Table of Contents

Table of Contents 1
Политики безопасности 2
- Общие сведения 3
- Фильтрация контента 4
- Веб-безопасность 7
- Инспектирование SSL 9
- Работа с внешними ICAP-серверами 12

Политики безопасности

Общие сведения

Product: SWG
Version: 7.5.x

С помощью политик безопасности администратор может:

- Настроить фильтрацию HTTP-контента. Например, запретить некоторым пользователям доступ к определенным категориям сайтов в заданное время или настроить антивирусную проверку веб-контента.
- Настроить опции веб-безопасности. Например, включить принудительный безопасный поиск и блокировку рекламы.
- Настроить правила инспектирования SSL. Например, для всех пользователей расшифровывать HTTPS для категории «Форумы», а для определенной группы — «Социальные сети». После того, как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP.
- Настроить публикацию HTTP/HTTPS-серверов.

События срабатывания правил регистрируются в журнале веб-доступа (**Журналы и отчёты → Журнал веб-доступа**).

Все правила журналируются только при включенной опции «Журналирование» в параметрах правил.

Фильтрация контента

Product: SWG
Version: 7.5.x

С помощью правил фильтрации контента вы можете разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS (если настроено инспектирование HTTPS). UserGate SWG может блокировать HTTPS-трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации UserGate SWG URL filtering или по спискам URL, в которых указаны только имена узлов. В этих случаях UserGate SWG использует SNI (Server Name Indication), а при отсутствии SNI — название узла из SSL-сертификата из пользовательских запросов для определения домена.

В качестве условий правила могут быть использованы параметры:

- Пользователи и группы.
- Наличие на веб-страницах определенных слов и выражений (морфология).
- Принадлежность сайтов категориям.
- URL.
- Зона и IP-адрес источника.
- Зона и IP-адрес назначения.
- Тип контента.
- Информация о реферере.
- Время.
- User agent браузера пользователя.
- HTTP-метод.
- Результат проверки подлинности браузера. Подробнее — в разделе « Работа с доверенными браузерами ».

ПримечаниеФлажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете менять порядок правил в списке, перетаскивая их мышью или используя кнопки «Выше», «Ниже», «Наверх» и «Вниз» на панели инструментов.

ПримечаниеЕсли запрещающее правило является более общим по сравнению с разрешающими правилами, то запрещающее правило отработает перед разрешающими, несмотря на порядок расположения. В итоге, запрещающее правило нужно делать более специфичным, чтобы порядок отрабатывался корректно.
ПримечаниеЕсли не создано ни одного правила, передача любого контента разрешена.

Чтобы создать правило контентной фильтрации, перейдите в раздел **Настройки → Политики безопасности → Фильтрация контента,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Название для страницы блокировки	Альтернативное название правила, которое может отображаться на странице блокировки. Если включено отображение названия правила, пользователю будет показано альтернативное название. Если оно не задано, отображается основное название правила
Описание	Описание правила
Действие	Действие правила: • **Запретить** — блокировать веб-страницу. • **Предупредить** — предупредить пользователя о том, что страница нежелательна для просмотра. Пользователь сам решает, отказаться от просмотра или нет. Запись о просмотре страницы заносится в журнал. • **Разрешить** — разрешить просмотр веб-страницы

