

Table of Contents

Table of Contents	1
Особенности работы	2
Особенности обработки списков IP и URL в правилах NGFW	3
Особенности реализации доступа к сервисам зон	4
Особенности работы межсетевого экрана UserGate	5
Формирование списков URL	6
Применение к пользователям политик UserGate	7
Алгоритм настройки защиты почтового трафика	10
Отображение страницы блокировки	11
Частота запроса аутентификации	13
Взаимодействие элементов экосистемы SUMMA	14

Особенности обработки списков IP и URL в правилах NGFW

Product: UserGate NGFW

KnowledgeBase: 

В правилах NGFW могут использоваться списки IP, гео IP и списки доменных имен. Эти списки представляют из себя разные сущности и обрабатываются в правилах по-разному.

В общем случае правила обработки выглядят так:

1. условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;
2. условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Особенности реализации доступа к сервисам зон

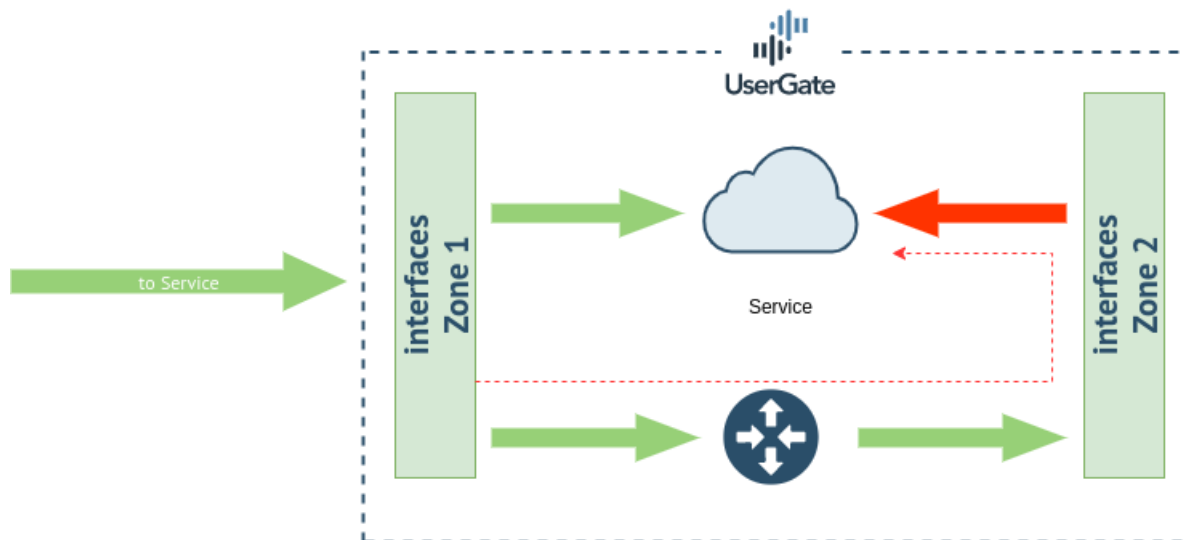
Product: UserGate NGFW

KnowledgeBase: 

В устройствах UserGate для корректной работы сервисов при наличии виртуальных маршрутизаторов (VRF) введены некоторые ограничения на доступ к сервисам зон.

Примечание Данные ограничения введены для следующих сервисов: SNMP, Кластер, VRRP, DNS, Агент авторизации, RIP, SNMP-прокси, SSH-прокси, NTP сервис.

Пакет будет пропущен к сервису, если он поступил на интерфейс зоны, в которой разрешена работа данного сервиса. Если затем, в результате внутренней маршрутизации, пакет был перенаправлен на интерфейс другой зоны (например, запрос из одной зоны осуществляется по IP-адресу, находящемуся в другой зоне), то такой пакет будет заблокирован даже несмотря на наличие доступа к сервису обеих зон.



