

Table of Contents

Table of Contents	1
Приложения	2
Установка сертификата локального удостоверяющего центра	3
Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0	9
Требования к сетевому окружению	13
Опции DHCP	16
Примеры генерации сертификатов для IKEv2 VPN	19

Установка сертификата локального удостоверяющего центра

Documentation: 

Product: NGFW

Version: 7.x

Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

Откройте папку, куда вы скачали рет-сертификат, переименуйте его в user.der и дважды нажмите на него:

Откроется информация о сертификате. Нажмите **Установить сертификат**:

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

Выберите хранилище сертификата и нажмите **Обзор**:

Выберите **Доверенные корневые центры сертификации** и нажмите **ОК**:

Нажмите **Готово**:

Когда появится предупреждение системы безопасности, нажмите **Да**:

Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в ОС MacOSX

Перейдите в папку, куда вы скачали рет-сертификат и дважды нажмите на него:

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

Введите свой пароль для подтверждения данной операции:

Сертификат установлен.

Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется одинаково для всех операционных систем. Рассмотрим установку на примере ОС Windows.

Откройте настройки браузера Firefox (**Инструменты → Настройки**):

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите **Просмотр сертификатов**:

Нажмите **Импортировать** и укажите путь к скачанному рет-сертификату:

Установите флажок **Доверять при идентификации веб-сайтов** и нажмите **ОК**:

Установка сертификата завершена.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

Documentation: ☒
Product: NGFW
Version: 7.x

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Криптомайнеры
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечения	Поздравительные открытки
	Развлечения
	Мода и красота
	Отдых и оздоровление
	Рестораны и еда
	Спорт
	Путешествия

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Здоровье и медицина	Здоровье и медицина
	Половое воспитание
Злоупотребление свободой СМИ - информация с ограниченным доступом. Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций	Оружие
Злоупотребление свободой СМИ - информация, содержащая скрытые вставки и иные технические способы воздействия на под-104№ п/п Тематическая категория Содержание скрытое воздействие сознание людей и (или) оказывающая вредное влияние на их здоровье	Сайты сомнительного содержания
Злоупотребление свободой СМИ - наркотические средства, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Ненависть и нетерпимость
	Насилие
Злоупотребление свободой СМИ -экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпимость
	Насилие
Знакомства	Знакомства
Информация с ограниченным доступом. Информация, составляющая государственную или иную охраняемую законом тайну	Политика
	Правительство
Информация, пропагандирующая порнографию	Порнография и насилие
Компьютерные игры	Игры
Корпоративные сайты	Бизнес
	Финансы
	Общие
	Недвижимость
Корпоративные сайты, интернет-представительства негосударственных учреждений	Некоммерческие и неправительственные организации
Личная и немодерируемая информация. Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги	Персональные сайты
	Частные IP-адреса
	Социальные сети
	Потоковое мультимедиа и загрузки
	Веб-почта

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Модерируемые доски объявлений (ресурсы данной категории, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты	Социальные сети
	Чаты
Наркотические средства. Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Наркотики
Нелегальная помощь школьникам и студентам. Банки готовых рефератов, эссе, дипломных работ и пр.	Школьные мошенничества
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной продукции и табачных изделий	Алкоголь и табак
Неприличный и грубый юмор. Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека	Сайты сомнительного содержания
Нижнее белье, купальники	Нудизм
Обеспечение анонимности пользователя, обход контентных фильтров. Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам	Анонимайзеры
	Переводчики
Образовательные ресурсы	Образование
Онлайн-казино и тотализаторы	Азартные игры
Отправка SMS с использованием интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS-сообщений	Реклама и всплывающие окна
Платные сайты	Паркованные домены
Поиск работы, резюме, вакансии	Поиск работы
Преступления - клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию)	Преступная деятельность
Преступления-клевета, экстремизм	Преступная деятельность
Программное обеспечение	Компьютеры и технологии
	Нелегальное ПО
	Информационная безопасность
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение	Ненависть и нетерпимость
Религии и атеизм	Религиозные культы
	Религия

