

Table of Contents

Table of Contents	1
Политики безопасности	2
Общие сведения	3
Фильтрация контента	4
Веб-безопасность	6
Инспектирование туннелей	7
Инспектирование SSL	8
Инспектирование SSH	10
Система обнаружения и предотвращения вторжений	12
Сценарии	15
Работа с внешними ICAP-серверами	16
Защита почтового трафика	22
Защита от DoS атак	24

Общие сведения

Documentation: 

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

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" и для определенной группы — "Социальные сети". После того как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Включить и настроить параметры COB.
- Настроить проверку почтовых протоколов SMTP и POP3 на наличие спама.
- Настроить журналирование или блокировку определенных команд АСУ ТП.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP, например, на DLP-системы.
- Настроить публикацию HTTP/HTTPS серверов.

События срабатывания данных правил регистрируются в соответствующих журналах статистики.

Правила фильтрации контента, веб-безопасности и инспектирования SSL доступны в журнале веб-доступа (**Журналы и отчёты → Журнал веб-доступа**).

Правила система обнаружения и предотвращения вторжений — в журнале COB (**Журналы и отчёты → Журнал COB**).

Правила АСУ ТП — в журнале АСУ ТП (**Журналы и отчёты → Журнал АСУ ТП**).

Правила Защита от DoS атак — в журнале трафика (**Журналы и отчёты → Журнал трафика**).

Все правила журналируются только при включении опции **Журналирование** в параметрах правил.

Фильтрация контента

Version: 7.0.1
Product: NGFW
Documentation: ☒

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

В качестве условий правила могут выступать:

- 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.
- Useragent браузера пользователя.
- HTTP-метод.

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

ПримечаниеПравила 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.

ПримечаниеЕсли не создано ни одного правила, то передача любого контента разрешена.

Чтобы создать правило контентной фильтрации, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Фильтрация контента** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Запретить — блокирует веб-страницу. Предупредить — предупреждает пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал. Разрешить — разрешает посещение.
Записывать в журнал правил	При активации данной 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.), то антивирусная проверка будет выполняться только при совпадении всех условий правила.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.
Страница блокировки	Указывает страницу блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Можно использовать внешнюю страницу, указав Использовать внешний URL , либо указать страницу блокировки NGFW. В этом случае можно выбрать желаемый шаблон страницы блокировки, который можно создать в разделе Шаблоны страниц .
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "*" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
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 оперирования на 72 категории. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие. Важно! Начиная с версии UserGate 5.0.6R6 администратор может переопределить категорию на любой сайт, на который, по его мнению, категория назначена не верно или не назначена совсем. Более подробно процедура изменения категории сайта описана в разделе Запросы в белый список. Важно! Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования, но без показа страницы блокировки.
URL	Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate, такие, как «Черный список UserGate», «Белый список UserGate», «Черный список Роскомнадзора», «Черный список фишинговых сайтов», «Поисковые системы без безопасного поиска». Администраторы также могут создавать собственные списки URL. Более подробно о работе со списками URL читайте в главе Списки URL. Важно! Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена хостов (доменов), но без показа страницы блокировки.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента.
Морфология	Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари, обновляемые компанией UserGate, в том числе список материалов, запрещенных Министерством Юстиции Российской Федерации, словари по темам «Суицид», «Терроризм», «Порнография», «Нецензурные выражения», «Азартные игры», «Наркотики», «Защита детей ФЗ-436». Словари доступны на русском, английском, немецком, японском и арабском языках. Администраторы также могут создавать собственные словари. Более подробно о работе с морфологическими словарями читайте в главе Морфология.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари.
Useragent	Useragent пользовательских браузеров, для которых будет применено данное правило. Администратор может добавить необходимые ему Useragent в разделе Useragent браузеров.
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET.
Рефереры	Список URL, в котором указаны рефереры для текущей страницы, таким образом правило сработает, если для данной страницы реферер совпадет со списком указанных URL. Данный функционал удобно использовать, чтобы, например, разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Важно! При настроенном инспектировании данных, передаваемых по протоколу TLS/SSL, и срабатывании правила контентной фильтрации Default allow, созданного по умолчанию, счётчик будет срабатывать только для правила инспектирования SSL. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Version: 7.0.1
Product: NGFW
Documentation:

С помощью раздела **Веб-безопасность** администратор может включить дополнительные параметры веб-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, например, сбоку на странице. NGFW решает эту проблему, выступая в качестве «баннерорезки».
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. Инжектируемый 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 данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.
- Включение журналирования поисковых запросов пользователей.
- Блокировка приложений социальных сетей. Социальные сети играют большую роль в нашей повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. NGFW 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. 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.

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

ПримечаниеЕсли не создано ни одного правила, то дополнительные функции веб-безопасности не применяются.