Параметр	Описание
Записывать в журнал правил	При активации этой опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики
Проверять потоковым антивирусом UserGate	Доступно только для правил с действием **Запретить**, т. е. при наличии вируса на странице ресурс будет запрещен. Если в правиле присутствуют другие условия (категории, время, и т. д.), антивирусная проверка будет выполняться только при совпадении всех условий правила
Сценарий	Выбор сценария, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии». **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработал ни один из триггеров сценария), правило не сработает
Страница блокировки	Выбор страницы блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Вы можете использовать внешнюю страницу, указав **Использовать внешний URL**, либо указать страницу блокировки на UserGate SWG. В последнем случае можно выбрать желаемый шаблон страницы блокировки, который создается в разделе «Шаблоны страниц». **Примечание**При создании правил контентной фильтрации целесообразно заранее продумать параметры страницы блокировки. Перед настройкой страницы блокировки определите источники подозрительных запросов и характер трафика: если трафик генерируют устройства (машины) без участия пользователей либо ожидается массовое обращение со стороны большого числа клиентов, в правилах рекомендуется указывать внешний URL страницы блокировки или https://127.0.0.1. Это позволит избежать частого повторного отображения локальной страницы блокировки и обеспечить более предсказуемое поведение устройства
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Максимальное количество GeoIP, которое может быть указано: 15. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов
Назначение	Зона, списки IP-адресов, GeoIP-адресов (не более 15 адресов) или доменов назначения трафика. **Важно!** Не добавляйте в списки строки с символом «*», они будут игнорироваться. **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. Для добавления списков доменов назначения используются списки из библиотеки URL. Эта же библиотека применяется при добавлении списков на вкладке **URL**. Следует различать эти два способа использования списков URL. Когда список URL используется как список доменов назначения, выполняется преобразование URL в доменные имена. После этого UserGate SWG каждые 5 минут выполняет разрешение доменных имен из списка в IP-адреса и хранит полученный результат во внутреннем кэше в течение времени жизни DNS-записи. По истечении времени жизни записи UserGate SWG автоматически обновляет IP-адрес. Таким образом, блокирующее или разрешающее правило с настроенным адресом назначения срабатывает по IP-адресам, связанным с доменными именами из списка. Когда список URL выбран на вкладке **URL**, фильтрация контента выполняется по URL, указанным в списке. Подробнее о работе со списками URL — в разделе « Списки URL». **Важно!** При настройке правила контентной фильтрации не рекомендуется использовать один список для адресов назначения и URL.
Пользователи	Список пользователей, групп, для которых применяется правило. Могут быть использованы пользователи типа Any , Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»

Параметр	Описание
Категории	Списки категорий UserGate URL filtering 4.0. Использование категорий требует наличия специальной лицензии. UserGate URL filtering 4.0 — это крупнейшая база электронных ресурсов, разделенных для удобства работы на категории. Вы можете переопределить категорию для любого сайта, на который, по вашему мнению, категория назначена не верно или не назначена совсем. Подробнее о процедуре изменения категории сайта — в разделе «Запросы в белый список» **Важно!** Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования. Страница блокировки в таком случае показана не будет.
URL	Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate. Вы также можете создавать собственные списки URL. Подробнее о работе со списками URL — в разделе «Списки URL» **Важно!** Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена узлов (доменов). Страница блокировки в таком случае показана не будет.
Типы контента	Списки типов контента. Предусмотрена возможность управления видео контентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Вы также можете создавать собственные группы типов контента. Подробнее о работе с типами контента — в разделе «Типы контента»
Морфология	Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари, обновляемые компанией UserGate. Словари доступны на русском, английском, немецком, японском и арабском языках. Вы также можете создавать собственные словари. Подробнее о работе с морфологическими словарями — в разделе «Морфология»
Время	Период, когда правило активно. Вы можете добавить необходимые временные интервалы в разделе « Календари»
Useragent	User agent пользовательских браузеров, для которых будет применено правило. Вы можете добавить необходимые user agent в разделе «User agent браузеров»
HTTP метод	Метод, используемый в HTTP-запросах. Как правило, это POST или GET
Рефереры	Список URL, в котором указаны рефереры (адреса страниц, с которых пользователь перешел к текущему ресурсу) для текущей страницы. Правило сработает, если для этой страницы реферер совпадет со списком указанных URL. Функция часто используется, чтобы разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую
Доверенные браузеры	Проверка подлинности браузера для предоставления доступа к ресурсам. Выберите созданное ранее в разделе **Настройки → Пользователи и устройства → Доверенные браузеры** подключение к серверу регистрации доверенных браузеров. Подробнее о создании подключения к серверу регистрации доверенных браузеров — в разделе «Работа с доверенными браузерами»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. **Важно!** При настроенном инспектировании данных, передаваемых по протоколам TLS/SSL, и срабатывании правила контентной фильтрации Default allow, созданного по умолчанию, счётчик будет срабатывать только для правила инспектирования SSL. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Веб-безопасность

Product: SWG
Version: 7.5.x

С помощью правил раздела **Веб-безопасность** вы можете включить дополнительные параметры безопасности для протоколов HTTP и HTTPS (если настроено инспектирование HTTPS). Доступны следующие параметры:

- Блокировка рекламы. Посещение безопасного сайта может быть связано с принудительным просмотром изображений нежелательного характера, размещенных на странице. UserGate SWG решает эту проблему, блокируя рекламные баннеры.
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. Скрипт будет вставлен в веб-страницы перед тегом </head>.
- Принудительное включение безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. С помощью этого инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например при фильтрации откликов на запросы по графическому или видео контенту.
- Включение журналирования поисковых запросов пользователей.
- Блокировка приложений социальных сетей. Социальные сети играют большую роль в повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. UserGate SWG может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

- Источник трафика.
- Пользователи и группы.
- Время.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете менять порядок правил в списке, перетаскивая их мышью или используя кнопки «Выше», «Ниже», «Наверх» и «Вниз» на панели инструментов.
ПримечаниеФлажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).
ПримечаниеЕсли не создано ни одного правила, дополнительные функции веб-безопасности не применяются.