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Система поиска изображений	Обмен картинками
	Поисковые системы и порталы
СМИ	Форумы и новостные ленты
	Новости
Табак, реклама табака, пропаганда потребления табака. Сайты, пропагандирующие потребление табака; реклама табака и изделий из него	Алкоголь и табак
Торговля и реклама	Реклама и всплывающие окна
	Покупки
Убийства, насилие	Жестокое обращение с детьми
	Насилие
Чаты	Чаты
	Сервисы мгновенных сообщений
Экстремистские материалы или экстремистская деятельность (экстремизм)	Ненависть и нетерпимость

Требования к сетевому окружению

Documentation: 

Product: NGFW

Version: 7.x

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate NGFW)	Доступ к веб-интерфейсу управления устройством
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS. Доступен в версии 7.3.3 и выше
Удаленный помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удаленный доступ к серверам технической поддержки. Доступ к серверам: 93.91.171.46; 178.154.221.222; - ra.entensys.com
NTP	UDP	123	Исходящий (до сервера точного времени). Входящий (от клиентов до UserGate NGFW, если он используется в качестве сервера точного времени)	Синхронизация времени
DNS	TCP/UDP	53	Входящий (от клиентов к UserGate NGFW, если он выступает в качестве DNS-сервера)	Сервис получения информации (IP-адрес) о доменах
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения
		9000-9100	Входящий (прием конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
		9712	Исходящий (от UserGate NGFW до UserGate MC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center

Связь с UserGate Management Center	TCP Протокол	Порт	Исходящий/Входящий	Функция
		2022	Исходящий (от UserGate NGFW до UserGate MC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей
Связь с UserGate Log Analyzer	TCP	9713	Входящий (от UserGate Log Analyzer к UserGate NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer
		2023	Входящий (от UserGate Log Analyzer к UserGate NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей
	TCP	22699 (передача данных на UserGate Log Analyzer 6.1.x), 22711 (передача данных на UserGate Log Analyzer 7.x.x, с использованием SSL)	Исходящий (от UserGate NGFW к UserGate Log Analyzer)	Передача журналов и телеметрии на сервер UserGate Log Analyzer.
Подключение конечных устройств с установленным ПО UserGate Client (доступно начиная с версии 7.1.0)	TCP	4045	Входящий (от конечного устройства на UserGate NGFW)	Подключение конечных устройств и прием телеметрии для проверки комплаенса
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 — для LDAP и 636 — для LDAP over SSL)
Captive-портал и страница блокировки	TCP	80, 443, 8002, 8043	Входящий (от браузера клиента на UserGate NGFW)	Отображение страницы авторизации Captive-портала и страницы блокировки
Kerberos	TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей по протоколу Kerberos
NTLM	TCP	445	Исходящий (на сервер аутентификации NTLM)	Аутентификация пользователей по протоколу NTLM
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+
Агент терминального сервиса	UDP	1812, 1813	Входящий (от агента на UserGate NGFW)	Доступ к серверу UserGate, необходимый для работы терминального агента
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UserGate NGFW)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows
Прокси-агент	UDP	8090	Входящий (от агента на UserGate NGFW)	Доступ к серверу UserGate, необходимый для работы прокси-агента, предоставляющего доступ в Интернет пользователям, работающим на ОС Windows
SNMP	UDP	161	Входящий (до UserGate NGFW)	Доступ к серверу UserGate по протоколу SNMP

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту
ICAP	TCP	1344	Исходящий (до серверов ICAP)	Сервис работы с серверами ICAP
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate NGFW на сервер DHCP). Входящий (UserGate NGFW выступает в качестве DHCP-сервера)	Сервис службы DHCP
BGP	TCP	179	Исходящий (передача информации соседним BGP-маршрутизаторам). Входящий (получение информации от соседних BGP-маршрутизаторов)	Сервис динамической маршрутизации BGP
OSPF	89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам). Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF
RIP	UDP	520	Исходящий (распространение соседним маршрутизаторам RIP-маршрутов). Входящий (получение от соседних маршрутизаторов RIP-маршрутов)	Сервис динамической маршрутизации RIP
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера syslog)	Экспорт журналов на сервер syslog

Опции DHCP

Documentation: ☒

Product: NGFW

Version: 7.x

Формат значений опций соответствует [RFC 2132](#).