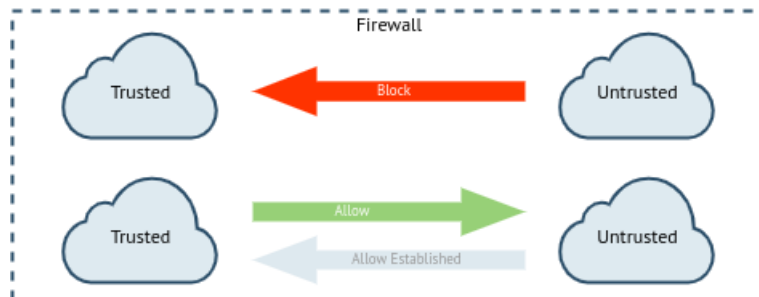
Особенности работы межсетевого экрана UserGate

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

В данном разделе рассмотрены некоторые особенности обработки трафика межсетевым экраном UserGate NGFW.

Запрещающие правила UG NGFW в целях безопасности имеют некоторые особенности в обработке пакетов — это, в свою очередь, может приводить к ситуации с не очевидной блокировкой пакетов. В качестве примера рассмотрим следующую ситуацию:

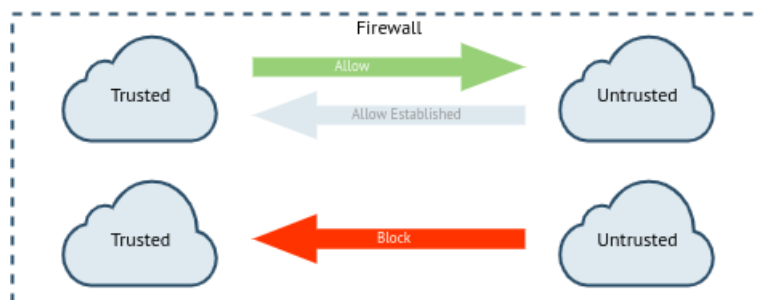


Примечание Параметр `fw_established` выключен

В этом примере доступ из сети Trusted не будет работать, поскольку, несмотря на то, что при создании второго правила, автоматически будет добавлено разрешающее правило для входящих пакетов уже установленного соединения, эти пакеты будут заблокированы, поскольку запрещающие правила межсетевого экрана блокируют любой пакет попадающий под их условия, в т.ч. и пакеты уже установленных сессий. Соответственно, ответные пакеты для разрешенных правилами ниже сессий будут также заблокированы, поскольку сначала попадут под действие запрещающего правила.

Таким образом, для корректной работы межсетевого экрана:

Первый вариант: необходимо размещать запрещающие правила ниже разрешающих, чтобы сначала отработали разрешающие правила, в т.ч. по пакетам уже установленных соединений, а уже потом вступали в работу запрещающие правила.



В данном случае, все будет работать правильно, поскольку сначала отработают разрешающие правила, и лишь потом будет заблокирован трафик, который не попадет под действие этих правил

Второй вариант: начиная с 6 версии возможно через cli установить значение `fw_established` в `true` - это создаст общее разрешающее правило для пакетов уже установленной сессии, выше всех правил FW.

Примечание Этот вариант является менее предпочтительным, поскольку это может привести к проблемам в журналировании всех пакетов и некорректной работе блокировки по приложениям.

Примечание Вариант с `fw_established` обычно имеет смысл при большом количестве правил, и только в том случае если вышеуказанные проблемы являются для вас несущественными.

Формирование списков URL

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

В списки URL добавляются записи, соответствующие стандарту, описанному в [RFC 1738](#).

Примечание Регистр букв имеет значение в URL при указании пути, в названии домена - нет.

1. Для доменов: регистр букв не имеет значение (определён в [RFC 1035](#)), т.е. при указании test.ru, также будут заблокированы домены Test.ru, TEST.ru и т.п.

2. Для URL: регистр букв не имеет значения при указании имени хоста, но учитывается в URI (адресе ресурса на веб-сервере; определено [RFC 3986](#)).

Примечание Если запись, начинается с http://, https://, ftp:// или содержит один или более символов косой черты (/), то такая запись считается URL.

URL применяются только для HTTP(S)-фильтрации. Имя домена применяется и для DNS-фильтрации, и для HTTP(S)-фильтрации.

