

Table of Contents

Table of Contents	1
Алгоритм обработки трафика	2
UserGate NGFW 7 Packet Flow	3

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)

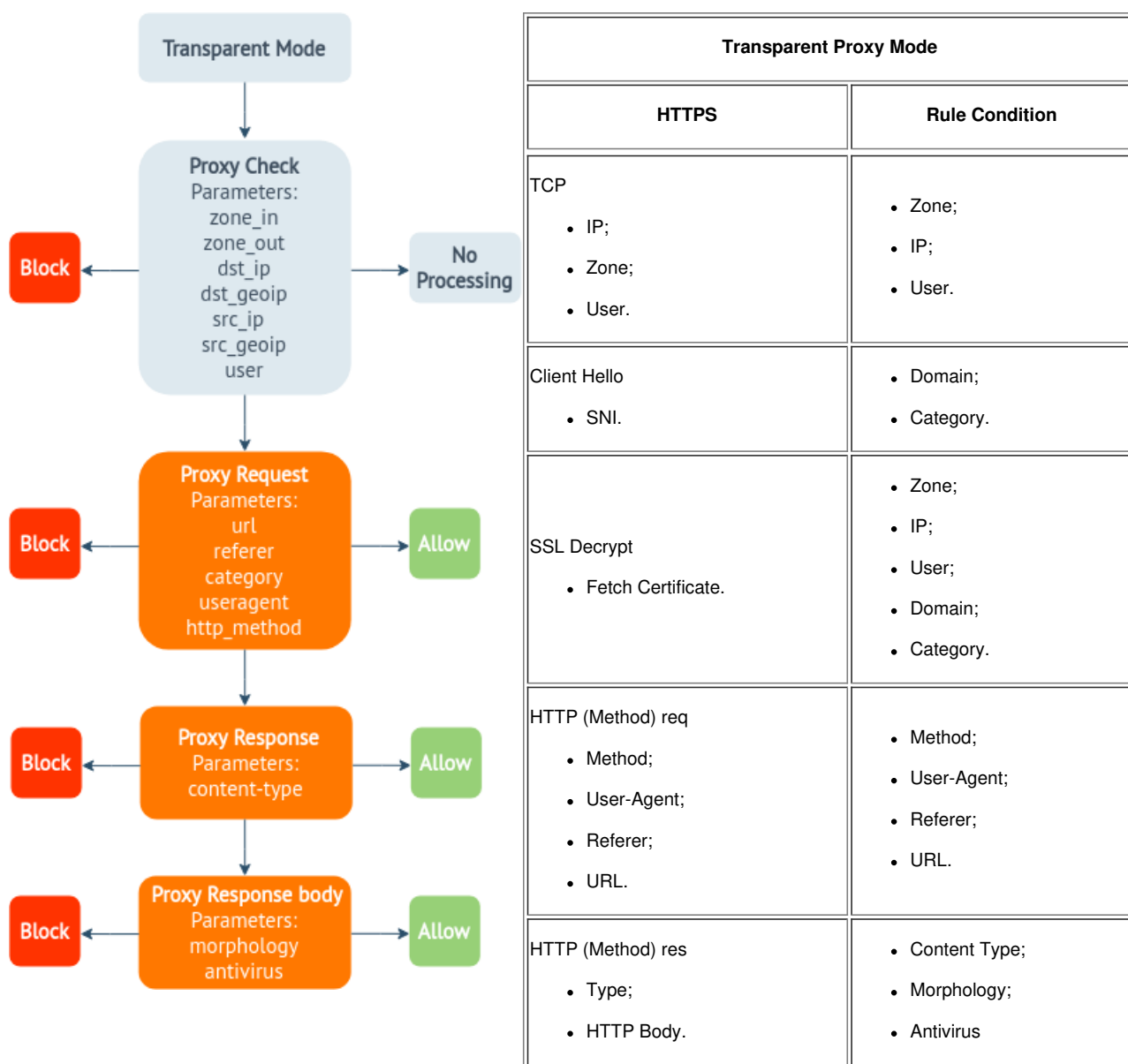
В режиме прозрачного прокси из всего потока в обработку модулем **Local Process** попадает только трафик, удовлетворяющий условиям политик, настроенных на NGFW.