Наименование	Описание
1	Маска подсети, из которой был получен адрес.
2	Разница во времени в подсети клиента относительно UTC (указывается в секундах).
3	Список IP-адресов доступных шлюзов.
6	Список DNS-серверов.
7	Список лог-серверов (MIT-LCS UDP).
9	Список LPR-серверов (RFC 1179).
13	Размер загрузочного образа для клиентов.
15	Имя домена.
16	Swap-сервер.
17	Путь корневого каталога для клиента.
18	Путь расширений BOOTP.
19	Применение пересылки IP-датаграмм.
20	Использование маршрутизации удаленного источника.
21	Политика фильтрации IP-адресов.
22	Максимальный размер датаграммы.
23	Значение TTL для IP по умолчанию.
26	Значение MTU для данного интерфейса.
27	Признак, что все подсети используют текущую конфигурацию MTU.
31	Определение использования сообщений ICMP для обнаружения маршрутизаторов.
32	Адрес, который используется для обращения к маршрутизатору.
33	Статичный список маршрутизации; состоит из пар «адрес назначения» — «адрес роутера».
34	Использование концевиков (trailers) при запросах ARP.
35	Тайм-аут кэш-памяти ARP.
36	Необходимость использования инкапсуляции данных Ethernet.

Наименование	Описание
37	Значение TTL для TCP-пакетов.
38	Интервал отправки контрольных пакетов TCP (TCP keep-alive).
40	Домен NIS.
41	Список серверов NIS.
42	Список серверов времени NTP.
44	Список IP-адресов серверов NetBIOS.
45	Список IP-адресов серверов рассылки датаграмм NetBIOS.
46	Тип узла NetBIOS.
47	Область NetBIOS.
48	IP-адреса серверов шрифтов X Windows (X Window System Font).
49	Диспетчер дисплея X Windows.
58	Время T1 — интервал времени, в течение которого клиент должен отправить запрос на обновление IP-адреса.
59	Время T2 — интервал времени (в секундах), в течение которого клиент должен отправить запрос на повторное связывание.
60	Опция используется клиентом DHCP для указания поставщика.
64	Имя домена NIS+.
65	Список серверов NIS+.
66	Имя сервера TFTP.
67	Название загрузочного файла.
68	Адреса домашних агентов (Mobile IP Home Agent).
69	Список серверов SMTP.
70	Список серверов POP3.
71	Список серверов NNTP.
74	Список серверов IRC.
77	Класс пользователя.
80	Опция позволяет получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
93	Архитектура системы клиента DHCP.

Наименование	Описание
94	Идентификатор сетевого интерфейса клиента DHCP.
97	Идентификатор клиента на основе UUID/GUID.
119	Список поиска DNS.
120	Список серверов SIP.
121	Список бесклассовых статических маршрутов.
125	Указание информации о поставщике.
255	Конец списка опций; обязательно должен присутствовать последним.

Documentation: 

Product: NGFW

Version: 7.x

Technology: Identification and Authentication

Генерация сертификатов на Linux с использованием OpenSSL

Пример генерации сертификатов в ОС Linux с помощью библиотеки OpenSSL на основе самоподписанного корневого сертификата.

Действия на стороне VPN-сервера

1. Создать самоподписанный корневой сертификат rootCA.

```
$ openssl genrsa -aes256 -passout pass:1234 -out rootCA.key 4096
```

```
$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem -subj "/C=RU/ST=Sib/L=Nsk/O=ep.local/OU=ep.local/CN=QA"
```

где rootCA.pem — это корневой сертификат.

Проверить, что сертификат корневой (в выводе должна быть строка: CA:TRUE):

```
$ openssl x509 -in rootCA.pem -text
```

2. На основе корневого сертификата создать сертификат для VPN-сервера.