Чтобы создать правило контентной фильтрации необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Веб-безопасность** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Блокировать рекламу	Активирует блокировку рекламы. Нажав на Исключения , администратор может выбрать URL-список сайтов, для которых блокировать рекламу не требуется.
Инжектор	Позволяет вставить произвольный код во все веб-страницы. Для редактирования вставляемого кода необходимо нажать на кнопку Код инжектора .
Безопасный поиск	Принудительно включает функцию безопасного поиска.
История поиска	Активирует запись поисковых запросов пользователей в журнал.
Блокировать приложения социальных сетей	Блокирует приложения в популярных социальных сетях.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. 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.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства .
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари .
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Version: 7.0.1
Product: NGFW
Documentation:

Раздел позволяет администратору настроить инспекцию данных, передающихся с использованием следующих протоколов туннелирования:

- GRE** (Generic Routing Encapsulation) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты.
- GTP-U** (General Packet Radio Service (GPRS) Tunneling Protocol for User Data) — протокол, используемый для переноса пользовательских данных в базовой сети GPRS и между сетью радиодоступа и базовой сетью.
- Нешифрованный IPsec** (IPsec Null Encryption) — протокол туннелирования для передачи по IPsec-туннелю нешифрованного трафика.

NGFW позволяет производить инспектирование туннелей. При включении данной настройки, все туннели, попадающие под правила инспектирования, будут раскрываться; трафик, передаваемый внутри этих туннелей, будет обрабатываться с помощью правил МЭ, СОВ, L7. После фильтрации трафик будет завернут обратно в туннель и передан по оригинальному адресу назначения.

По умолчанию, в NGFW создана зона для инспектирования туннелей — **Tunnel inspection zone**. Данной зоне будут принадлежать все адреса источников и назначения инкапсулированных в туннель пакетов.

Примечание Все адреса источников и назначений инкапсулированных в туннель пакетов могут принадлежать только одной зоне.

Включить инспектирование и назначить другую зону для инспектируемых туннелей можно в разделе **UserGate → Настройки** модуль **Зона для инспектируемых туннелей**.

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.

Чтобы создать правило инспектирования туннелей, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование туннелей** и указать необходимые параметры; будут проверяться все туннели, подходящие под заданные условия.

Наименование	Описание
Включено	Включение/отключение правила инспектирования туннелей.
Название	Название правила инспектирования.
Описание	Описание правила инспектирования.
Действие	Действия правила инспектирования: - Инспектировать. - Не расшифровывать.
Инспектирование туннелей	Выбор типа туннеля, который необходимо инспектировать: - GRE. - GTP-U. - Нешифрованный IPsec.
Вставить	Место вставки создаваемого правила в списке правил — наверх, вниз или выше выбранного существующего правила.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.

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

Version: 7.0.1
Product: NGFW
Documentation:

С помощью данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу TLS/SSL, это в первую очередь HTTPS, а также почтовые протоколы SMTPS и POP3S. В UserGate используется известная технология man-in-the-middle (MITM), при которой контент расшифровывается на сервере, а затем анализируется.

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности. Дешифрование SMTPS и POP3S необходимо для блокирования спама.

С помощью правил данного раздела можно настроить инспектирование HTTPS только для определенных категорий, например, «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и при этом не расшифровывать другие категории, например, «Финансы», «Правительство» и т.п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе - **SNI** (Server Name Indication), а если SNI отсутствует, то поле **Subject Name** в сертификате сервера. Содержимое поля **Subject Alternative Name** игнорируется.

После дешифрования данные шифруются сертификатом, выписанным центром сертификации, указанным в разделе **Сертификаты**. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить сертификат центра сертификации в доверенные корневые сертификаты. Более подробно это описано в разделе [Приложение 1. Установка сертификата локального удостоверяющего центра](#).

Аналогично браузерам пользователя некоторые почтовые серверы и пользовательские почтовые программы не принимают почту, если сертификат был подменен. В этом случае необходимо произвести в почтовых программах настройки, отключающие проверку сертификатов, или добавить исключения для сертификата UserGate. Подробно о том, как это сделать, смотрите в документации на почтовое ПО.

ПримечаниеПравила 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.

ПримечаниеФлажок [Инvertировать](#) меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то SSL не перехватывается и не дешифруются, соответственно, контент, передаваемый по SSL, не фильтруется.

Чтобы создать правило инспектирования SSL, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование SSL** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Действие	Расшифровать. Не расшифровывать. Расшифровать и переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL. При выборе данного действия необходимо указать Профиль пересылки SSL (о настройке профилей пересылки читайте в разделе Профили пересылки SSL).
Профиль SSL	Выбор профиля SSL. Параметры, указанные в данном профиле, будут использованы как для установки SSL-соединения от браузера пользователя к серверу UserGate, так и при построении SSL-соединения от сервера UserGate к запрашиваемому веб-ресурсу. Подробнее о профилях SSL смотрите в главе Профили SSL .
Блокировать сайты с некорректными сертификатами	Позволяет блокировать доступ к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или не доверяемым центром сертификации.
Проверять по списку отозванных сертификатов	Проверять сертификат сайта в списке отозванных сертификатов (CRL) и блокировать, если он там найден.
Блокировать сертификаты с истекшим сроком действия	Блокировать сертификаты, срок действия которых истек.
Блокировать самоподписанные сертификаты	Блокировать самоподписанные сертификаты.
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any , Unknown , Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства .
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.

Наименование	Описание
Адрес назначения	Списки IP-адресов назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Сервис	Сервис, для которого необходимо дешифровать трафик. Может быть HTTPS, SMTPS, POP3S.
Категории	Списки категорий UserGate URL filtering 4.0.
Домены	Списки доменов. Доменные имена, для которых применяется данное 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/). Более подробно о работе со списками URL читайте в главе Списки URL .
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари .
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

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

Documentation: ☒
Product: NGFW
Version: 7.0.1

При помощи данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу SSH (Secure Shell). SSH также позволяет создавать зашифрованные туннели для практически любых сетевых протоколов.