Например, настроено правило контентной фильтрации, блокирующее список URL, содержащий запись http://test.ru/example. В этом случае:

- test.ru - регистр букв не имеет значения, т.е. http://Test.ru/example (и подобные) будут заблокированы;
- example - регистр букв имеет значение, т.е. http://test.ru/Example (и подобные) заблокированы не будут.

Блокировка расширений возможна только через списки URL. Например, для блокировки файла с расширением .exe необходимо добавить следующие записи (необходимо учесть всевозможные комбинации): /*exe\$, /*EXE\$, /*Exe\$, /*eXe\$, /*exE\$, /*EXe\$, /*ExE\$, /*eXE\$.

Version: 6.x, 7.x

Technology: Identification and Authentication

Product: UserGate NGFW

В данном разделе в общем будут рассмотрены алгоритмы аутентификации пользователей на UserGate и условия применения политик.

Аутентификация локальных пользователей

Если на UserGate настроена аутентификация локальных пользователей, то возможны следующие случаи:

1. **Аутентификация по явно указанному IP-адресу.** IP-адрес указывается во вкладке **Статические IP/MAC/VLAN** свойств пользователя в разделе **Пользователи и устройства → Пользователи**. В этом случае пользователь считается аутентифицированным на UserGate.
2. **Аутентификация по логину/паролю.** При получении от неизвестного клиента HTTP-запроса UserGate перенаправляет его на страницу аутентификации captive-портала.

Политики применяются к локальным пользователям автоматически.

Аутентификация на серверах RADIUS, TACACS+

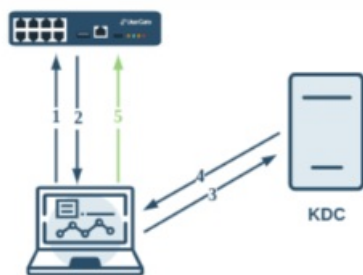
При получении от неизвестного клиента HTTP-запроса UserGate перенаправляет его на страницу аутентификации captive-портала. Пользователь вводит логин/пароль, а UserGate отправляет данные на сервер (RADIUS или TACACS+) для проверки их корректности.

Аутентификация через LDAP-коннектор

1. **LDAP-коннектор с загруженным keytab.** При получении от неизвестного клиента HTTP-запроса UserGate перенаправляет его на страницу аутентификации captive-портала. Пользователь вводит логин/пароль, UserGate получает Kerberos-тикет для данного пользователя и расшифровывает его с помощью загруженного keytab-файла.
2. **LDAP-коннектор без загруженного keytab.** При получении от неизвестного клиента HTTP-запроса UserGate перенаправляет его на страницу аутентификации captive-портала. Пользователь вводит логин/пароль, UserGate посылает LDAP-запрос на сервер аутентификации для проверки корректности введённых логина и пароля.

Примечание Пользователи должны состоять в группе Domain Users (идентификатор группы: 513).

Аутентификация Kerberos



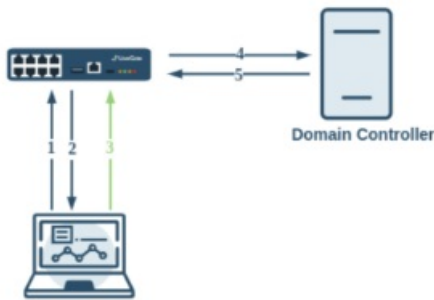
При получении от неизвестного клиента HTTP-запроса UserGate отправляет клиенту сообщение HTTP 401 или HTTP 407 с требованием аутентификации.

При явно указанном прокси, получая от клиента HTTP-запрос, UserGate отвечает сообщением HTTP 407 (Proxy Authentication Required).

При прозрачном проксировании UserGate перехватывает HTTP-запрос от клиента и отправляет сообщение HTTP 302, указывая в Location auth домен captive-портала. При получении от клиента GET на auth домен captive-портала UserGate отвечает сообщением HTTP 401 (Unauthorized).