- Требования — **key usage: server auth**;
- Указать subjectAltName соответствующее DNS-имени VPN-сервера.

```
$ openssl genrsa -aes256 -passout pass:1234 -out server.pass.key 4096
```

```
$ openssl rsa -passin pass:1234 -in server.pass.key -out server-key.pem
```

где server-key.pem — это приватный ключ.

Для генерации запроса на выпуск сертификата создать файл openssl-server.cnf с данными для запроса сертификата. **Пример** заполненного данными файла:

```
[ req ]
prompt = no
days = 365
req_extensions = v3_req
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
C = Ru
ST = Sib
L = Nsk
O = ep.local
OU = ep.local
CN = vpnserver.ep.local #dns name vpn-сервера
emailAddress = mail1@ep.local

[ v3_req ]
keyUsage = critical, digitalSignature
extendedKeyUsage = serverAuth
subjectAltName = @sans

[ sans ]
DNS.0 = vpnserver.ep.local # dns name vpn-сервера
```

Создать запрос на выпуск сертификата с учетом данных из созданного выше файла openssl-server.cnf. На этом этапе прописывается секция Subject сертификата:

```
$ openssl req -new -key server-key.pem -out server.csr -config openssl-server.cnf
```

Подписать запрос корневым сертификатом. На этом этапе прописывается секция X509v3 extensions сертификата:

```
$ openssl x509 -CAcreateserial -req -extfile openssl-server.cnf -extensions v3_req -days 365 -in server.csr -CA rootCA.pem -CAkey rootCA.key -out server-cert.pem
```

где server-cert.pem — это сертификат VPN-сервера.

3. Импортировать сертификат VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера (server-cert.pem) и приватного ключа (server-key.pem).

4. Импортировать корневой сертификат в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированный файл самоподписанного корневого сертификата (rootCA.pem) без указания приватного ключа.

5. Создать профиль клиентских сертификатов в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить

импортированный на предыдущем шаге корневой сертификат и выбрать поле для авторизации **Common-name** или **Subject alt name** для получения имени пользователя.

6. На этапе настройки VPN будет необходимо создать профиль безопасности VPN. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля безопасности VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера необходимо перейти в раздел **VPN → Серверные профили безопасности** и нажать кнопку **Добавить**. В открывшемся окне указать необходимые параметры профиля безопасности (подробнее смотрите в разделе [Настройка VPN](#)). При использовании протокола IKEv2 для организации VPN необходимо указать импортированный в пункте 3 сертификат VPN-сервера и профиль пользовательского сертификата, созданного в пункте 5, если в качестве режима аутентификации будет указан PKI.

Действия на стороне VPN-клиента

1. Создать сертификат для VPN-клиента.

Для генерации запроса на выпуск сертификата для VPN-клиента создать файл `openssl-client.cnf` с данными для запроса сертификата. **Пример** заполненного данными файла.

```
[ req ]
prompt          = no
days           = 365
req_extensions  = v3_req
distinguished_name = req_distinguished_name
```

```
[ req_distinguished_name ]
C          = Ru      #      необязательный параметр
ST         = Sib     #      необязательный параметр
L          = Nsk     #      необязательный параметр
O          = ep.local # имя домена, необязательный параметр
OU         = ep.local # имя домена, необязательный параметр
CN         = user1@ep.local #Обязательный. Идентификатор пользователя, которому выдан сертификат
```

```
[ v3_req ]
keyUsage          = critical, digitalSignature
extendedKeyUsage  = clientAuth
subjectAltName    = email:user1@ep.local # Пользователь, под учетной записью которого будет выполняться подключение к VPN-серверу.
```

Пример файла `openssl-client.cnf` с запросом на выпуск сертификата, когда VPN-пользователь добавлен локально на UG NGFW (без домена).

```
[ req ]
prompt          = no
days           = 365
req_extensions  = v3_req
distinguished_name = req_distinguished_name
```

```
[ req_distinguished_name ]
C          = Ru      #      необязательный параметр
ST         = Sib     #      необязательный параметр
L          = Nsk     #      необязательный параметр
O          = ep.local # имя домена, необязательный параметр
OU         = ep.local # имя домена, необязательный параметр
CN         = user1   # обязательный. Идентификатор пользователя, которому выдан сертификат
```

```
[ v3_req ]
keyUsage          = critical, digitalSignature
extendedKeyUsage  = clientAuth
subjectAltName    = otherName:msUPN;UTF8:user1
```

Где `user1` — логин учетной записи пользователя, созданной в UG NGFW. Подробнее о создании локальных учетных записей — в разделе [«Пользователи и группы»](#).

