

Table of Contents

Table of Contents	1
Пользователи и устройства	2
Пользователи и группы	3
Серверы аутентификации	5
Профили аутентификации	12
Настройка Captive-портала	13
Профили MFA (мультифакторной аутентификации)	17
Пользователи терминальных серверов	19
Прокси-агент для Windows	21
Управление гостевыми пользователями	22
Radius accounting	24
Политики BYOD	25
Агент аутентификации для Windows	26

Пользователи и группы

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

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности NGFW могут быть применены к пользователям или группам пользователей. Возможность применения политик только к тем пользователям, которым это необходимо, позволяет администратору гибко настроить свою сеть в соответствии с потребностями организации.

Идентификация пользователя — это базисная функция NGFW. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. NGFW использует различные механизмы для идентификации пользователей:

- Идентификация по явно указанному IP-адресу
- Идентификация по имени и паролю
- Идентификация пользователей терминальных серверов Microsoft с помощью специального агента терминального сервиса
- Идентификация пользователей с помощью агента авторизации (для Windows-систем)
- Идентификация с помощью протоколов NTLM, Kerberos

Идентификация пользователей по имени и паролю возможна через Captive-портал, который, в свою очередь, может быть настроен на идентификацию пользователей с помощью каталогов Active Directory, Radius, TACACS+, NTLM, Kerberos или локальной базы пользователей.

NGFW определяет следующие типы пользователей:

Наименование	Описание
Пользователь Unknown	Представляет множество пользователей, не идентифицированных системой.
Пользователь Known	Представляет множество пользователей, идентифицированных системой. Методы идентификации пользователей могут быть различными и более подробно будут описаны далее в этой главе.
Пользователь Any	Любой пользователь является объединением множеств пользователей Known и Unknown .
Определенный пользователь	Конкретный пользователь, определенный и идентифицированный в системе, например, пользователь DOMAIN\User, идентифицированный с помощью авторизации в домене Active Directory.

Пользователи и группы пользователей могут быть заведены на самом устройстве NGFW — это так называемые **локальные пользователи и группы** или могут быть получены с внешних каталогов, например, Microsoft Active Directory.

Группы

Группы пользователей позволяют объединить пользователей для более удобного управления политиками безопасности.

Пользователи

В данном разделе можно добавить локальных пользователей. Здесь же можно временно отключить пользователей или включить их заново.

Обязательными параметрами для создания локального пользователя являются имя пользователя и логин. Остальные параметры являются необязательными, но для корректной идентификации необходимо указать:

- Логин и пароль — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
- IP-адрес или диапазон, MAC-адрес для идентификации с помощью комбинации MAC и IP-адресов. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанных MAC и/или IP-адреса.
- VLAN ID для идентификации пользователя по тегу VLAN. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанного VLAN.
- Почтовые адреса — email пользователя. Если указан, может быть использован для отсылки пользователю информации по электронной почте, например, 2-й фактор многофакторной организации.
- Номера телефонов — телефоны пользователя. Если указан, может быть использован для отсылки пользователю информации по SMS, например, 2-й фактор многофакторной организации.

В случае, если у пользователя указан и логин, и пароль, и IP/MAC/VLAN адреса, система использует идентификацию по адресу, то есть идентификация по адресу является более приоритетной.

Учетные записи пользователей LDAP здесь не отображаются, но эти пользователи также могут быть использованы в политиках безопасности.

Серверы аутентификации

Version: 6.1.9

Documentation: ☒

Внимание! На версиях UserGate старше 6.1.8 этот раздел носит название Сервера авторизации.

"Серверы аутентификации" - это внешние источники учетных записей пользователей(сервера аутентификации), например, LDAP-сервер, или серверы, производящие аутентификацию для UserGate, например, Radius, TACACS+, Kerberos, SAML. Система поддерживает следующие типы серверов аутентификации:

- LDAP-коннектор.
- Сервер аутентификации пользователей Radius.
- Сервер аутентификации пользователей TACACS+.
- Сервер аутентификации Kerberos.
- Сервер аутентификации NTLM.
- Сервер аутентификации SAML (SSO).

Серверы аутентификации Radius, TACACS+, NTLM, SAML могут осуществлять только аутентификацию пользователей, в то время как LDAP-коннектор позволяет также получать информацию о пользователях и их свойствах.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.
- Осуществлять аутентификацию пользователей через домены Active Directory/FreeIPA с использованием методов аутентификации Captive-портал, Kerberos, NTLM.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Более подробно о настройке Captive-портала смотрите раздел Настройка Captive-портала .
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.
Kerberos keytab	Здесь можно загрузить keytab-файл для аутентификации Kerberos. Подробно об аутентификации Kerberos и создании keytab-файла смотрите в разделе Метод аутентификации Kerberos.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Примечание

Для аутентификации пользователей с помощью LDAP-коннектора необходимо, чтобы пользователи входили в доменную группу Domain users.

Настройка LDAP-коннектора завершена. Для авторизации LDAP пользователей по имени и паролю необходимо создать правила Captive-портала. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Для добавления пользователя или группы пользователей LDAP в правила фильтрации необходимо нажать на **Добавить пользователя LDAP/Добавить группу LDAP**, в поле поиска указать как минимум один символ, входящий в имена искомых объектов, после чего нажать на **Поиск** и выбрать желаемые группы/пользователей.

Сервер аутентификации пользователей Radius

Сервер аутентификации Radius позволяет аутентифицировать пользователей на серверах Radius, то есть UserGate выступает в роли Radius-клиента. При аутентификации через Radius-сервер UserGate посылает на серверы Radius информацию с именем и паролем пользователя, а Radius-сервер отвечает, успешно прошла аутентификация или нет.