Чтобы создать правило веб-безопасности, перейдите в раздел **Настройки → Политики безопасности → Веб-безопасность**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Записывать в журнал правил	При активации этой опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики
Блокировать рекламу	Блокировка рекламы. По ссылке **Исключения** вы может выбрать URL-списки сайтов, для которых блокировка рекламы не требуется
Инжектор	Встраивание произвольного кода во все веб-страницы. Для редактирования встраиваемого кода нажмите **Код инжектора**
Безопасный поиск	Принудительно включить функцию безопасного поиска
История поиска	Запись поисковых запросов пользователей в журнал

Параметр	Описание
Блокировать приложения социальных сетей	Блокировка приложений в социальных сетях
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGater SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов
Пользователи	Список пользователей, групп, для которых применяется правило. Могут быть использованы пользователи типа Any , Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Время	Интервал активности правила. Вы можете добавить необходимые временные интервалы в разделе « Календари»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Инспектирование SSL

Product: SWG
Version: 7.5.x

В этом разделе вы можете настроить инспекцию данных, передаваемых по протоколу TLS/SSL. UserGate SWG с функцией SSL-инспектирования выступает в роли доверенного посредника (Man-in-the-Middle, MitM).

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности.

С помощью правил раздела вы можете настроить инспектирование HTTPS только для определенных категорий, например «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и не расшифровывать другие категории, например «Финансы», «Правительство» и т. п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе — SNI (Server Name Indication). При отсутствии SNI может использоваться поле Subject Name в сертификате сервера. Содержимое поля Subject Alternative Name игнорируется.

UserGate SWG перехватывает исходящий запрос на установление SSL-соединения и производит подмену сертификата сервера на свой, выписанный внутренним корневым центром сертификации. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить корневой сертификат центра сертификации в доверенные корневые сертификаты. Подробнее — в разделе «Установка сертификата локального удостоверяющего центра».

Если корневой сертификат доверен, браузер считает полученный сертификат легитимным и устанавливает безопасное SSL-соединение между пользователем и UserGate SWG.

Далее UserGate SWG устанавливает новое, отдельное SSL-соединение с конечным сервером. В итоге UserGate SWG работает как посредник: получает данные от пользователя, проверяет их, шифрует и отправляет на внешний сервер, и наоборот.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете менять порядок правил в списке, перетаскивая их мышью или используя кнопки «Выше», «Ниже», «Наверх» и «Вниз» на панели инструментов.
ПримечаниеФлажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).
ПримечаниеЕсли не создано ни одного правила, SSL не перехватывается и не дешифруются. При этом контент, передаваемый по SSL, не фильтруется.

Чтобы создать правило инспектирования SSL, перейдите в раздел **Настройки → Политики безопасности → Инспектирование SSL**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правил
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Записывать в журнал правил	При активации этой опции информация о срабатывание правила будет регистрироваться в « Журнале веб-доступа»
Действие	Выполняемое действие: • Расшифровать. • Не расшифровывать. • Расшифровать и переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет передана в соответствии с правилом и профилем инспектирования SSL. При выборе этого действия укажите профиль пересылки SSL. Подробнее о настройке профилей пересылки — в разделе «Профили пересылки SSL»
Профиль SSL	Выбор профиля SSL. Параметры, указанные в этом профиле, будут использованы как для установки SSL-соединения от браузера пользователя к UserGate SWG, так и при построении SSL-соединения от UserGare SWG к запрашиваемому веб-ресурсу. Подробнее о профилях SSL — в разделе « Профили SSL»
Блокировать сайты с некорректными сертификатами	Блокировка доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или выдан недоверенным центром сертификации