Правила данного раздела могут inspectировать SSH-трафик для определённых пользователей и/или их групп, зон и адресов источников и получателей данных, а также типов сервисов, передаваемых через SSH-туннель. Имеется календарь для применения каждого правила в выбранные дни недели и время суток.

ПримечаниеПравила 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.

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

ПримечаниеЕсли не создано ни одного правила или все правила отключены, то SSH не перехватывается и не дешифруется, то есть передаваемые по SSH данные не inspectируются.

Чтобы включить возможность inspectирования контента SSH необходимо:

Наименование	Описание
Шаг 1. Разрешить сервис SSH-прокси на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис SSH-прокси для той зоны, со стороны которой будет инициирован трафик SSH.
Шаг 2. Создать необходимые правила inspectирования SSH.	Правило inspectирования SSH определяет критерии и действия, применяемые к трафику SSH.

Чтобы создать правило inspectирования SSH, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Inspectирование SSH** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Расшифровывать или не расшифровывать передаваемые данные.
Записывать в журнал правил	Регистрировать срабатывание правила в соответствующем журнале статистики (лог-файле).
Блокировать удаленный запуск shell	Не разрешать удаленному пользователю запуск shell (интерпретатора командной строки, оболочки).
Блокировать удаленное выполнение по SSH	Не разрешать удаленному пользователю выполнение любых команд и скриптов по SSH.
Редактировать команду SSH	Команда linux, которую требуется передать, в формате ssh user@host 'command' Например, ssh root@192.168.1.1 reboot
Блокировать SFTP	Блокировать соединение SFTP (Secure File Transfer Protocol).
Вставить	Место вставки создаваемого правила в списке правил - наверх, вниз или выше выбранного существующего правила.
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 читайте в главе Пользователи и устройства .
Источник	Зоны и/или списки IP-адресов источника трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса .
Адрес назначения	Списки IP-адресов назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса .
Сервис	Сервис, для которого необходимо дешифровать трафик. Поле обязательно для заполнения.
Время	Временной интервал, в течение которого правило активно. Можно добавить разнообразные периоды в разделе Календари .

Наименование	Описание
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики .
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Система обнаружения и предотвращения вторжений (COB), или Intrusion Detection and Prevention System (IDPS), позволяет распознавать вредоносную активность внутри сети или со стороны интернета. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз, а также предоставление отчетов. Выявление проблем безопасности осуществляется с помощью использования эвристических правил и анализа сигнатур известных атак. База данных правил и сигнатур предоставляется и обновляется разработчиками UserGate при наличии соответствующей лицензии. COB отслеживает и блокирует подобные атаки в режиме реального времени. Возможными мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал.

Для начала работы COB необходимо:

Наименование	Описание
Шаг 1. Создать необходимые профили COB.	Профиль COB — это набор сигнатур, релевантных для защиты определенных сервисов. Администратор может создать необходимое количество профилей COB для защиты различных сервисов. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты сервиса. Например, для защиты сервиса, работающего по протоколу TCP, не стоит добавлять сигнатуры, разработанные для протокола UDP. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.
Шаг 2. Создать требуемые правила COB.	Правила COB определяют действие COB для выбранного типа трафика, который будет проверяться модулем COB в соответствии с назначенными профилями COB.

Для настройки профилей COB необходимо создать профиль в разделе **Библиотеки → Профили COB** и затем добавить в него необходимые сигнатуры. Сигнатуры COB поставляются и постоянно обновляются UserGate при наличии соответствующей подписки. Каждая сигнатура имеет определенные поля:

Наименование	Описание
Сигнатура	Название сигнатуры.
Уровень угрозы	Риск сигнатуры по 5-бальной шкале.
Протокол	Протокол, для которого разработана данная сигнатура: • IP. • ICMP. • TCP. • UDP.
ОС	Операционная система, для которой разработана данная сигнатура.