Сервер Radius не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере Radius) или **Unknown** (не прошедших аутентификацию).

Для создания сервера аутентификации Radius необходимо нажать на кнопку **Добавить**, выбрать **Добавить Radius-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секрет	Общий ключ, используемый протоколом Radius для аутентификации.
Хост	IP-адрес сервера Radius.
Порт	UDP-порт, на котором сервер Radius слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.

После создания сервера аутентификации необходимо настроить Captive-портал для использования метода аутентификации Radius. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер аутентификации TACACS+ позволяет аутентифицировать пользователей на серверах TACACS+. При аутентификации через TACACS+ сервер UserGate посылает на серверы TACACS+ информацию с именем и паролем пользователя, а сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Сервер TACACS+ не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших аутентификацию).

Для создания сервера аутентификации TACACS+ необходимо нажать на кнопку **Добавить**, выбрать **Добавить TACACS+ сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.

Наименование	Описание
Порт	Порт, на котором сервер TACACS+ слушает запросы на аутентификации. По умолчанию это порт TCP 49.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+. Внимание! Чтобы данная опция работала, необходимо также настроить её на стороне сервера TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет аутентифицировать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю единожды авторизовавшись в системе SSO прозрачно проходить авторизацию на всех ресурсах, поддерживающих аутентификацию SAML. UserGate может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для аутентификации клиента.

Внимание! Сервер SAML IDP не может предоставить свойства пользователей в UserGate поэтому, если не настроено подключение к домену AD с помощью LDAP-коннектора, в политиках фильтрации можно использовать только пользователей типа Known (успешно прошедших аутентификацию на сервере SAML) или Unknown (не прошедших аутентификацию).

Настройка ADFS

Для использования аутентификации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи соответствующие серверу UserGate для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть Trusted .
Шаг 2. Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 3. Изменить адрес Домен auth captive-портала.	Изменить адрес Домен auth captive-портала в разделе Настройки на созданную на предыдущем шаге запись DNS. Подробно об изменении адреса домена Auth Captive-портала смотрите в разделе Общие настройки .
Шаг 4. Настроить сервер SAML IDP.	Статью по настройке Microsoft ADFS можно найти на сайте Microsoft . Необходимо добавить на сервере SAML IDP запись о сервис-провайдере USERGATE, указывая созданное на шаге 1 FQDN имя. В процессе установки ADFS будет сгенерирована ссылка на xml-файл вида <code>https://<adfs-server>/federationmetadata/2007-06/federationmetadata.xml</code> с конфигурацией и сертификатом ADFS. Эта ссылка понадобится для настройки сервера SAML-авторизации на UserGate NGFW.
Шаг 5. Создать сервер авторизации пользователей SAML IDP.	Создать в USERGATE сервер аутентификации пользователей SAML IDP.

Настройка UserGate NGFW

Для создания сервера аутентификации пользователей SAML IDP необходимо в разделе **Пользователи и устройства → Серверы авторизации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** выполнив следующие шаги

Наименование	Описание
Шаг 1. Заполнить поле SAML metadata URL	SAML metadata URL - это путь где можно скачать xml-файл (полученный ранее при настройке ADFS) с корректной конфигурацией для сервис-провайдера (клиента) SAML. Также заполнить все необходимые поля кроме URL для метаданных SAML IDP (оно появится после сохранения).
Шаг 2. Нажать на кнопку Загрузить	При этом происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла.
Шаг 3. Нажать кнопку Сохранить	При этом произойдет автоматическое заполнение поля URL для метаданных SAML IDP .
Шаг 4. Открыть для редактирования только что созданный SAML IDP сервер.	Теперь можно скопировать автоматически сгенерированную ссылку на файл метаданных UserGate NGFW из поля URL для метаданных SAML IDP .
Шаг 5. Передать метаданные UserGate NGFW на сервер ADFS	С помощью данной ссылки нужно передать данные на ADFS сервер (в настройках ADFS сервера загрузить этот файл аналогично как это сделано на UserGate NGFW.).

Это предпочтительный метод настройки сервера аутентификации SAML IDP.

Описание полей Сервера авторизации доступных для заполнения:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL до файла метаданных сервера ADFS, который необходимо получить. Создается при настройке ADFS.
Сертификат SAML IDP	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: - Создать новый сертификат из скачанного - если при настройке был использован метод загрузки xml- файла, то сертификат автоматически создается и ему назначается роль SAML IDP (смотрите раздел Управление сертификатами). - Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе Сертификаты, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP. - Не использовать сертификат. Примечание Сертификат нужен для установки SSL/TLS соединения между ADFS и UserGate NGFW.
Single sign-on URL	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single sign-on binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout URL	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Сервер аутентификации NTLM

Аутентификация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При аутентификации с помощью NTLM сервер UserGate работает с контроллерами домена, которые выполняют проверку пользователя, который получает доступ в интернет.

Сервер NTLM не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере NTLM) или **Unknown** (не прошедших аутентификацию).

Аутентификация NTLM может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан. Настройка UserGate не отличается от режима работы аутентификации.