Получив ответ от UserGate, пользователь обращается в центр распределения ключей своей сети (KDC) с целью получения для своих учётных данных Kerberos-тикета. Затем полученный Kerberos-тикет пользователь отправляет на сервер UserGate, который расшифровывает его с помощью загруженного keytab. UserGate записывает в базу данных имя и IP-адрес пользователя и просматривает группы LDAP, указанные в тикете. Если указанные группы LDAP используются в политиках UserGate, то UserGate добавит эти группы к информации о пользователе, если нет, то информация об этих группах не будет записана в базу данных.

Аутентификация NTLM



При получении от неизвестного клиента HTTP-запроса UserGate отправляет клиенту сообщение HTTP 401 или HTTP 407 с требованием аутентификации.

При явно указанном прокси, получая от клиента HTTP-запрос, UserGate отвечает сообщением HTTP 407 (Proxy Authentication Required).

При прозрачном проксировании UserGate перехватывает HTTP-запрос от клиента и отправляет сообщение HTTP 302, указывая в Location auth домен captive-портала. При получении от клиента GET на auth домен captive-портала UserGate отвечает сообщением HTTP 401 (Unauthorized).

Получив ответ от UserGate, пользователь отправляет данные для аутентификации на сервер UserGate. UserGate пересылает их на контроллер домена. В случае корректности логина/пароля считаем пользователя аутентифицированным.

Применение политик к пользователям, проходящим аутентификацию через LDAP-коннектор и по NTLM

Для применения политик (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) к пользователям, аутентифицирующимся через LDAP-коннектор или NTLM, необходимо:

1. Выполнить logout на UserGate.

Для выполнения logout пользователю необходимо перейти на страницу Logout captive-портала и нажать **Выйти/Logout**.

Сбросить аутентификацию всех пользователей можно в разделе **Пользователи и устройства → Серверы аутентификации** (кнопка **Сбросить аутентификацию всех пользователей**) веб-интерфейса UserGate. Также можно сбросить сессии отдельных пользователей с помощью интерфейса командной строки (CLI); для выполнения команды необходимо знать IP-адрес пользователя (<IP-address>):

- UserGate NGFW 6.x.x:
`UTM> usersession terminate -ipv4 <IP-address>`
- UserGate NGFW 7.0.x:
`Admin@UGOS# execute terminate usersession <IP-address>`
- UserGate NGFW 7.1.x:
`Admin@nodename# execute termination user-sessions ip <IP-address>`

2. Очистить кэш LDAP-записей на UserGate.

Очистка доступна через интерфейс командной строки (CLI), используйте команду:

- UserGate NGFW 6.x.x:
`UTM> cache ldap-clear`
- UserGate NGFW 7.x.x:
`Admin@UGOS# execute cache ldap-clear`

3. Пройти аутентификацию на UserGate.

Применение политик к пользователям, проходящим аутентификацию по Kerberos

Для применения политик (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) к пользователям, аутентифицирующимся по Kerberos, необходимо:

1. Выполнить logout на UserGate.

Для выполнения logout пользователю необходимо перейти на страницу Logout captive-портала и нажать **Выйти/Logout**.

Сбросить аутентификацию всех пользователей можно в разделе **Пользователи и устройства → Серверы аутентификации** (кнопка **Сбросить аутентификацию всех пользователей**) веб-интерфейса UserGate. Также можно сбросить сессии отдельных пользователей с помощью интерфейса командной строки (CLI); для выполнения команды необходимо знать IP-адрес пользователя (<IP-address>):

- UserGate NGFW 6.x.x:
`UTM> usersession terminate -ipv4 <IP-address>`

- UserGate NGFW 7.0.x:

Admin@UGOS# execute terminate usersession <IP-address>

- UserGate NGFW 7.1.x:

Admin@nodename# execute termination user-sessions ip <IP-address>

2. Получить новый Kerberos-тикет с обновлённым списком LDAP-групп. Для обновления тикета необходимо, например, повторно аутентифицироваться на клиентском компьютере.

3. Очистить кэш LDAP-записей на UserGate.

Очистка доступна через интерфейс командной строки (CLI), используйте команду:

- UserGate NGFW 6.x.x:

UTM> cache ldap-clear

- UserGate NGFW 7.x.x:

Admin@UGOS# execute cache ldap-clear

4. Пройти аутентификацию на UserGate.