Наименование	Описание
Категория	Категория сигнатуры — группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup. • attack_response — сигнатуры, определяющие ответы на известные сетевые атаки. • coinminer — скачивание, установка, деятельность известных майнеров. • dns — известные уязвимости DNS. • dos — сигнатуры известных Denial of services атак. • exploit — сигнатуры известных эксплоитов. • ftp — известные FTP-уязвимости. • imap — известные IMAP-уязвимости. • info — потенциальная утечка информации. • ldap — известные LDAP-уязвимости. • malware — скачивание, установка, деятельность известных malware. • misc — другие известные сигнатуры. • netbios — известные уязвимости протокола NETBIOS. • phishing — сигнатуры известных phishing атак. • pop3 — известные уязвимости протокола POP3. • rpc — известные уязвимости протокола RPC. • scada — известные уязвимости протокола SCADA. • scan — сигнатуры, определяющие попытки сканирования сети на известные приложения. • shellcode — сигнатуры, определяющие известные попытки запуска программных оболочек. • smtp — известные уязвимости протокола SMTP. • snmp — известные уязвимости протокола SNMP. • sql — известные уязвимости SQL. • telnet — известные попытки взлома по протоколу telnet. • tftp — известные уязвимости протокола TFTP. • user_agents — сигнатуры подозрительных Useragent. • voip — известные уязвимости протокола VoIP. • web_client — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps — сигнатуры, определяющие известные попытки взлома различных веб-приложений. • worm — сигнатуры, определяющие сетевую активность известных сетевых червей.
Класс	Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Поддерживаются следующие классы: • arbitrary-code-execution — попытка запуска произвольного кода. • attempted-admin — попытка получения административных привилегий. • attempted-dos — попытка совершения атаки Denial of Service. • attempted-recon — попытка атаки, направленной на утечку данных. • attempted-user — попытка получения пользовательских привилегий. • bad-unknown — потенциально плохой трафик. • command-and-control — попытка общения с C&C центром • default-login-attempt — попытка логина с именем/паролем по умолчанию. • denial-of-service — обнаружена атака Denial of Service. • exploit-kit — обнаружен exploit kit • misc-activity — прочая активность. • misc-attack — обнаружена атака. • shellcode-detect — обнаружен исполняемый код. • string-detect — обнаружена подозрительная строка. • suspicious-login — попытка логина с использованием подозрительного имени пользователя. • trojan-activity — обнаружен сетевой троян. • web-application-attack — обнаружена атака на веб-приложение.
Описание	Более подробное описание сигнатуры.

При добавлении сигнатур в профиль COB администратор может использовать гибкую возможность фильтрации сигнатур, например, выбрать только те сигнатуры, которые имеют очень высокий риск, протокол — TCP, категория — botcc, класс — все.

Правила COB определяют трафик, к которому применяется профиль COB и действие, которое модуль COB должен предпринять при срабатывании сигнатуры. При срабатывании сигнатуры доступна запись трафика. Настройка захвата пакетов производится в разделе **UserGate → Настройки → Настройка PCAP** . Загрузка и просмотр файлов PCAP доступны в журнале COB.

ПримечаниеПравила 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/Низе, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

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

ПримечаниеПравилами COB анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур в любом из направлений производится действие, настроенное в правилах.

ПримечаниеЕсли не создано ни одного правила, то COB ничего не анализирует и не защищает от угроз.

Для настройки правил COB необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → COB** и заполнить поля правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: • Разрешить — не блокировать трафик. • Журналировать — не блокировать и записать в журнал. • Запретить — блокировать и записать в журнал.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Сервис	Тип сервиса, например, HTTP, DNS или другие.
Профили	Список профилей COB, сигнатуры которых будут использованы в данном правиле COB. Профили COB задаются для правил с действиями Запретить и Журналировать. Для разрешающих правил задать профиль COB невозможно; такая реализация позволяет настроить исключения для определённого типа трафика.
Профили исключения	Список профилей COB, сигнатуры которых будут исключены из сигнатур, указанных в профилях в разделе Профили COB; могут быть использованы только в правилах с действием Запретить или Журналировать. Данная возможность позволяет использовать централизованно создаваемые профили сигнатур, например, Профиль UserGate, изменять содержимое которых администратор не может, но при этом исключить из этого профиля ряд сигнатур, которые избыточны или создают ложные срабатывания.

Сценарии

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

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря концепции SOAR (Security Orchestration, Automation and Response). NGFW реализует данную концепцию с помощью механизма сценариев. Сценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности, позволяя администратору настроить реакцию NGFW на определенные события, произошедшие за некое продолжительное время. Примером работы сценариев могут являться решение следующих задач:

- Заблокировать или ограничить пропускную способность на 30 минут пользователя, у которого за последние 10 минут было обнаружено 5 попыток использования приложения torrent.
- Заблокировать или ограничить пропускную способность пользователя или группы пользователей, указанной в правиле, при срабатывании одного из следующих триггеров — открытие пользователем сайтов, относящихся к группе категорий Threats, срабатывание COB сигнатур высокого риска для трафика данного пользователя, блокировка вируса в трафике данного пользователя.
- Заблокировать или ограничить пропускную способность пользователя, если он выбрал лимит трафика в 10 Гб за месяц.

ПримечаниеСценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.

Для начала работы со сценариями необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимые сценарии.	В разделе Политики безопасности → Сценарии создать необходимые сценарии.
Шаг 2. Указать созданные сценарии в правилах межсетевого экрана или в правилах пропускной способности.	Добавить созданный сценарий в правила межсетевого экрана или в правила пропускной способности. Более подробно о работе с правилами межсетевого экрана или пропускной способности смотрите раздел Политики сети .

При создании сценария необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает сценарий.
Название	Название сценария.
Описание	Описание сценария.
Применить для	Возможны варианты: • Одного пользователя — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий. • Всех пользователей — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в поле Пользователи/Группы правила.
Продолжительность	Время в минутах, в течении которого сценарий будет активным после его активации. Столько же будет работать правило межсетевого экрана или пропускной способности, в котором используется данный сценарий.
Условия	Задаются условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, то необходимо указать, сработают ли сценарий при совпадении одного или всех условий.
Условия срабатывания	Возможны следующие условия для использования в сценарии: • Категория URL — совпадения указанных категорий UserGate URLF в трафике пользователя. • Обнаружен вирус. • Приложение — обнаружено указанное приложение в трафике пользователя. • COB — сработка системы обнаружения вторжений. • Типы контента — обнаружены указанные типы контента в трафике пользователя. • Размер пакета — размер пакета в трафике пользователя превысил указанное значение. • Сессий с одного IP — количество сессий с одного IP-адреса превысило указанное значение. • Объем трафика — объем трафика пользователя превысил определенный лимит за указанную единицу времени. • Проверка состояния — проверка состояния какого-либо ресурса, который должен быть доступен с NGFW. Проверка может осуществляться с помощью команды istrip ring, запроса DNS или выполнения HTTP GET.