Для настройки аутентификации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить синхронизацию времени с контроллером домена.	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и - опционально - запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 2. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть Trusted .
Шаг 3. Изменить адрес Домен Auth Captive-портала .	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки . Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала .
Шаг 4. Добавить NTLM-сервер авторизации.	В разделе Серверы авторизации нажать на кнопку Добавить , выбрать Добавить NTLM-сервер и указать название и имя домена Windows. Для корректной работы авторизации NTLM, необходимо, чтобы указанное здесь имя домена разрешалось(resolve) в IP-адреса контроллеров домена.
Шаг 5. Создать правило Captive-портала с авторизацией NTLM.	Настроить Captive-портал для использования метода авторизации NTLM. Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 6. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM
Шаг 7. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate в качестве адреса прокси сервера. Примечание Вместо IP-адреса можно использовать доменное имя, но для NTLM важно, чтобы это имя было не из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos. Важно! В настройках UserGate имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.
Шаг 8. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность , выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security , выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password) Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации Kerberos

Аутентификация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При аутентификации через Kerberos сервер UserGate работает с контроллерами домена, которые выполняют проверку пользователя, который получает доступ в интернет.

Аутентификация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для аутентификации Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть Trusted. Примечание Для корректной работы создайте записи типа A, не используйте CNAME-записи.
Шаг 2. Создать пользователя для сервера UserGate.	Создать пользователя в домене AD, например, kerb@domain.loc с опцией password never expires. Установите пароль пользователю kerb. Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb. Важно! Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.
Шаг 3. Создать keytab-файл.	На контроллере домена, создать keytab файл, выполнив следующую команду из-под администратора (команда в одну строку!): <pre>ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab</pre> Введите пароль пользователя kerb. Важно! Команда чувствительна к регистру букв. В данном примере: auth.domain.loc - DNS-запись, созданная для сервера UserGate на шаге 1 DOMAIN.LOC - Kerberos realm domain, обязательно большими буквами! kerb@DOMAIN.LOC - имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Шаг 4. Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 5. Настроить синхронизацию времени с контроллером домена.	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и - опционально - запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 6. Изменить адрес Домен auth captive-портала .	Изменить адрес Домен auth captive-портала и опционально адрес Домен logout captive-портала в разделе Настройки на созданные на предыдущем шаге записи DNS. Подробно об изменении адресов доменов смотрите в разделе Общие настройки .
Шаг 7. Создать LDAP-коннектор и загрузить в него keytab-файл.	Создать сервер аутентификации типа LDAP коннектор и загрузить полученный на предыдущем шаге keytab-файл. Важно! Не используйте в качестве пользователя для LDAP-коннектора, пользователя, созданного ранее для работы Kerberos. Необходимо использовать отдельную учетную запись. Подробно о настройке LDAP-коннектора смотрите раздел LDAP-коннектор.
Шаг 8. Создать правило Captive-портала с авторизацией Kerberos.	Настроить Captive-портал для использования метода аутентификации Kerberos. Более подробно о Captive-портале рассказывается в разделе Настройка Captive-портала .
Шаг 9. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.
Шаг 10. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени USERGATE, созданного на шаге 3.

Наименование	Описание
Шаг 11. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность, выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security, выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password) Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Критически важно! Если браузер осуществляет запрос по https, но на NGFW дешифрование не настроено, то NGFW не в состоянии вмешаться в трафик и вставить туда требование авторизоваться по Kerberos. Для того, чтобы была возможность это сделать, в NGFW по умолчанию идёт правило [Decrypt all for unknown users](#), которое включает дешифрование трафика для не авторизованных подключений.

Метод аутентификации HTTP Basic

Аутентификация Basic позволяет авторизовать пользователей с явно указанным прокси сервером по базе локальных и LDAP-пользователей. Не рекомендуется использовать данный тип аутентификации поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификацию HTTP Basic можно использовать для автоматической авторизации утилит командной строки, которым необходим доступ в интернет, например:

```
curl -x 192.168.179.10:8090 -U user: password http://www.msn.com
```

Для аутентификации HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть Trusted.
Шаг 2. Изменить адрес Домен Auth Captive-портала .	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки. Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 3. Создать правило Captive-портала с аутентификации HTTP Basic.	Настроить Captive-портал для использования метода аутентификации HTTP Basic. При настройке, помимо метода HTTP Basic, необходимо добавить базу пользователей, по которой будет проверяться аутентификация (например, добавить методы аутентификации Локальный пользователь или Сервер LDAP). Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 4. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM.
Шаг 5. Настроить прокси-сервер на компьютерах пользователей	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate в качестве адреса прокси сервера.

Профили аутентификации

Version: 6.1.9, 5.x

Documentation: ☒

Внимание! На версиях UserGate старше 6.1.8 этот раздел носит название Профили авторизации.

Профиль аутентификации позволяет указать набор способов и параметров аутентификации пользователей, которые в дальнейшем можно будет использовать для авторизации в различных подсистемах UserGate, например, Captive-портал, VPN, веб-портал и т.д. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства** → **Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название Captive-профиля.
Описание	Описание Captive-профиля.
Профиль MFA	Профиль мультифакторной авторизации. Должен быть предварительно создан в разделе Профили MFA, если планируется использовать мультифакторную авторизацию с данным профилем аутентификации. Профиль определяет способ доставки одноразового пароля для второго метода авторизации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее. Важно! Мультифакторная авторизация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только те, где пользователь явно вводит свои учетные данные в веб-форму страницы авторизации. В связи с этим, мультифакторная авторизация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Данный параметр определяет, через сколько секунд UserGate переведет пользователя из Known users в Unknown users при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя).
Время жизни авторизованного пользователя	Данный параметр определяет, через сколько секунд UserGate переведет пользователя из Known users в Unknown users . По происшествии указанного времени пользователю потребуются повторно авторизоваться на Captive-портале.
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя.
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации.
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например, сервер авторизации Active Directory или RADIUS. Если указано более одного метода аутентификации, то они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов авторизации, таких как: • Локальный пользователь - авторизация по базе данных локально заведенных пользователей. • Принять политику -- не требуется авторизация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип авторизации необходимо применять совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • HTTP Basic -- аутентификация с помощью устаревшего метода HTTP Basic. • Аутентификация Kerberos -- аутентификация с помощью Kerberos.