Алгоритм настройки защиты почтового трафика

Version: 6.x

Product: UserGate NGFW

В данной статье приведён общий порядок действий для настройки защиты почтового трафика.

Примечание Необходимо придерживаться данного порядка выполнения действий.

1. Проверить наличие лицензии на модули **Mail security** и **KAS**.

Примечание Наличие лицензии KAS обязательно; без неё защита почтового трафика работать не будет. [Лицензия KAS входит в подписку модуля Mail Security](#).

Для проверки наличия лицензии KAS обратитесь в службу технической поддержки UserGate.

2. Включить правило DNAT, используемое для публикации почтового сервера по сервисам SMTP, SMTPS и т.п..

Примечание В случае повторного включения правила DNAT, также необходимо выключить и включить правило защиты почтового трафика, т.к. после выключения правила DNAT модуль защиты почтового трафика не будет видеть его.

3. Включить правило защиты почтового трафика, которое настроено с такими же условиями, что и правило DNAT (с указанием в правиле защиты почтового трафика внутренних адресов почтовых серверов в качестве адресов назначения (панель **Адрес назначения**, вкладка **Назначение**).
4. Настройте правило инспектирования SSL, указав зоны источника, сервисы SMTPS, POP3S. Правило следует расположить выше правил, пропускающих трафик без инспектирования, и убедиться, что почтовый трафик попадает под действие созданного правила.

Отображение страницы блокировки

Version: 6.x, 7.x

Product: UserGate NGFW

Рассмотрим случаи, когда страница блокировки будет или не будет отображена.

UserGate работает в режиме **Transparent Proxy Mode**:

Протокол прикладного уровня	Политика межсетевого экрана	Политика инспектирования SSL	Политика фильтрации контента	Ответ браузера
HTTP	разрешающая	включена или нет	разрешающая	Нет.
	запрещающая	включена или нет	разрешающая	Страница блокировки UserGate не отображается. Ответ браузера: Failed to connect. Connection Timed out.
	разрешающая	включена или нет	запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate не отображается. Ответ браузера: The connection was reset.
HTTP to non-resolve domain	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate не отображается. Ответ браузера: Could not resolve host.
HTTPS	разрешающая	нет	разрешающая	Нет.
	запрещающая	включена или нет	разрешающая	Страница блокировки UserGate не отображается. Ответ браузера: Failed to connect. Connection Timed out.
	разрешающая	нет	запрещающая	Нет.
	разрешающая	включена	запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate не отображается. Ответ браузера: The connection was reset.
	разрешающая	включена	запрещающая	Нет, если не прошла расшифровка SSL.
HTTPS to non-resolve domain	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate не отображается. Ответ браузера: Could not resolve host.

UserGate работает в режиме **Explicit Proxy Mode**:

Протокол прикладного уровня	Политика межсетевого экрана	Политика инспектирования SSL	Политика фильтрации контента	Ответ браузера
HTTP	разрешающая	включена или нет	разрешающая	Нет.
	запрещающая	включена или нет	разрешающая	Страница auth.captive UserGate. Ответ браузера: Connection error: error timeout.
	разрешающая	включена или нет	запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate.
HTTP to non-resolve domain	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	разрешающая	Страница auth.captive UserGate. Ответ браузера: Connection error: the hostname or domain name could not be found.
HTTPS	разрешающая	нет	разрешающая	Нет.
	запрещающая	включена или нет	разрешающая	Страница auth.captive UserGate. Ответ браузера: Connection error: error timeout.
	разрешающая	нет	запрещающая	Нет.
	разрешающая	включена	запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate.
	разрешающая	включена	запрещающая	Нет, если не прошла расшифровка SSL.
HTTPS to non-resolve domain	разрешающая	включена или нет	общая запрещающая	Страница блокировки UserGate.
	разрешающая	включена или нет	разрешающая	Страница auth.captive UserGate. Ответ браузера: Connection error: the hostname or domain name could not be found.

Частота запроса аутентификации

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

UserGate не производит аутентификацию пользователей при каждом HTTP-запросе, т.к. это привело бы к неоправданному увеличению объёма сетевого трафика, задержкам при загрузке HTTP-ресурсов и, в случаях использования внешних источников учётных записей пользователей, повышению нагрузки на серверы аутентификации.