Product: NGFW
Documentation: 
Version: 7.0.1

Описание

NGFW позволяет передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. В данном случае NGFW будет выступать в роли ICAP-клиента.

NGFW поддерживает гибкие настройки при работе с ICAP-серверами, например, администратор может задать правила, согласно которым на ICAP-серверы будет направляться только выборочный трафик, или настроить работу с фермой ICAP-серверов.

Общие настройки

Для того, чтобы настроить работу NGFW с внешними серверами ICAP, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать ICAP-сервер.	В разделе Политики безопасности → ICAP-серверы нажать на кнопку Добавить и создать один или более ICAP-серверов.
Шаг 2. Создать правило балансировки на ICAP-серверы (опционально).	В случае, если требуется балансировка на ферму ICAP-серверов, создать в разделе Политики сети → Балансировка нагрузки балансировщик ICAP-серверов. В качестве серверов используются ICAP-серверы, созданные на предыдущем шаге.
Шаг 3. Создать правило ICAP.	В разделе Политики безопасности → Правила ICAP создать правило, которое будет задавать условия пересылки трафика на ICAP-серверы или фермы серверов. Важно! Правила ICAP применяются сверху вниз в списке правил. Срабатывает только первое правило, для которого совпали все условия, указанные в настройках правила.

Для создания ICAP-сервера в разделе **Политики безопасности → ICAP-серверы** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название ICAP-сервера.
Описание	Описание ICAP-сервера.
Адрес сервера	IP-адрес ICAP-сервера.
Порт	TCP-порт ICAP-сервера, значение по умолчанию 1344.
Максимальный размер сообщения	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
Период проверки доступности сервера ICAP	Устанавливает время в секундах, через которое NGFW посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.
Пропускать при ошибках	Если эта опция включена, то NGFW не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен (не отвечает на запрос OPTIONS).
Reqmod путь	• Включено — включает использование режима Reqmod. • Путь на сервере ICAP для работы в режиме Reqmod . Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима reqmod.
Respmod путь	• Включено — включает использование режима Respmod. • Путь на сервере ICAP для работы в режиме Respmod . Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима respmod.
Посылать имя пользователя	• Включено — включает отсылку имени пользователя на ICAP-сервер. • Кодировать в base64 — кодировать имя пользователя в base64, это может потребоваться, если имена пользователей содержат символы национальных алфавитов. • Название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — X-Authenticated-User.
Посылать IP-адрес	• Включено — включает отсылку IP-адреса пользователя на ICAP-сервер. • Название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Ip.
Посылать MAC-адрес	• Включено — включает отсылку MAC-адреса пользователя на ICAP-сервер. • Название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Mac.

Для создания правила балансировки на серверы ICAP в разделе **Политики сети → Балансировка нагрузки** необходимо выбрать **Добавить → Балансировщик ICAP** и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает правило.

Наименование	Описание
Название	Название правила.
Описание	Описание правила.
ICAP-серверы	Список серверов ICAP, на которые будет распределяться нагрузка, созданный на предыдущем шаге.

Для создания ICAP-правила необходимо нажать **Добавить** в разделе **Политики безопасности → ICAP-правила** и заполнить необходимые поля.

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может 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.
ICAP-серверы	ICAP-сервер или балансировщик серверов ICAP, куда NGFW будет пересылать запросы.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей.
Адрес назначения	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). 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.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента .
Категории	Списки категорий UserGate URL filtering.
URL	Списки URL.
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET. Если не используется SSL Inspection, то возможно применение метода CONNECT.
Сервис	Возможны варианты: - HTTP — веб-трафик. - SMTP — почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа. - POP3 — почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа. Важно! Перед использованием сервисов SMTP и POP3 в правилах ICAP необходимо создать правило защиты почтового трафика для данных сервисов. Подробнее о защите почтового трафика смотрите в разделе Защита почтового трафика .

Работа с несколькими серверами ICAP

UserGate поддерживает работу с несколькими серверами ICAP. В общем случае без балансировки данные передаются на ICAP сервера по порядку их перечисления, в случае если сервер ICAP не отвечает: поведение UserGate зависит от настройки **Действие** в правилах ICAP:

- Пропустить** - запрос не передаются на ICAP сервер
- Переслать** - запрос передается на сервер и ожидается ответ, если ответ не поступает, запрос отправляется следующему по списку ICAP серверу.

- **Переслать и игнорировать** - запрос передается на сервер, ответ не ожидается.