Настройка Captive-портала

Version: 6.1.9, 5.x

Documentation: 

Captive-портал позволяет авторизовать неизвестных пользователей (**Unknown users**) с помощью методов авторизации с использованием каталогов Active Directory, Radius, TACACS+, SAML IDP, Kerberos, NTLM или локальной базы пользователей. Кроме этого, с помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail.

Следует помнить, что:

- Идентифицированные пользователи, например, у которых в свойствах пользователя явно указан IP-адрес, идентифицированные с помощью агентов авторизации терминальных серверов или для систем Windows, не авторизуются на Captive-портале. Такие пользователи уже относятся к типу **Known users** и не требуют дополнительной идентификации.
- Авторизация с помощью Captive-портала возможна только для протоколов HTTP и HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователя **Known users**, то пользователи не смогут получить доступ в интернет по этому протоколу до тех пор, пока они не станут идентифицированными, то есть не запустят у себя браузер и не пройдут авторизацию на Captive-портале.
- Для авторизации пользователей, работающих по протоколу HTTPS, необходимо настроить инспектирование SSL, иначе авторизация работать не будет.
- Если Captive-портал использует метод авторизации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Настройка Captive-портала сводится к следующим шагам:

Наименование	Описание
Шаг 1. Создать метод авторизации, например, авторизация с помощью домена Active Directory.	В веб-консоли UserGate в разделе Пользователи и устройства → Серверы аутентификации нажать на кнопку Добавить и создать сервер авторизации.
Шаг 2. Создать профиль аутентификации, в котором указать необходимые методы авторизации.	В веб-консоли UserGate в разделе Пользователи и устройства → Профили аутентификации нажать на кнопку Добавить и создать профиль авторизации, используя созданный ранее метод авторизации.
Шаг 3. Создать Captive-профиль, в котором указать необходимые профили аутентификации.	В веб-консоли UserGate в разделе Пользователи и устройства → Captive-профили нажать на кнопку Добавить и создать Captive-профиль, используя созданный ранее профиль авторизации.
Шаг 4. Создать правило Captive-портала.	Правило Captive-портала определяет трафик, к которому должны быть применены методы идентификации пользователей, указанные в Captive-профиле. В веб-консоли UserGate в разделе Пользователи и устройства → Captive-портал нажать на кнопку Добавить и создать правило Captive-портала.
Шаг 5. Настроить DNS для доменов auth.captive и logout.captive.	Служебные доменные имена auth.captive и logout.captive используются UserGate для авторизации пользователей. Если клиенты используют в качестве DNS-сервера сервер UserGate, то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса сервера UserGate, который подключен в клиентскую сеть. Альтернативное решение - настроить параметры Домен auth captive-портала и Домен logout captive-портала . Более детально эти параметры описаны в разделе Общие настройки .
Шаг 6. Разрешить работу сервисов Captive-портал и HTTP(S)-проxy в зоне.	В веб-консоли UserGate в разделе Сеть → Зоны выбрать зону источника Captive-правила с Шага 4 , нажать кнопку Редактировать . В открывшемся окне перейти во вкладку Контроль доступа и установить флаги в пунктах Captive-портал и страница блокировки и HTTP(S)-проxy .

Создание методов авторизации подробно рассматривалось в предыдущих главах. Рассмотрим более подробно создание Captive-профиля и правил Captive-портала.

Чтобы создать Captive-профиль, необходимо в разделе **Captive-профили** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название Captive-профиля.
Описание	Описание Captive-профиля.
Шаблон страницы авторизации	Выбрать шаблон страницы авторизации. Создавать страницы авторизации можно в разделе Библиотеки → Шаблоны страниц . Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, то следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).
Метод идентификации	Метод, с помощью которого UserGate запомнит пользователя. Возможны 2 варианта: • Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю. Данный метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и сервером UserGate. Это рекомендуемое значение, устанавливаемое по умолчанию. • Запоминать cookie. После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя. Данный метод позволяет авторизовать пользователей, находящихся за NAT-устройством, но авторизуется только протокол HTTP(S) и только в том браузере, в котором происходила авторизация через Captive-портал. Кроме этого, для авторизации HTTPS-сессий пользователя UserGate будет принудительно дешифровать все HTTPS-соединения. Для правил межсетевого экрана пользователь, идентифицированный по cookie, будет всегда определен как Unknown user.
Профиль аутентификации	Созданный ранее профиль авторизации, определяющий методы аутентификации.
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
Разрешить браузерам запомнить авторизацию	Включает возможность сохранить авторизацию в браузере на указанное время в часах. Для сохранения авторизационной информации используются cookie.
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется авторизация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице авторизации. Если данный параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.
HTTPS для страницы аутентификации	Использовать HTTPS при отображении страницы авторизации Captive-портала для пользователей. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. Более подробно о сертификатах смотрите в разделе Управление сертификатами .

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке **Регистрация гостевых пользователей**. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться 2 типа - SMS и email. Более подробно о создании профиля оповещения смотрите в главе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.