В UserGate реализована периодическая аутентификация пользователей. В случае успешной аутентификации UserGate сопоставляет идентификатор пользователя и его IP-адрес и записывает в базу данных информацию о пользователе. Пока пара идентификатор/IP-адрес хранится в базе пользователь считается авторизованным (Known) и UserGate не требует его повторной авторизации. Срок хранения данных об авторизации пользователя определяется двумя параметрами профиля авторизации UserGate:

1. **Время жизни авторизованного пользователя** определяет период, по истечении которого информация о пользователе будет удалена из базы данных, пользователь будет Unknown, пока повторно не авторизуется на captive-портале UserGate.

Значение по умолчанию составляет 86400 секунд, т.е. 24 часа. Данное значение оптимально, если рабочие места в организации являются персональными, в противном случае рекомендуется использовать профиль авторизации с меньшим временем жизни авторизованного пользователя, например, 900 секунд (15 минут).

2. **Время бездействия до отключения** определяет промежуток времени, по истечении которого UserGate сбросит авторизацию пользователя, если от него не было получено ни одного сетевого пакета (информация о пользователе будет удалена из базы). Авторизация будет сброшена, даже если время жизни авторизованного пользователя еще не истекло.

Значение по умолчанию составляет 900 секунд, т.е. 15 минут.

Примечание Современные операционные системы и ПО постоянно ведут некоторую фоновую сетевую активность, поэтому данный таймер не будет срабатывать, если рабочее место пользователя не выключено, а, например, заблокировано.

Version: 7.1.x

Product: NGFW, UGMC, LogAn, SIEM, UGC

Все элементы экосистемы UserGate SUMMA взаимодействуют друг с другом по защищённым каналам.

MC-NGFW, MC-LogAn/SIEM

UserGate MC для всех коммуникаций с элементами экосистемы (NGFW, LogAn, SIEM) использует зашифрованный SSH-туннель. Туннель инициируется со стороны элемента экосистемы. Внутри туннеля открывается несколько портов на каждой из сторон, чтобы MC и устройство могли между собой общаться.

SSH-соединение происходит только через ключи. Обмен ключами между устройством и MC происходит при регистрации устройства в MC.

В настройках контроля доступа зон, через которые устанавливаются соединения с другими элементами экосистемы, настраивается доступ для соответствующих сервисов (на MC — порты TCP 9712 и 2022).

Для работы туннеля устройства должны передать в MC свой открытый ключ, он отправляется через порт 9712 на стороне MC в виде AES-зашифрованного сообщения. Ключ для шифрования вычисляется из специальной строки, которую администратор должен получить на MC и ввести в консоли устройства при настройке работы с MC. MC принимает сообщение, расшифровывает, извлекает открытый SSH-ключ, добавляет его в свои настройки, после этого сохраняет в базе данных объект *Managed Device*, чтобы его нельзя было инициализировать ещё раз.

SSH-сервер на стороне MC слушает внешний порт 2022, он используется для коммуникации с уже подключёнными устройствами экосистемы.

Когда NGFW открывает туннель, в нём создаются несколько слушающих портов на каждой из сторон:

- NGFW, порт 127.0.0.1:9999 туннелируется в XML-RPC сервис приёма телеметрии, keep alive ping, итд. (порт 4042 на MC).
- MC, порт 127.0.0.1:\$RAND_1 туннелируется в XML-RPC сервис NGFW (порт 4040 на стороне NGFW).
- MC, порт 127.0.0.1:\$RAND_2 туннелируется в HTTP-порт веб-консоли NGFW (порт 8001 на стороне NGFW).

\$RAND_1 и \$RAND_2 генерируются случайным образом из свободных портов в момент создания туннеля и сохраняются в конфигурации MC.

- NGFW периодически отправляет XML-RPC запросы с телеметрией/статусом на локальный порт 9999, а они через туннель попадают в MC.
- Также NGFW периодически опрашивает другие сервисы на порту 9999, чтобы получить от MC обновления конфигурации, если они есть.