ПримечаниеДля каждого пользователя необходимо выпускать свой сертификат, изменяя файл `openssl-client.cnf`.

Поле `subjectAltName` используется, если в профиле клиентского сертификата поле для получения имени пользователя будет указано, как **Subject alt name**.

Сгенерировать приватный ключ для VPN-клиента:

```
$ openssl genrsa -aes256 -passout pass:1234 -out client.pass.key 4096
```

```
$ openssl rsa -passin pass:1234 -in client.pass.key -out client-key.pem
```

Создать запрос на выпуск сертификата с учетом данных из созданного выше файла `openssl-client.cnf` и подписать его корневым сертификатом:

```
$ openssl req -new -key client-key.pem -out client.csr -config openssl-client.cnf
```

```
$ openssl x509 -CAcreateserial -req -extfile openssl-client.cnf -extensions v3_req -days 365 -in client.csr -CA rootCA.pem -CAkey rootCA.key -out client-cert.crt
```

3. Для использования в клиентах с ОС Windows в сценарии Remote Access VPN создать файл `client.pfx`, содержащий закрытый ключ и сертификат пользователя. Файл загружается в Windows и используется для подключения к VPN.

```
$ openssl pkcs12 -export -passout pass:1234 -out client.pfx -inkey client-key.pem -in client-cert.crt
```

4. Файл `client.pfx` импортировать в Windows и расположить в разделе **Локальный компьютер**, хранилище — **Личное**.

5. Для использования клиентского сертификата на стороне узла — VPN-клиента в сценарии Site-to-Site VPN с IKEv2 необходимо импортировать созданный сертификат VPN-клиента. Для этого в консоли администратора NGFW, исполняющего роль VPN-клиента перейти в раздел **UserGate**

→ **Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-клиента (client-cert.crt) и приватного ключа (client-key.pem). Далее, на этапе настройки VPN при создании клиентского профиля безопасности VPN необходимо перейти в раздел **VPN → Клиентские профили безопасности** и нажать кнопку **Добавить**. В открывшемся окне указать необходимые параметры профиля безопасности (подробнее — в разделе «[Профили клиентских сертификатов](#)»). При использовании протокола IKEv2 для организации VPN необходимо в поле Сертификат клиента указать импортированный ранее сертификат VPN-клиента.

Генерация сертификатов Центром Сертификации Microsoft Server

Пример генерации сертификатов Центром Сертификации Microsoft Server для сценария Remote Access VPN.

1. Выпустить Центром Сертификации корневой сертификат (rootCA).
2. Выпустить на основе корневого сертификата (rootCA) сертификат VPN-сервера.
 - Указать требования — **key usage: server auth**;
 - Минимальный размер ключа - **4096**;
 - Указать **subjectAltName** соответствующее **DNS-имени VPN-сервера**.
 - Создать шаблон для выдачи пользовательских сертификатов. UPN атрибут пользователя должен совпадать с атрибутами сертификата CN и/или SAN:principal name.

Действия на стороне VPN-сервера

1. Импортировать корневой сертификат (rootCA) в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать**.
2. Импортировать сертификат VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать**.
3. Создать профиль клиентского сертификата в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный ранее корневой сертификат и выбирать поле для авторизации **Common-name** или **Subject alt name** для получения имени пользователя.
4. В разделе **VPN → Серверные профили безопасности** добавить в **Remote access VPN profile**:
 - Сертификат в поле **Сертификат сервера**.
 - Выбрать созданный **Профиль пользовательского сертификата**.
 - Выбрать **Режим аутентификации** — посредством сертификатов **PKI**.