Балансировка нагрузки ICAP серверов

В UserGate возможна балансировка нагрузки на ICAP сервера. Реализовать это возможно двумя способами:

1. Балансировщик ICAP серверов:

Для настройки необходимо:

- Создать объекты Серверы ICAP в пункте меню **UserGate → Политики безопасности → ICAP серверы** как указано в примере ниже:

The dialog box is titled "Свойства ICAP-сервера". It has two tabs: "Общие" (selected) and "Данные". The "Общие" tab contains the following fields:

- Название: Сервер ICAP-1
- Описание: (empty text area)
- Адрес сервера: 10.10.10.10
- Порт: 1344
- Максимальный размер сообщения: 512 КБ (with a note: "Установите в 0, чтобы отключить.")
- Период проверки доступности сервера ICAP: 60 секунд
- Пропускать при ошибках: (unchecked checkbox)

At the bottom are buttons "Сохранить" and "Отмена".

- Создать "Балансировщик ICAP", для этого в пункте **UserGate → Политики сети → Балансировка нагрузки**, следует нажать кнопку **Добавить** и выбрать пункт **Добавить балансировщик ICAP**, далее установить чекбокс **Включено** и ввести название балансировщика:

The dialog box is titled "Балансировщик серверов ICAP". It has two tabs: "Общие" (selected) and "ICAP-серверы". The "Общие" tab contains the following fields:

- Включено: (checked checkbox)
- Название: Балансировщик ICAP - 1
- Описание: (empty text area)

At the bottom are buttons "Сохранить" and "Отмена".

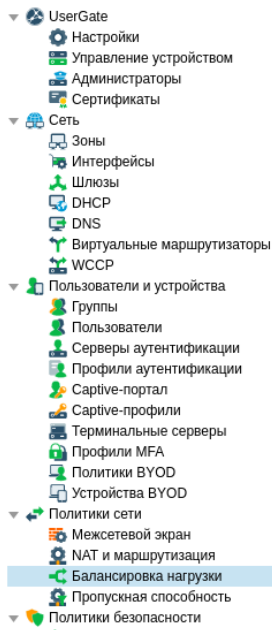
- Далее на вкладке **ICAP-серверы**, необходимо добавить ранее созданные ICAP серверы используя кнопку **Добавить**:

The dialog box is titled "Выбор ICAP-сервера". It has a search bar with the text "Фильтр:" and a "Поиск" button. Below the search bar is a list of servers:

Название
Сервер ICAP
Example ICAP server

At the bottom are buttons "Добавить" and "Заккрыть".

- И нажать кнопку **Сохранить**. В результате будет создан **Балансировщик ICAP**:



Балансировка нагрузки		
Добавить Редактировать Удалить Включить Отключить		
✓		
Тип балансировщика	Название	Профили
ICAP	Балансировщик ICAP	Сервер ICAP Example ICAP server

- После этого можно будет выбрать созданный балансировщик в настройке **ICAP-правил**.

Внимание! Данный способ балансировки не проверяет доступность ICAP серверов участвующих в балансировке. В случае недоступности ICAP серверов, поведение UserGate будет регламентироваться значением настройки Действие в ICAP правилах(см. выше).

Балансировка TCP/IP

Примечание Данный способ балансировки ICAP серверов является предпочтительным, хоть и более сложным, из-за наличия механизма проверки доступности и аварийного режима.

Второй вариант балансировки серверов ICAP возможен с использованием **Балансировщика TCP/IP**.

- В меню **UserGate → Политики сети → Балансировка нагрузки** нажимаем кнопку **Добавить**. Выбираем **Балансировщик TCP/IP**, указываем название, виртуальный IP адрес балансировщика (один из интерфейсов UserGate), порт реального сервера ICAP (по умолчанию 1344):

Свойства правила

Общие

Реальные серверы

Аварийный режим

Мониторинг

Включено:

☒

Название:

Балансировщик ICAP (TCP/IP)

Описание:

IP-адрес виртуального сервера:

10.0.0.1

Порт:

1344

Протокол:

TCP

Метод балансировки:

Weighted round robin

Сохранить

Отмена

- На вкладке **Реальные серверы** нужно указать IP адреса и порты реальных ICAP серверов, режим работы следует выбрать **Маскирование с подменой IP-источника (SNAT)** :

Свойства правила

Общие | Реальные серверы | Аварийный режим | Мониторинг

Добавить | Редактировать | Удалить

IP-адрес

Свойства сервера

IP-адрес: 10.10.10.10

Порт: 1344

Вес: 50

Режим: Маскарадинг с подменой IP-источника (SNAT)

Сохранить | Отмена

- На вкладке Аварийный режим, можно указать резервный сервер ICAP, который примет запросы в случае недоступности основных серверов ICAP. Пример настройки приведен ниже:

Свойства правила

Общие | Реальные серверы | Аварийный режим | Мониторинг

Включено: ☒

IP-адрес: 10.10.10.13

Порт:

Режим: Маскарадинг с подменой IP-источника (SNAT)

Сохранить | Отмена

- На вкладке мониторинг можно настроить параметры проверки доступности серверов, участвующих в балансировке, можно выбрать метод, интервал проверки и количество неудачных попыток, для признания узла недоступным. Пример настройки приведен ниже:

Свойства правила

Общие | Реальные серверы | Аварийный режим | Мониторинг

Режим: connect

Сервис: tcp

Запрос:

Ожидаемый ответ:

Интервал проверки: 60 (в секундах)

Время ожидания: 60 (в секундах)

Число неудачных попыток: 10

Сохранить | Отмена

Примечание Метод Connect проверки сервера позволяет проверить, что сервер отвечает по указанному порту. Это надежнее метода ping.