Параметр	Описание
Проверять по списку отозванных сертификатов	Проверка сертификата сайта в списке отозванных сертификатов (CRL). Если сертификат найден в списке, сайт будет заблокирован
Блокировать сертификаты с истекшим сроком действия	Блокировка сертификатов, срок действия которых истек
Блокировать самоподписанные сертификаты	Блокировка самоподписанных сертификатов
Пользователи	Список пользователей и групп, для которых применяется правило. Могут быть использованы пользователи типа Any , Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Количество указанных GeoIP не может быть больше 15. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов
Адрес назначения	Списки IP-адресов назначения трафика. **Важно!** Количество указанных GeoIP не может быть больше 15. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов. Подробнее о работе со списками IP-адресов — в разделе « IP-адреса»
Сервисы	Сервис, для которого необходимо дешифровать трафик
Категории	Списки категорий UserGate URL filtering 4.0
Домены	Списки доменов. Доменные имена, для которых применяется правило. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена (www.example.com, а не http://www.example.com/home/). Подробнее о работе со списками URL — в разделе «Списки URL»
Время	Интервал активности правила. Вы можете добавлять необходимые временные интервалы в разделе « Календари»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

По умолчанию создано правило инспектирования «SSL Decrypt all for unknown users», которое необходимо для аутентификации неизвестных пользователей через Captive-портал.

Работа с внешними ICAP-серверами

Product: SWG
Version: 7.5.x

ICAP (Internet Content Adaptation Protocol) — это протокол, предназначенный для передачи HTTP-сообщений на внешние серверы с целью их обработки и адаптации. Он работает поверх TCP и по своей структуре напоминает HTTP.

ICAP позволяет прокси-серверам и шлюзам безопасности перенаправлять трафик на выделенные серверы для обработки контента, например для антивирусной проверки, фильтрации или проверки системами предотвращения утечки конфиденциальных данных (data loss prevention, DLP).

Взаимодействие по протоколу ICAP строится по модели «клиент —сервер»:

- ICAP-клиент — это устройство, которое перехватывает HTTP-трафик (прокси-сервер или шлюз безопасности). Клиент инкапсулирует исходное HTTP-сообщение (запрос или ответ) в ICAP-запрос и отправляет его на сервер.
- ICAP-сервер — это устройство, которое принимает трафик от клиента, обрабатывает его и возвращает результат. Роль ICAP-сервера могут выполнять системы DLP, серверы антивирусной проверки или сервисы для модификации контента.

Протокол определяет два основных режима обработки трафика, которые соответствуют направлению движения данных:

- Режим модификации запроса (request modification, REQMOD). В этом режиме ICAP-клиент отправляет на ICAP-сервер HTTP-запрос пользователя. Это актуально, например, при загрузке файла на веб-ресурс (метод POST), чтобы проверить отправляемый контент на наличие конфиденциальных данных.
- Режим модификации ответа (response modification, RESPMOD). В этом режиме ICAP-клиент отправляет на ICAP-сервер HTTP-ответ от веб-сервера. RESPMOD применяется, например, при скачивании файла пользователем: ICAP-сервер проверяет загружаемый объект на наличие вредоносного кода до его доставки пользователю.

Помимо основных методов REQMOD и RESPMOD, протокол поддерживает метод OPTIONS, который позволяет клиенту узнать возможности сервера (например, поддерживаемые методы) перед отправкой данных. В UserGate SWG метод OPTIONS также используется для мониторинга доступности ICAP-серверов.

UserGate SWG при работе с внешними ICAP-серверами исполняет роль ICAP-клиента, передавая HTTP-трафик на ICAP-серверы для дополнительной проверки.

UserGate SWG поддерживает гибкую настройку работы с ICAP-серверами. Вы можете создавать отдельные правила для проверки запросов и ответов (режимы REQMOD и RESPMOD), направляя на ICAP-серверы только выборочный трафик, а также настраивать работу с фермой ICAP-серверов.

Настройка работы с ICAP-серверами

Для работы с внешними ICAP-серверами:

1. Создайте профиль ICAP-сервера.
2. Если необходимо распределять трафик на несколько серверов, вы можете создать правило балансировки трафика на ICAP-серверы.
3. Создайте правило ICAP.

HTTP-запросы пользователя или ответы целевого веб-сервера будут отправляться на проверку на ICAP-серверы при срабатывании ICAP-правила с определенными действиями — «Переслать» или «Переслать и игнорировать».