Наименование	Описание
Тема оповещения	Тема оповещения (только для email-оповещений).
Письмо оповещения	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль.
Дата и время окончания	Время, когда учетная запись временного пользователя будет отключена.
Время жизни	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена.
Длина пароля	Определяет длину пароля для создаваемого пользователя.
Сложность пароля	Определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы.
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи. О группах для временных пользователей читайте в главе Гостевой портал .

Чтобы создать правило Captive-портала, необходимо нажать на кнопку **Добавить** в разделе **Captive-портал** и указать необходимые параметры:

Наименование	Описание
Название	Название правила Captive-портала.
Описание	Описание правила Captive-портала.
Captive-профиль	Выбрать Captive-профиль, созданный ранее. Доступно действие Не использовать аутентификацию , при выборе которого авторизация не будет требоваться.
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
Источник	Адреса источника. В качестве источника можно указать определенную зону, например, зону LAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Адреса назначения. В качестве адресов можно указать определенную зону, например, зону WAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Категории	Категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.
URL	Списки URL, для которых будет применяться правило.

Наименование	Описание
Время	Время, когда данное правило будет активно.

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

ПримечаниеУсловия, указанные во вкладках правила, применяются согласно логике "И", то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику "ИЛИ", то это достигается путем создания нескольких правил.

ПримечаниеПравила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил с помощью соответствующих кнопок.

ПримечаниеПри обработке правил применяется только первое сработавшее правило.

В случае, если необходимо сменить пользователя после его авторизации в системе или выйти из системы, необходимо перейти на URL <http://logout.captive> и нажать на кнопку **Выйти**.

Профили MFA (мультифакторной аутентификации)

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: 

Мультифакторная аутентификация — это метод идентификации и аутентификации пользователя, где используются два или более различных типа идентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

NGFW поддерживает мультифакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации и следующих типов в качестве второго:

- **TOTP** (Time-based One Time Password) токена в качестве второго. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром; более подробно о TOTP можно прочитать в https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. В качестве TOTP-токена могут выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например, Google Authenticator.
- **SMS** — получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory.
- **Email** — получение одноразового пароля по электронной почте. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory.

Чтобы настроить мультифакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить авторизацию с помощью Captive-портала.	Мультифакторная авторизация работает только при авторизации пользователей с помощью Captive-портала. Смотрите раздел для подробной информации.
Шаг 2. Создать профиль мультифакторной авторизации.	В разделе консоли Пользователи и устройства → Профили MFA создать профиль мультифакторной авторизации. При создании профиля указать необходимые настройки доставки второго фактора авторизации. Возможно создать 3 типа доставки: • MFA через TOTP — доставка второго фактора авторизации с помощью токенов TOTP. • MFA через SMS — доставка второго фактора авторизации с помощью SMS. • MFA через email — доставка второго фактора авторизации с помощью email.

Для способа доставки **MFA через TOTP** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Инициализация TOTP	Для получения токенов TOTP необходимо произвести первоначальную инициализацию устройства или ПО клиента. Для этого требуется ввести уникальный ключ в устройство или ПО клиента. Передать первоначальный код для инициализации TOTP можно следующими средствами: • Показать на странице Captive-портала после первой успешной авторизации. Для этого варианта необходимо выбрать Показать ключ на странице Captive -портала. • Выслать с помощью SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки SMS (профиль SMPP). • Выслать с помощью email. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки email (профиль SMTP).
Показывать QR-код	Показывать QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.

В случае, если пользователь утратил токен, администратор может потребовать повторной инициализации TOTP-токена. Для этого ему необходимо выбрать данного пользователя в списке пользователей (**Пользователи и устройства** → **Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей авторизации пользователю будет предложено заново проинициализировать свой токен.

Для способа доставки **MFA через SMS** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробно о настройке профилей отсылки сообщений через SMS смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Для способа доставки **MFA через email** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по электронной почте смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Тема	Тема оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Пользователи терминальных серверов

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: 

Терминальный сервер служит для удаленного обслуживания пользователя с предоставлением рабочего стола или консоли. Как правило, один терминальный сервер предоставляет свой сервис нескольким пользователям, а в некоторых случаях десяткам или даже сотням пользователей. Проблема идентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и NGFW не может корректно идентифицировать сетевые подключения пользователей. Для решения данной проблемы предлагается использование специального агента терминального сервиса. Каждому пользователю выделяется диапазон портов, с использованием которых происходит соединение пользователя, т.е. исходные порты подменяются на порты из выделенного для пользователя диапазона.

Агент терминального сервиса должен быть установлен на все терминальные серверы, пользователей которых необходимо идентифицировать. Агент представляет собой сервис, который передает на NGFW информацию о пользователях терминального сервера и об их сетевых соединениях. В силу специфики работы протокола TCP/IP, агент терминального сервиса может идентифицировать трафик пользователей, передаваемый только с помощью TCP и UDP протоколов. Протоколы, отличные от TCP/UDP, например, ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей, в случае использования на терминальных серверах авторизации Active Directory, требуется настроенный сервер Active Directory коннектор.

Чтобы начать работу с аутентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис агент аутентификации на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис Агент аутентификации для той зоны, со стороны которой расположены серверы терминального доступа.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажать на кнопку Настроить и задать пароль агентов терминального сервера.
Шаг 3. Установить агент терминального сервера.	Установить агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке следует задать IP-адрес NGFW и заданный на предыдущем шаге пароль.
Шаг 4. Добавить необходимые серверы в консоли NGFW.	В разделе Пользователи и устройства → Терминальные серверы необходимо добавить агентов терминального сервера, указав имя и адрес хоста. После получения данных с указанного в настройках хоста и совпадении пароля, указанного в пункте 2, авторизация пользователей будет включена автоматически. При обновлении версии NGFW агенты терминальных серверов, которые ранее отображались в веб-консоли, будут продолжать работать.