- Теперь можно создать ICAP сервер используя виртуальный IP адрес балансировщика TCP/IP и далее использовать этот сервер в правилах ICAP.

Защита почтового трафика

При наличии настроенной проверки почтового трафика, NGFW может проверять трафик по протоколам SMTP и POP3. IMAP не поддерживается, в том числе, и при настройке SSL инспектирования. Проверяться может и зашифрованный трафик этих протоколов.

Поддерживается 2 типа проверки:

- блокировка SMTP по наличию IP адреса сервера-отправителя в одной из баз DNSBL; наиболее эффективный метод быстро и с минимальными затратами ресурсов отсеять сообщения от очевидных и явных спамеров;
- маркировка сообщений по результатам проверки на спам; требует наличия также лицензии на модуль Mail security.

Внимание! Блокировка по результатам антиспам проверки НЕ рекомендуется. Рекомендуется принятие решения "спам/не спам" на стороне почтового сервера (или дополнительного антиспам приложения), где маркировка выставляемая NGFW была бы одним из критериев, с большим весом.

Посмотреть статистику работы антиспам модуля можно в дашборде, подключив соответствующие виджеты "Сводные показатели защиты почты" или "Графики защиты почты".

Важно! В журналах работа антиспама не отображается.

В настройках антиспам можно задать как белый, так и черный список IP адресов. Здесь речь идет именно об IP адресах, от которых сразу не будет приниматься соединение (для черных списков) без анализа каких-то дополнительных данных. В самих правилах можно добавлять списки адресов на вкладках envelope from / envelope to. Если в правиле будет стоять действие Блокировать, то это правило будет работать как черный список, если Пропустить — как белый.

В этих списках можно использовать символ * в значении "любой". То есть *@domain.com обозначает все адреса этого домена.

Раздел **Защита почтового трафика** позволяет настроить проверку транзитного почтового трафика на предмет наличия в нем спам-сообщений. Поддерживается работа с почтовыми протоколами POP3(S) и SMTP(S). Защита почтового трафика требует наличия соответствующего модуля в лицензии NGFW.

Как правило, необходимо защищать почтовый трафик, входящий из интернета на внутренние почтовые серверы компании, и, в некоторых случаях, защищать исходящий почтовый трафик от серверов или пользовательских компьютеров.

Для защиты почтового трафика, приходящего из интернета на внутренние почтовые серверы, необходимо:

Наименование	Описание
Шаг 1. Опубликовать почтовый сервер в сеть Интернет.	Смотрите раздел Правила DNAT . Рекомендуется создать отдельные правила DNAT для SMTP и POP3 протоколов, а не публиковать оба протокола в одном правиле. Обязательно укажите в качестве сервиса протокол SMTP, а не TCP.
Шаг 2. Включить поддержку сервисов SMTP(S) и POP3(S) в зоне, подключенной к сети Интернет.	Смотрите раздел Настройка зон .
Шаг 3. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для защиты почтового трафика в случаях, когда не требуется публиковать почтовый сервер, действия сводятся к следующим шагам:

Наименование	Описание
Шаг 1. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для настройки правил фильтрации почтового трафика необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Защита почтового трафика** и заполнить поля правила.

ПримечаниеПравила 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.

ПримечаниеЕсли не создано ни одного правила, то почтовый трафик не проверяется.

ПримечаниеДля срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Действие, применяемое к почтовому трафику при совпадении всех условий правила: • Пропустить — пропускает трафик без изменений. • Маркировать — маркирует почтовые сообщения специальным тэгом в теме письма или дополнительном поле. • Блокировать с ошибкой — блокирует письмо, при этом сообщает об ошибке доставки письма серверу SMTP для SMTP(S)-трафика или клиенту POP3 для POP3(S)-трафика. • Блокировать без ошибки — блокирует письмо без уведомления о блокировке.
Проверка	Метод проверки почтового трафика: • Проверка антиспамом UserGate — проверяет почтовый трафик на наличие спама. • DNSBL проверка — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам.
Заголовок	Поле, куда помещать тег маркировки.
Маркировка	Текст тега, который маркирует письмо.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). 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.
Пользователи	Пользователи или группы пользователей, к которым применяется данное правило.
Сервис	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило.
Envelope from	Почтовый адрес отправителя письма, указанный в поле Envelope from . Только для протокола SMTP.
Envelope to	Почтовый адрес адресата письма, указанный в поле Envelope to . Только для протокола SMTP.

Рекомендуемые настройки защиты от спама следующие.

Для протокола SMTP(S):

- Первое правило в списке — **блокировка с помощью DNSBL**. Рекомендуется оставить списки **Envelope from/Envelope to** пустыми. В этом случае DNSBL будет отбрасывать подключения SMTP-серверов, замеченных в распространении спама, еще на этапе коннекта. При наличии email адресатов в этих списках система будет вынуждена принимать сообщения целиком для анализа этих полей, что увеличит нагрузку на сервер и ухудшит производительность проверки почтового трафика.
- Второе правило — **маркировка** писем с помощью антиспама UserGate. Здесь можно использовать любые исключения, в том числе и по **Envelope from/Envelope to**.

Для протокола POP3(S):

- Действие — **Маркировать**.
- Проверка — **Антиспам UserGate**.