Создание профиля ICAP-сервера

Чтобы создать профиль ICAP-сервера:

В разделе **Настройки → Политики безопасности → ICAP-серверы,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Название	Название профиля ICAP-сервера
Описание	Описание профиля ICAP-сервера
IP-адрес	IP-адрес ICAP-сервера
Порт	TCP-порт ICAP-сервера, значение по умолчанию: 1344
Максимальный размер сообщения	Максимальный размер сообщения (в килобайтах), направляемого на ICAP-сервер. Чтобы выполнить проверку связи с сервером без отправки данных, укажите в этом поле значение 0

Параметр	Описание
Период проверки соединения с ICAP-сервером	Интервал времени в секундах, через который UserGate SWG посылает запрос на ICAP-сервер для проверки его доступности. Текущее состояние ICAP-сервера отображается в веб-интерфейсе с помощью цветового индикатора
Вес при балансировке	Числовое значение, определяющее относительный вес сервера при балансировке трафика. Запросы распределяются пропорционально заданным весам. Значение 0 исключает сервер из пула балансировки
Максимальное количество соединений	Максимальное количество соединений с сервером, которые могут быть установлены одновременно
Пропускать трафик при ошибке или недоступности ICAP-сервера	При недоступности ICAP-сервера или возникновении непредвиденной ошибки при его работе, переданный на проверку трафик обрабатывается со статусом «Пропустить»
Путь REQMOD	Настройка работы с ICAP-сервером в режиме REQMOD (режим модификации запроса): • **Включено** — использовать в режиме REQMOD; • **Путь REQMOD** — укажите путь обращения к службе ICAP в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер. Можно указать путь в следующих форматах: ◦ /path — путь на сервере ICAP; ◦ icap://icap-server:port/path — указание полного URI
Путь RESPMOD	Настройка работы с ICAP-сервером в режиме RESPMOD (режим модификации ответа): • **Включено** — использовать в режиме RESPMOD; • **Путь RESPMOD** — укажите путь обращения к службе ICAP в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер. Можно указать путь в следующих форматах: ◦ /path — путь на сервере ICAP; ◦ icap://icap-server:port/path — указание полного URI
Передавать имя пользователя	Передача на ICAP-сервер имени пользователя. Параметры для настройки: • **Включено** — отправлять имя пользователя на ICAP-сервер. • **Кодировать в base64** — кодирование имени пользователя в base64. Может потребоваться, если имена пользователей содержат символы национальных алфавитов. • **Название заголовка** — заголовок, который будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — X-Authenticated-User
Передавать IP-адрес пользователя	Передача на ICAP-сервер IP-адреса пользователя. Параметры для настройки: • **Включено** — оправлять IP-адрес пользователя на ICAP-сервер. • **Название заголовка** — заголовок, который будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Ip
Передавать MAC-адрес пользователя	Передача на ICAP-сервер MAC-адреса пользователя. Параметры для настройки: • **Включено** — отправлять MAC-адрес пользователя на ICAP-сервер. • **Название заголовка** — заголовок, который будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Mac

Создание ICAP-правила

ICAP-правила создаются отдельно для режимов обработки запросов и ответов REQMOD и RESPMOD (доступно в версии 7.5.1 и выше). В веб-консоли UserGate SWG в разделе **Настройки → Политики безопасности → ICAP-правила** созданные правила сгруппированы по режимам обработки. Сначала выполняются правила режима REQMOD, затем — RESPMOD. В каждом режиме срабатывает только первое правило, в котором выполняются все указанные условия.

С помощью параметра «Порядок применения правил» в свойствах ICAP-правила (доступно в версии 7.5.1 и выше) вы можете управлять приоритетом обработки трафика правилами фильтрации контента относительно ICAP-правил. Например, вы можете блокировать передачу HTTP-запросов на ICAP-серверы для трафика, запрещенного политикой контентной фильтрации, выбрав в правиле порядок применения: «Правила контентной фильтрации ➔ ICAP-правила».

Важно!Не рекомендуется создавать ICAP-правила одного режима обработки с одинаковыми условиями, действиями и серверами назначения, но различающиеся только приоритетом выполнения (до или после фильтрации контента). Такая конфигурация приводит к повторной отправке трафика на ICAP-сервер, увеличению задержек и дополнительной нагрузке на серверы. Для обеспечения корректной и оптимальной работы политики обработки трафика рекомендуется использовать уникальные условия применения правил в рамках одного режима (REQMOD или RESPMOD).

