NAT** (настройка правил NAT, DNAT, Policy-based routing, Port Forwarding и Network Mapping) и передаётся на выходной интерфейс.

Т.к. в **Transparent Proxy Mode** из всего потока в обработку попадает только трафик, удовлетворяющий условиям политик, настроенных на UserGate, то **Transparent Proxy Mode** является более производительным при большом потоке веб-трафика по отношению к **Explicit Proxy Mode**.