UserGate теперь будет получать информацию о пользователях.

Агент терминального сервера позволяет авторизовывать не только доменных, но и локальных пользователей терминального сервера. Для этого необходимо добавить в файл конфигурации (%ALLUSERSPROFILE%\Entensys\Terminal Server Agent\tsagent.cfg) следующий параметр:

LocalDomain = 1

После изменения файла конфигурации сервис терминального агента нужно перезапустить.

Таких пользователей также необходимо добавить в NGFW как локальных. О добавлении пользователей читайте в разделе [Пользователи](#). При добавлении необходимо указать **Логин** в формате: «*имя компьютера_имя пользователя*»; пароль указывать не нужно.

Примечание Имя компьютера должно состоять из букв, цифр и знака подчёркивания. Использование тире в имени компьютера возможно только в том случае, если используются только доменные пользователи.

Параметры терминального сервера могут быть изменены путём внесения изменений в файл конфигурации агента авторизации для терминальных серверов. После внесения изменений агент авторизации необходимо перезапустить.

Ниже представлен список параметров файла tsagent.cfg:

- **TimerUpdate:** периодичность отправки данных (указывается в секундах).
- **MaxLogSize:** максимальный размер журнала работы сервиса (указывается в Мбайт).
- **SharedKey:** пароль для подключения агента.
- **SystemAccounts:** может принимать значения **0** или **1**. При значении параметра **SystemAccounts=1** включает передачу информации о соединениях системных аккаунтов (system, local service, network service) и портах, используемых для соединения, на NGFW.
- **FQDN:** может принимать значения **0** или **1**. Значение параметра **FQDN=1** соответствует использованию FQDN (Fully Qualified Domain Name), например, «example.com» вместо «example».

- **ServerPort**: номер порта NGFW, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- **ServerAddress**: IP-адрес устройства UserGate, принимающего соединение от агента авторизации.
- **UserCount**: максимальное количество пользователей.
- **BlockDNS**: может принимать значения **0** или **1**. При **BlockDNS=1** происходит замена порта источника на свободный порт из выделенного для пользователя диапазона при DNS запросе (UDP:53); при **BlockDNS=0** — отправка трафика происходит без замены порта.
- **BlockUDP**: может принимать значения **0** или **1**. Значение параметра **BlockUDP=1** соответствует замене порта источника на свободный порт из выделенного для пользователя диапазона при отправке трафика UDP; при **BlockUDP=0** — отправка трафика происходит без замены порта.
- **ExcludeIP**: в случае, если на терминальном сервере настроены несколько IP-адресов, то все они будут использованы для аутентификации пользователей. Параметр ExcludeIP позволяет ограничить аутентификацию пользователей с определённых IP-адресов терминального сервера:
 - IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
 - Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
 - Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
 - Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP** . Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore** .
- **ExcludePorts**: диапазон, порты из которого не будут подменяться на порты из выделенного для пользователя диапазона портов (диапазон портов указывается следующим образом: **ExcludePorts=port1-port2**).
- **NAT_IP**: необходим при наличии NAT между терминальным сервером и UserGate: замена IP-адреса терминального сервера на один из адресов указанного диапазона. Адреса указываются в следующем виде: **NAT_IP="12.3.4-1.1.1.1;2.2.2-5.5.5.5"**.

Для исключения из рассылки определенных адресов и/или подсетей терминальным агентом помимо добавления параметра **ExcludeIP** в файл конфигурации tsagent.cfg он может быть активирован и в реестре сервера следующим образом:

- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Прокси-агент для Windows

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: 

Для пользователей, работающих на операционной системе Windows, существует возможность предоставить доступ в интернет через явно указанный прокси-сервер программам, которые не поддерживают работу через прокси-сервер. Иногда также возникает необходимость предоставить таким программам доступ в интернет в случае, когда NGFW не является шлюзом в интернет по умолчанию для пользовательских компьютеров. Для подобных случаев можно использовать прокси-агент. Прокси-агент пересылает все TCP-запросы, идущие не на локальные адреса, на NGFW, который выступает для них прокси-сервером.

Примечание Прокси-агент не авторизует пользователя на NGFW, таким образом, если необходима авторизация, то потребуется настроить один из способов авторизации пользователей, например, установить агент авторизации для Windows.

Установить прокси-агент возможно вручную либо с использованием политик Active Directory.

Прокси-клиент может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 ГБ оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске.

Если устанавливаете не политикой, то для настройки агента необходимо создать текстовый файл utmagent.cfg в директории %ALLUSERSPROFILE%\Entensys\UTMAgent\. В файле конфигурации следует указать:

ServerName=10.255.1.1

ServerHttpPort=8090

LocalNetwork=192.168.1.0/24; 192.168.0.0/24; 192.168.30.0/24;

где ServerName и ServerHttpPort — IP-адрес и порт прокси-сервера на NGFW, по умолчанию это порт 8090.

Примечание LocalNetwork — список сетей, которые не нужно направлять в прокси. Сеть интерфейсов машины не направляется в прокси по умолчанию.