Свойства серверного профиля безопасности

Общие | Фаза 1 | Фаза 2

Название: RA_VPN

Описание:

ИКЕ версия: IKEv2

Режим ИКЕ: Основной

Тип идентификации: отсутствует

Значение идентификации:

Общий ключ: *****

Общий ключ (повтор): *****

Сертификат сервера: rootCA_vpn_CERT

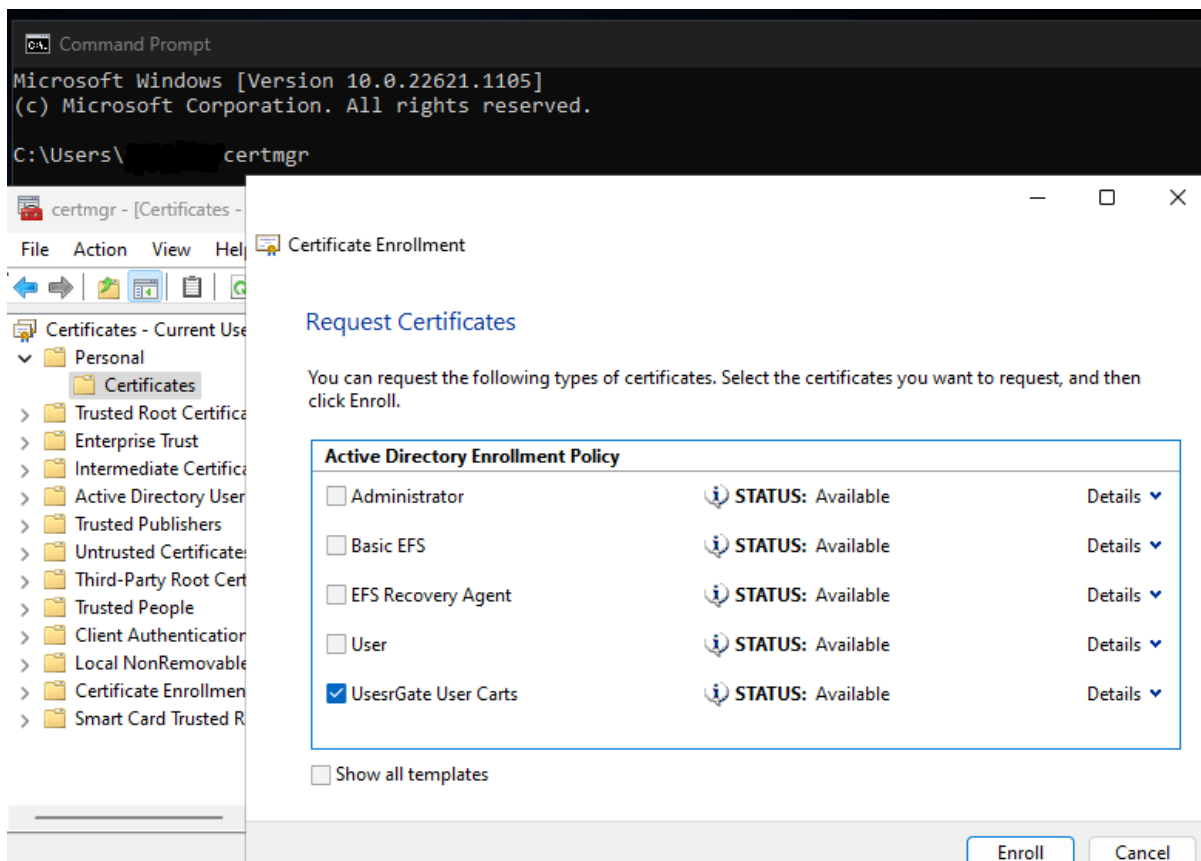
Режим аутентификации: PKI

Профиль сертификата пользователя: client_CERT

Сохранить Отмена

Действия на стороне VPN-клиента

1. Запросить сертификат на клиентской машине согласно созданному ранее шаблону пользовательского сертификата.



2. Полученный сертификат расположить в репозиторий Локальный компьютер, хранилище — Личное.