Итоговый порядок применения ICAP-правил определяется не только их принадлежностью к группе (REQMOD, RESPMOD) и порядковым номером в списке, но и фазой приоритизации (до или после применения правил фильтрации контента). Это означает, что правило с большим порядковым номером, но с приоритетом «до фильтрации контента», может быть выполнено раньше правила с меньшим номером, но имеющим приоритет «после фильтрации контента».

Чтобы создать ICAP-правило:

В разделе **Настройки ➔ Политики безопасности ➔ ICAP-правила,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги»
Описание	Описание правила
Действие	Действие правила: • **Пропустить** — не посылать данные на ICAP-сервер. Создав правило с таким действием, вы можете явно исключить определенный трафик из пересылки на серверы ICAP. • **Переслать** — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Это стандартный режим работы большинства ICAP-серверов. • **Переслать и игнорировать** — переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика
Вставить	Выбор места расположения правила в общем списке правил
Режим проверки	Выбор режима проверки сообщений (доступно в версии 7.5.1 и выше): • **REQMOD** — проверка и модификация запросов (ICAP-сервер получает HTTP-запрос пользователя до его отправки на веб-сервер и может его проверить или изменить); • **RESPMOD** — проверка и модификация ответов (ICAP-сервер обрабатывает HTTP-ответ от веб-сервера перед тем, как он будет отправлен пользователю)
Порядок применения правил	Параметр, определяющий порядок применения правил ICAP и контентной фильтрации (доступно в версии 7.5.1 и выше). Может применяться в сценариях, когда пользователь обращается к ресурсу, запрещенному политикой контентной фильтрации (например, при скачивании файла), чтобы такие запросы могли блокироваться до передачи на ICAP-сервер. Управлять приоритетом выполнения правил контентной фильтрации и ICAP можно для обоих стеков правил (REQMOD и RESPMOD). Значения параметра: • **ICAP-правила ➔ Правила контентной фильтрации**; • **Правила контентной фильтрации ➔ ICAP-правила**

Параметр	Описание
ICAP-серверы	Выбор ICAP-серверов или балансировщиков ICAP-серверов, на которые UserGate SWG будет пересылать трафик. Правила с действием «Пропустить» допускается создавать без добавления ICAP-серверов. Общие правила обработки трафика ICAP-серверами: • В одно правило можно добавить несколько профилей — как отдельных ICAP-серверов, так и балансировщиков. • Очередность обработки зависит от типа профиля: ◦ Сначала трафик последовательно проходит через выделенные ICAP-серверы в порядке их расположения в правиле. ◦ Затем трафик передается балансировщикам, которые опрашиваются также в порядке их расположения в правиле. • Логика работы балансировщиков: выбирается один из управляемых ICAP-серверов на основе настроенного алгоритма распределения нагрузки. Если выбранный сервер не блокирует трафик, обработка передается следующему балансировщику из списка. • Обработка прекращается, как только один из ICAP-серверов блокирует трафик или когда исчерпан весь список серверов. При использовании балансировщика нагрузки рекомендуется устанавливать одинаковые значения следующих параметров для всех обслуживаемых ICAP-серверов: • «Пропускать трафик при ошибке или недоступности ICAP-сервера»; • «Максимальный размер сообщения». Подробнее о балансировщике ICAP — в разделе « Балансировка нагрузки»
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки доменов источника трафика. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение (resolution) доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP-адреса и списки IP-адресов или доменов
Пользователи	Список пользователей, групп, для которых применяется правило. Могут быть использованы пользователи типа Any , Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей
Назначение	IP-адреса, GeoIP или списки доменов назначения трафика. **Важно!** Строки с символом « *» в таких списках не работают (игнорируются). Каждые пять минут UserGate SWG производит разрешение (resolution) доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP-адреса и списки IP-адресов или доменов
Типы контента	Условие срабатывания правила по типу контента. Вы также можете создавать собственные группы типов контента. Подробнее о работе с типами контента — в разделе «Типы контента»
Категории	Условие срабатывания правила по категориям URL. Подробнее о работе с категориями URL — в разделе « Категории URL»
URL	Условие срабатывания правила по спискам URL. Подробнее о работе со списками URL — в разделе « Списки URL»
HTTP-метод	Тип HTTP-метода, применяемого в запросах (обычно POST или GET)
Сервис	Указание типа сервиса (HTTP)

Параметр	Описание