Если запрос от программы, установленной на компьютере, происходит на адрес, находящийся в одной подсети с адресом интерфейса компьютера, то этот запрос не перехватывается прокси-агентом и не перенаправляется на адрес прокси-сервера. Аналогично, если какая-либо программа, установленная на этом компьютере, обращается на адрес из подсети, указанной в параметре LocalNetwork, то этот запрос также не перенаправляется агентом на прокси-сервер.

Сервис прокси-агента слушает локальный порт 8080.

После создания или изменения файла конфигурации необходимо перезапустить сервис прокси-агента.

Если вы устанавливаете через GPO, прокси-агент поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft

Все необходимые параметры для корректной работы прокси-агента задаются при настройке групповой политики. При установке параметры вносятся в реестр пользовательского компьютера и имеют приоритет перед файлом .cfg. При удалении агента политикой значения реестра не удаляются, сохраняясь в ветке реестра:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Entensys\UTMAgent

Управление гостевыми пользователями

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1

Documentation: 

NGFW позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или email.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать администратора гостевых пользователей (опционально).	- В разделе Администраторы нажать кнопку Добавить и создать профиль администратора, разрешающий Гостевой портал для чтения и записи в закладке Разрешения для веб-консоли. Данный профиль дает доступ в консоль управления временными пользователями. - Создать учетную запись администратора и назначить ей созданную роль. Более подробно о создании администраторов NGFW смотрите соответствующий раздел руководства.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей. Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Подключиться к консоли управления Гостевого портала.	В браузере перейти на адрес https://IP_NGFW:8001/ta Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1.
Шаг 4. Создать список пользователей.	В консоли нажать на кнопку Добавить и заполнить поля: - Количество пользователей. - Комментарий. Дата и время окончания — время, когда учетная запись гостевого пользователя будет отключена. Длина пароля — определяет длину пароля для создаваемого пользователя. Сложность пароля — определяет сложность пароля для создаваемого пользователя. Возможны варианты: - Цифры. - Буквы + цифры. - Буквы + цифры + спецсимволы. Время жизни — продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена. Группа — созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи.

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через email).	В разделе Библиотеки → Профили оповещений нажать кнопку Добавить и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений.

Наименование	Описание
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи.	В разделе Пользователи и устройства в подразделе Captive-профили создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон Captive portal: email auth или Captive portal: SMS auth , в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времена действия учетной записи. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений .
Шаг 4. Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль.	В разделе Пользователи и устройства → Captive-портал создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства Настройка Captive-портала .

Radius accounting

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: 

NGFW может прозрачно аутентифицировать пользователей, уже прошедших аутентификацию на внешнем сервере RADIUS. NGFW не взаимодействует с сервером RADIUS, а только отслеживает информацию RADIUS accounting, перенаправленную от RADIUS клиента. RADIUS accounting содержит информацию об имени и IP-адресе пользователя. Для настройки нужно выполнить следующие шаги:

Наименование	Описание
Шаг 1. Завести пользователя в NGFW.	Завести необходимых локальных пользователей в NGFW. Смотрите раздел Пользователи.
Шаг 2. Разрешить сервис Агент авторизации на требуемой зоне.	В разделе Сеть → Зоны , выберите зону, на интерфейс которой планируется отсылать RADIUS-accounting. Разрешите сервис Агент авторизации . Более подробно о настройке зон смотрите в разделе Настройка зон.
Шаг 3. Настроить пароль агентов терминального сервиса.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажмите на кнопку Настроить и укажите пароль агента терминального сервиса. Данный пароль будет использоваться в качестве RADIUS secret при настройке сервера RADIUS.
Шаг 4. Добавить источник RADIUS accounting в веб-консоли NGFW.	В разделе Пользователи и устройства → Терминальные серверы необходимо добавить источник информации RADIUS accounting, указав имя и IP-адрес хоста.
Шаг 5. Настроить RADIUS accounting.	Настроить отсылку информации RADIUS accounting на NGFW, указав в качестве IP-адреса сервера IP-адрес UserGate, порт — UDP 1813. Указать RADIUS secret, совпадающий с паролем агента для терминального сервера, указанным на шаге 3. Имя пользователя необходимо передавать в атрибуте RADIUS User-Name (type=1), IP-адрес пользователя — в атрибуте RADIUS Framed-IP-Address (type=8), а IP-адрес сервера RADIUS — в атрибуте RADIUS NAS_IP_Address (type=4). Более подробно о настройке сервера RADIUS смотрите в руководстве на используемый вами сервер RADIUS и RADIUS клиент. Важно! Период обновления информации RADIUS accounting должен быть не более 120 секунд.

После выполнения данной настройки, NGFW будет сопоставлять имя пользователя и присылаемый сервером RADIUS accounting IP-адрес пользователя. В зависимости от передаваемой информации NGFW будет вести себя следующим образом:

Наименование	Описание
RADIUS сервер прислал имя пользователя, который не заведен на NGFW.	На Accounting-запрос будет ответ Accounting reject. Данные о пользователях не изменятся.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Start или Interim-Update.	Указанному пользователю присвоится переданный IP-адрес. Имя пользователя начнет отображаться в журналах для данного IP-адреса. Пользовательские правила начнут применяться для трафика данного IP-адреса. Если у пользователя уже был IP-адрес, отличный от переданного, то пользователю будет присвоено 2 и более IP-адресов. Если пользователю уже присвоен данный IP-адрес, то ничего не происходит. Если этот IP-адрес присвоен другому пользователю, то он будет удален у того пользователя и будет присвоен пользователю, указанному в запросе.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Stop.	У указанного пользователя удалится переданный IP-адрес. Имя пользователя перестанет отображаться в журналах для данного IP адреса. Пользовательские правила перестанут применяться для трафика данного IP-адреса.