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.

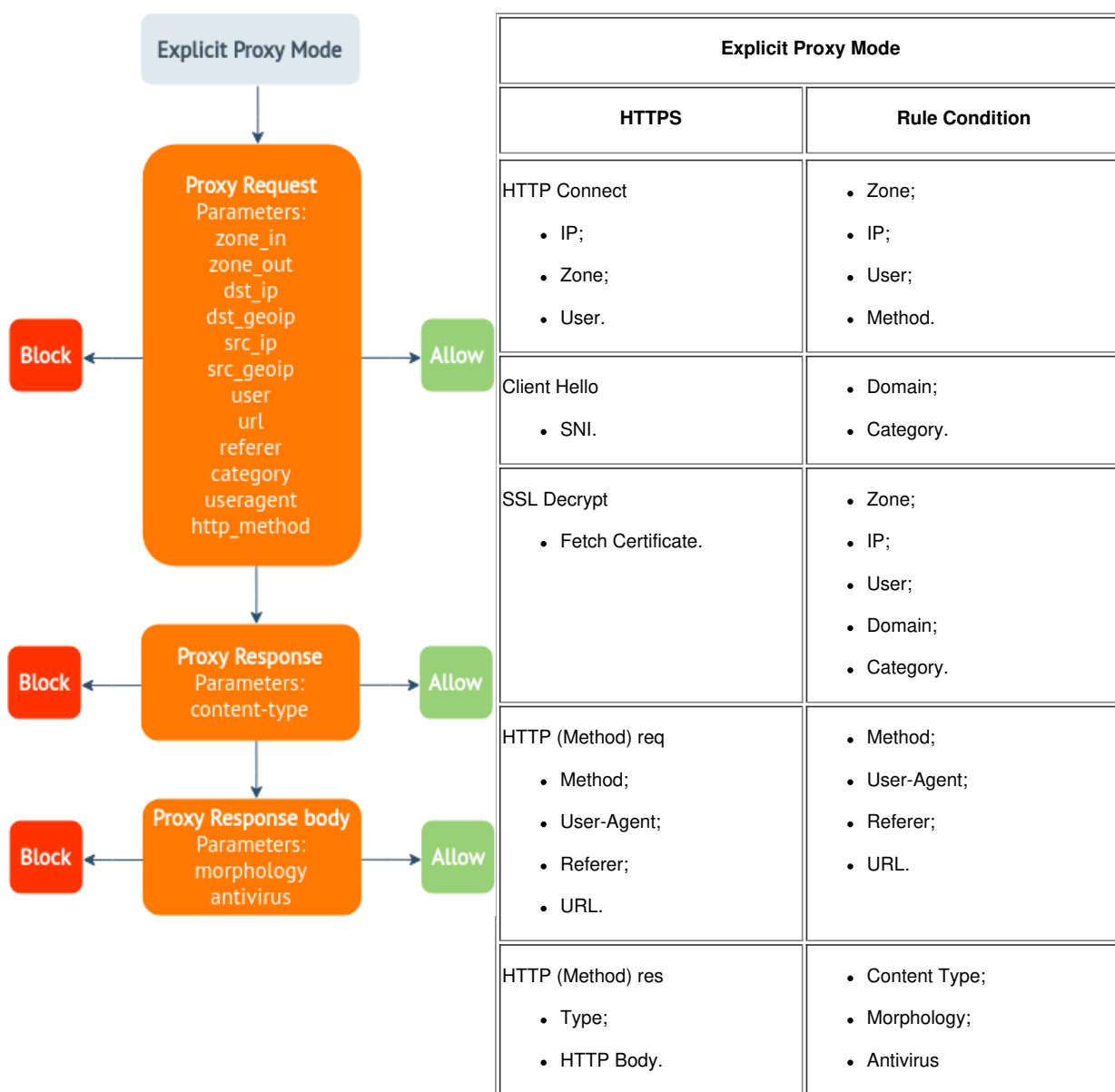
Путь прохождения пакетов в режиме явного прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:

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 соответствия 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.