Настройки антиспама

Настройки BATV

BATV (Bounce Address Tag Validation) — технология, помогающая различать реальные возвраты писем от возвратов спама.

Подделка адресов отправителей (особенно тех, кто не использует SenderPolicyFramework и YahooDomainKeys для защиты от подделки своих адресов) широко применяется спамерами. Часть спама принимается MX'ами получателей, но при доставке на следующий сервер — relay может возвращаться отправителю. А так как адрес отправителя поддельный, реальные невинные владельцы адресов получают возврат спама, который не посылали. Также часть писем спам-рассылки маскируется под возвращаемые письма, поскольку некоторые антиспам-проверки предполагают, что возвращаемые письма не могут содержать спам-сообщения, чем и пользуются злоумышленники. Для отличия реальных возвращаемых писем от поддельных и применяется технология BATV.

Отключать прием возвращаемых писем нельзя, т.к. это нарушает связность сети (нормальные письма тоже иногда не доставляются и возвращаются), поэтому требуется как-то отличать нормальные возвраты от возвращаемого чужого спама. Тогда и была предложена технология BATV. Использование BATV может быть полезно в тех системах, где контентные фильтры спама не справляются с детектированием спама в возвращаемых письмах.

Может быть включена, либо выключена. Других настроек не предполагается.

Серверы DNSBL

DNSBL проверка — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам. DNSBL или спам-база — это черный список доменных имен и ip-адресов, замеченных в распространении спам сообщений.

Внимание!Появление в этом списке того или иного сервера, не является однозначным признаком принадлежности писем с этого сервера к спам-рассылкам. Частота ложных срабатываний в этой технологии зависит от используемых списков DNSBL и определяется индивидуально. В любом случае, появление сервера в списках DNSBL должно квалифицироваться как дополнительный, но не основной признак спам-рассылки.

В сети существуют десятки различных DNSBL, каждый из которых использует свои собственные критерии для добавления и исключения из своего списка IP адреса или домена. Большинство спам-фильтров используют различные DNSBL для проверки того, чтобы входящие электронные письма не отправлялись с сайтов, доменные имена которых занесены в черный список. Как правило, DNSBL являются первой линией защиты от спама. Например, в список серверов добавляются адреса серверов DNSBL: cbl.abuseat.org, zen.spamhaus.org и т.д. Белый и черный список добавляет или убирает определенные адреса из этой проверки.

Белый список DNSBL

Список серверов исключенных из DNSBL проверки.

Черный список DNSBL

Список запрещенных серверов в дополнение к тем, что есть списках DNSBL.

Documentation: ☒
Product: NGFW
Version: 7.0.1

NGFW позволяет гранулировано настроить параметры защиты сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP). Грубая настройка производится в свойствах зон (смотрите раздел [Настройка зон](#)), более точная настройка производится в данном разделе. Используя правила защиты DoS, администратор может указать специфические настройки защиты от DoS атак для определенного сервиса, протокола, приложения и т.п. Чтобы создать правила защиты DoS администратору необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профили DoS защиты.	В разделе Политики безопасности → Профили DoS нажать на кнопку Добавить и создать один или более профилей DoS защиты.
Шаг 2. Создать правила защиты DoS.	В разделе Политики безопасности → Правила защиты DoS создайте правила, используя профили защиты, созданные на предыдущем шаге.

Настройка профиля защиты DoS подобна настройке защиты от DoS на зонах NGFW. При создании профиля необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Агрегировать	Данная настройка регулирует, будет ли NGFW суммировать количество пакетов, проходящих в секунду, для всех IP-адресов источника трафика, или будет производить подсчет индивидуально для каждого IP-адреса. В случае активации данной настройки необходимо устанавливать достаточно высокие значения количества пакетов/сек в настройках закладки Защита DoS и в закладке Защита ресурсов .
Защита DoS	Данная настройка позволяет указать параметры защиты от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: Порог уведомления — при превышении количества запросов над указанным значением происходит запись события в системный журнал. Порог отбрасывания пакетов — при превышении количества запросов над указанным значением NGFW начинает отбрасывать пакеты, и записывает данное событие в системный журнал.
Защита ресурсов	Данная настройка позволяет ограничить количество сессий, которые будут разрешены для защищаемого ресурса, например, опубликованного сервера: Включено: включает ограничение количества сессий. Ограничить число сессий: задается число сессий.

Чтобы создать правило защиты DoS, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Правила защиты DoS** и указать необходимые параметры.

ПримечаниеПравила 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.

ПримечаниеЧекбокс **Инvertировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Запретить — безусловно блокирует трафик подобно действию правил Межсетевого экрана. Разрешить — разрешает трафик, защита от DoS не применяется. Может быть использовано для создания исключений. Защитить — применить профиль защиты от DoS атак.
Профиль DoS	В случае, если выбрано действие Защитить , необходимо указать профиль защиты DoS. Если при использовании профиля DoS с защитой ресурсов не использовать дополнительные условия, например адрес назначения, то будут учитываться все транзитные соединения.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии . Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Записывать в журнал правил	Записывает в журнал трафика информацию о трафике при срабатывании правила. Возможны варианты: Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идеуентификации пользователей читайте в главе Пользователи и устройства.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом "" в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. 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.
Сервис	Тип сервиса, например, HTTP или HTTPS.
Время	Интервалы времени, когда правило активно.

