

Table of Contents

Table of Contents	1
Пользователи и устройства	2
Серверы аутентификации	3
Профили аутентификации	8

Серверы аутентификации

Product: WAF
Version: 7.x

Серверы аутентификации — это внешние источники учетных записей пользователей, например, LDAP-сервер, или серверы, производящие аутентификацию для WAF, например, RADIUS, TACACS+, SAML. Система поддерживает следующие типы серверов аутентификации:

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.

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, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то WAF получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, WAF будет использовать резервный. В случае недоступности части контроллеров домена с площадки, где работает WAF, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе.
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.
Срок жизни LDAP-кэша	Срок жизни LDAP-кэша (от 1 до 48 часов). Новый срок жизни применяется к новым записям, добавляемым в LDAP-кэш после того, как администратор его установит. (Доступно начиная с релиза UGOS 7.1.3).
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.
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.

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

Настройка LDAP-коннектора завершена.

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 RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть WAF выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер WAF 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 WAF, поэтому, если пользователи не были заведены в WAF предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере RADIUS) или **Unknown** (не прошедших авторизацию).

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 RADIUS. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При авторизации через TACACS+ WAF 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 WAF, поэтому, если пользователи не были заведены в WAF предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

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+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером 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 авторизовать 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. WAF может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации

клиента.

Сервер SAML IDP не может предоставить свойства пользователей в WAF 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).

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

Наименование	Описание
Создать DNS-записи для WAF.	На контроллере домена создать DNS-запись, соответствующую WAF, для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса WAF, подключенного в сеть Trusted .
Настроить DNS-серверы на WAF.	В настройках WAF в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Настроить сервер SAML IDP.	Добавить на сервере SAML IDP запись о сервис-провайдере WAF, указывая созданное на шаге 1 FQDN имя.
Создать сервер аутентификации пользователей SAML IDP.	Создать в WAF сервер аутентификации пользователей SAML IDP.

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

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку Загрузить происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера аутентификации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации.
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.
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 авторизации с помощью NTLM WAF работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в Интернет.

Сервер NTLM не может предоставить список пользователей в WAF, поэтому, если пользователи не были заведены в WAF предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), 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 WAF не отличается от режима работы авторизации.

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Настроить синхронизацию времени с контроллером домена.	В настройках WAF включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Создать DNS-запись для WAF.	На контроллере домена создать DNS-записи, соответствующие WAF 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 WAF, подключенного в сеть Trusted .
Добавить NTLM-сервер.	В разделе Серверы аутентификации нажать на кнопку Добавить , выбрать Добавить NTLM-сервер и указать название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена.
Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса WAF в качестве адреса прокси-сервера. Важно! 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 WAF 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.
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 авторизации через Kerberos WAF работает с контроллерами домена, которые выполняют проверку пользователя, получающего 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 авторизации с помощью Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Создать DNS-записи для NGFW.	На контроллере домена создать DNS-записи, соответствующие WAF, для использования в качестве доменов для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса WAF, подключенного в сеть Trusted . Важно! Для корректной работы создайте записи типа A, не используйте CNAME-записи.

Наименование	Описание
Создать пользователя для NGFW.	Создать пользователя в домене AD, например, <code>kerb@domain.loc</code> с опцией password never expires. Установите пароль пользователю <code>kerb</code>. Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя <code>kerb</code> или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя <code>kerb</code>. Важно! Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.
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 <code>kerb</code>. Важно! Команда чувствительна к регистру букв. В данном примере: <code>auth.domain.loc</code> — DNS-запись, созданная для сервера UserGate на шаге 1 <code>DOMAIN.LOC</code> — Kerberos realm domain, обязательно большими буквами! <code>kerb@DOMAIN.LOC</code> — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
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.
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. Подробнее о настройке LDAP-коннектора смотрите раздел LDAP-коннектор.
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.
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).

Профили аутентификации

Product: WAF
Version: 7.x

Профиль аутентификации позволяет указать набор способов и параметров авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах WAF. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства** → **Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Время бездействия до отключения	Данный параметр определяет, через сколько секунд WAF 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 WAF переведет пользователя из Known users в Unknown users . По происшествии указанного времени пользователю потребует 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 аутентификации 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 аутентификации, таких как: • Локальный пользователь — аутентификация по базе данных локально заведенных пользователей. • Принять политику — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип аутентификации 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 по протоколу Kerberos.