Похожим образом происходит установление туннеля между MC и устройствами LogAn/SIEM. При открытии туннеля со стороны LogAn/SIEM, в нём создаются несколько слушающих портов на каждой из сторон:

- LogAn/SIEM, порт 127.0.0.1:9999 туннелируется в XML-RPC сервис приёма телеметрии, keep alive ping, итд. (порт 4042 на MC).
- MC, порт 127.0.0.1:\$RAND_1 туннелируется в XML-RPC сервис LogAn/SIEM (порт 4041 на стороне LogAn/SIEM).
- MC, порт 127.0.0.1:\$RAND_2 туннелируется в HTTP-порт веб-консоли LogAn/SIEM (порт 8010 на стороне LogAn/SIEM).
- MC, порт 127.0.0.1:\$RAND_3 туннелируется в SSL-порт приёма статистики от устройств с установленным ПО UserGate Client на стороне LogAn/SIEM (порт 22711 или порт 22699 — для устройств с ПО ниже версии 7).

\$RAND_1, \$RAND_2, \$RAND_3 генерируются случайным образом из свободных портов в момент создания туннеля и сохраняются в конфигурации MC.

LogAn/SIEM-NGFW

На NGFW в настройках контроля доступа зоны, через которую устанавливается соединение с LogAn/SIEM, необходимо открыть доступ для соответствующих сервисов интеграции (порты TCP 9713 и 2023).

LogAn/SIEM при интеграции сначала сам подключается к NGFW с помощью параметров, настроенных в сенсоре UserGate, и передаёт в NGFW настройки для подключения.

Для работы туннеля LogAn/SIEM должен сначала передать в NGFW свой открытый ключ, он отправляется через порт 9713 на стороне NGFW в виде AES-зашифрованного сообщения. Ключ для шифрования вычисляется из специальной строки (токена), которую администратор должен получить на NGFW при настройке подключения к LogAn/SIEM. Токен вводится на LogAn/SIEM при настройке сенсора UserGate для интеграции с NGFW. SSH-сервер на стороне NGFW слушает внешний порт 2023, он используется для установления SSH-туннеля со стороны LogAn/SIEM для передачи настроек подключения.

Далее NGFW собирает свои данные в локальном кэше и периодически по таймеру передаёт их в зашифрованном виде в модуль statistics в LogAn/SIEM, устанавливая соединение по порту TCP 22711 (или TCP 22699 — для устройств с ПО ниже версии 7), которые должны быть разрешены в контроле доступа соответствующей зоны на устройстве LogAn/SIEM.

UGC-MC, UGC-NGFW

Конечные устройства с установленным ПО UserGate Client (UGC) взаимодействуют с MC и NGFW по протоколу HTTPS через порт 4045.

На NGFW доступ к порту TCP 4045 должен быть разрешён в настройках доступа зоны, через которую происходит подключение конечных устройств (порт не должен быть доступен извне, по умолчанию открывается в зоне Trusted и в зонах VPN). Сертификат и профиль SSL для соединения с конечными устройствами устанавливается в общих настройках NGFW. Конечное устройство регистрируется в NGFW и периодически отправляет данные телеметрии.

В процессе регистрации на MC конечные устройства обмениваются с MC ключами шифрования, обращаясь к MC по порту 9712. Конечные устройства отправляют на MC данные телеметрии на порт 4045 с взаимной проверкой сертификатов. В ответ MC отправляет на конечное устройство параметры настроек и мониторинга конечного устройства.

Также на MC для каждого подключённого и активного сервера LogAn/SIEM открывается порт из диапазона 22000:22711, предназначенный для приёма статистики на соответствующий узел LogAn/SIEM. Порт назначается при интеграции устройства LogAn/SIEM в MC и сохраняется в конфигурации MC в специальной таблице. Подключение конечных устройств с установленным UGC к этому порту прозрачно пробрасывается на MC к подключённому устройству LogAn/SIEM через установленный SSH-туннель; в случае его недоступности, соединение не устанавливается. Конечные устройства периодически отправляют на этот порт данные, зашифрованные при помощи закрытого ключа и сертификата устройства.