Политики BYOD

Version: 6.1.9, 5.x

Documentation: ☒

Многие компании поддерживают работу сотрудников с персональных устройств, принадлежащих самим сотрудникам. Это так называемые устройства BYOD (Bring Your Own Device). UserGate дает администратору возможность управлять BYOD устройствами, например, установив ограничения на типы разрешенных устройств, на количество устройств, с которых пользователь может получить доступ к сети одновременно, или указав конкретные устройства, с которых будет разрешен доступ в интернет.

Примечание Управление BYOD требует наличия корректно настроенной авторизации пользователей через Captive-портал. Пользовательские устройства, не авторизованные с помощью Captive-портала, не могут управляться с помощью политик BYOD. Более подробно о Captive-портале смотрите в главе [Настройка Captive-портала](#).

Для управления устройствами BYOD необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать правило Captive-портала.	Подробнее о создании правил Captive-портала смотрите раздел Настройка Captive-портала .
Шаг 2. Создать политику BYOD.	Создать одно или несколько правил политики BYOD.

Примечание Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Примечание Если не создано ни одного правила, то разрешены все типы устройств.

Чтобы создать правило политики BYOD, необходимо нажать на кнопку **Добавить** в разделе правил **Политики BYOD** и указать необходимые параметры:

Наименование	Описание
Название	Название правила политики BYOD.
Описание	Описание правила политики BYOD.
Действие	Разрешить : разрешает подключение к сети устройств, удовлетворяющих условиям правила. Запретить : запрещает подключение к сети устройств, удовлетворяющих условиям правила.
Подтверждение администратора	Только для разрешающих правил. Если данная опция включена, то после первой успешной авторизации пользователя через Captive-портал устройство пользователя помещается в список устройств BYOD, но доступ в сеть не предоставляется до подтверждения данного устройства администратором.
Разрешено устройств всего	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь может получать доступ в сеть. Если в правиле используются типы пользователей Known , Unknown или Any , то данный параметр не применяется.
Разрешено устройств одновременно	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь одновременно может получать доступ в сеть. Если в правиле используются типы пользователей Known , Unknown или Any , то данный параметр не применяется.
Пользователи и группы	Список пользователей и групп пользователей, для которых применяется данное правило политики BYOD.
Тип устройства	Тип устройств, для которых применяется данное правило политики BYOD.

Устройства, с которых пользователи подключаются в сеть, отображаются в разделе **Пользователи и устройства → Устройства BYOD**. Администратор может запретить доступ пользователя с определенного устройства, выбрав устройство в списке и нажав на кнопку **Отключить**, или разрешить доступ, нажав на кнопку **Включить**. Здесь же можно подтвердить доступ пользователя с определенного устройства в случае, если политика BYOD требует подтверждение устройства администратором.

Агент аутентификации для Windows

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

Для пользователей, работающих на операционной системе Windows, входящих в домен Active Directory, существует еще один способ аутентификации — использовать специальный агент аутентификации. Агент представляет собой сервис, который передает на NGFW информацию о пользователе, его имя и IP-адрес, соответственно, NGFW будет однозначно определять все сетевые подключения данного пользователя, и аутентификация другими методами не требуется. Чтобы начать работу с пользователями посредством агента аутентификации, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис агент аутентификации на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис Агент аутентификации для той зоны, со стороны которой находятся пользователи.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажать на кнопку Настроить и задать пароль агентов терминального сервера.
Шаг 3. Установить агент аутентификации.	Установить агент аутентификации на все компьютеры, для которых необходимо идентифицировать пользователей. Агент аутентификации может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 Гб оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске. Агент аутентификации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. С помощью административного шаблона администратор может задать IP-адрес и порт сервера UserGate, и заданный на предыдущем шаге пароль. Более подробно о разворачивании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft. Агент может быть установлен и без использования групповых политик. Для этого необходимо установить агент из инсталлятора и указать необходимые параметры для подключения к серверу UserGate в следующих ключах реестра: <pre>[HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""</pre>

NGFW теперь будет получать информацию о пользователях. В политиках безопасности можно использовать имена пользователей, как они указаны в Active Directory, для этого необходим настроенный LDAP-коннектор. Если коннектор не настроен, то можно использовать пользователей **Known** и **Unknown**.

Примечание В параметрах агента в качестве адреса назначения «ServerIP» следует указывать IP-адрес интерфейса UserGate NGFW, на который поступают запросы агента, или FQDN, разрешающийся в этот IP-адрес.
Примечание Журнал агента аутентификации можно найти здесь:
[\Users\<username>\AppData\Roaming\Entensys\Entensys Auth Client\entsagent.log](#)

Установленный агент аутентификации отправляет информацию обо всех IP-адресах, назначенных на интерфейсы устройства. В некоторых сценариях может возникнуть необходимость исключить из этой информации определенные IP-адреса с помощью указания сети или диапазона в настройках агента.

Исключить рассылку определенных адресов и/или подсетей агентом аутентификации можно с помощью параметра **ExcludeIP**. Параметр ExcludeIP может иметь следующие настройки:

- IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n, указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
- Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
- Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
- Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP** . Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore** .

Параметр ExcludeIP может быть активирован в системе несколькими способами:

- Добавлен в файл конфигурации агента tsagent.cfg, который создается в разделе: \users\<username>..ApplicationData\Entensys. После внесения изменений агент аутентификации необходимо перезапустить. В этом случае настройки параметра будут действовать только для пользователя, под учетной записью которого создан файл.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

