

Table of Contents

Table of Contents	1
Настройка раздела Политики безопасности	2
Настройка фильтрации контента	3
Настройка веб-безопасности	6
Настройка правил инспектирования туннелей	8
Настройка инспектирования SSL	10
Настройка инспектирования SSH	13
Настройка COB	15
Настройка сценариев	17
Настройка правил защиты почтового трафика	22
Настройка правил ICAP	24
Настройка ICAP-серверов	26
Настройка правил защиты DoS	28
Настройка профилей DoS	30

Настройка фильтрации контента

Product: UserGate NGFW

Version: 7.0.1

Documentation: 

Настройка правил контентной фильтрации производится на уровне **security-policy content-filtering**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Параметр	Описание
PASS DENY WARNING	Действие правила контентной фильтрации: • PASS — разрешить посещение веб-страницы. • DENY — блокировать веб-страницу. • WARNING — предупредить пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила контентной фильтрации. Для указания названия правила: name("Content filtering rule example") .
desc	Описание правила. Например: desc("Content filtering rule example set via CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
virus_usergate	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием Запретить ; возможны значения: • virus_usergate(yes) или virus_usergate(true) — использовать проверку потоковым антивирусом UserGate. • virus_usergate(no) или virus_usergate(false) — не использовать проверку потоковым антивирусом UserGate.
Страница блокировки	Выбор страницы блокировки; если страница не указана, то используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например, DENY("Blockpage (RU)") . Подробнее о настройке страниц блокировки читайте в разделе Настройка шаблонов страниц . Можно использовать внешнюю страницу, задав внешний URL: redirect(302, "http://www.example.com") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило контентной фильтрации (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователей (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".

Параметр	Описание
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка типов контента: response.header.Content-Type = lib.mime(); в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.
morphology	Список баз словарей морфологии, по которым будут проверяться веб-страницы. Для задания списка баз словарей морфологии: morphology = lib.morphology(); в скобках необходимо указать название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка морфологии и.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent(); в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET.
request.header.Referer	Список URL, в котором указаны рефереры для текущей страницы, или категория URL, к которой относится реферер. Чтобы указать список или категорию URL: request.header.Referer = lib.url() (в скобках необходимо указать название списка) или request.header.Referer = "URL category" Подробнее о настройке списков URL через CLI читайте в разделе Настройка списков URL; о категориях URL — Настройка категорий URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка веб-безопасности

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка веб-безопасности производится на уровне **security-policy safe-browsing**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать следующие данные:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила веб-безопасности. Например: name("Safe browsing rule example") .
desc	Описание правила, например, desc("Safe browsing rule example set via CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование
enable_adblock	Блокировка рекламы • enable_adblock(yes) или enable_adblock(true). • enable_adblock(no) или enable_adblock(false).
url_list_exclusions	Список сайтов, для которых блокировать рекламу не требуется: url_list_exclusions("URL list name") . О создании и настройке списков URL с использованием CLI читайте в разделе Настройка списков URL .
enable_injector	Инжектирование кода в веб страницы: • enable_injector(yes) или enable_injector(true). • enable_injector(no) или enable_injector(false).
custom_injector	Код инжектора.
safe_search	Использование функции безопасного поиска: • safe_search(yes) или safe_search(true). • safe_search(no) или safe_search(false).
search_history_logging	Журналирование поисковых запросов пользователей: • search_history_logging(no) или search_history_logging(false) — отключить журналирование поисковых запросов пользователей. Если при создании правила search_history_logging не указано, функция журналирования отключена. • search_history_logging(yes) или search_history_logging(true) — включить журналирование поисковых запросов пользователей.

Параметр	Описание
social_sites_block	Блокировка приложений социальных сетей: • social_sites_block(yes) или social_sites_block(true). • social_sites_block(no) или social_sites_block(false).
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.
user	Пользователи и группы пользователей, для которых применяется правило веб-безопасности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка правил инспектирования туннелей

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил инспектирования туннелей производится на уровне **security-policy tunnel-inspection**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо задать следующие параметры:

Параметр	Описание
OK PASS	Действие правила инспектирования туннелей: • OK — Инспектировать. • PASS — Не расшифровывать
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования туннелей. Например: name("Tunnel inspection rule example") .
desc	Описание правила. Например: desc("Tunnel inspection rule example configured via CLI") .
service	Тип туннеля: • service = gre: инспектирование туннелей GRE. • service = gtpu: инспектирование туннелей GTP-U. • service = ipsec_null: инспектирование нешифрованных IPsec-туннелей
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика, например, dst.zone = "Tunnel inspection zone" . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Настройка инспектирования SSL

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил инспектирования SSL производится на уровне **security-policy ssl-inspection**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Параметр	Описание
OK PASS	Действие правила инспектирования SSL: • OK — Расшифровать. • PASS — Не расшифровывать • OK ... forward — Расшифровать и переслать; forward указывается среди свойств правила. При настройке правила с действием Расшифровать и переслать необходимо указать профиль пересылки SSL. Подробнее о создании и настройке с использованием CLI профилей пересылки читайте в разделе Настройка профилей пересылки SSL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования SSL. Для указания названия правила: name("SSL inspection rule example") .
desc	Описание правила. Например: desc("SSL inspection rule example configured in CLI") .
ssl_forward_profile	Профиль пересылки SSL; профиль необходимо указать при настройке правила инспектирования SSL с действием Расшифровать и переслать. Указывается в формате: ssl_forward_profile("SSL forward profile example") .
ssl_profile	Профиль SSL; указывается: ssl_profile("Default SSL profile") . Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
block_invalid_cert	Блокирование доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат отозван, выписан на другое доменное имя или недоверенным центром сертификации, срок действия сертификата истёк. Доступно в правилах с действием Расшифровать : • block_invalid_cert(yes) или block_invalid_cert(true) — включение блокировки. • block_invalid_cert(no) или block_invalid_cert(false) — отключение блокировки.
check_revoc_cert	Проверка сертификата сайта в списке отозванных сертификатов (CRL) и блокирование доступа, если он там найден. Доступно в правилах с действием Расшифровать : • check_revoc_cert(yes) или check_revoc_cert(true) — включение проверки сертификата. • check_revoc_cert(no) или check_revoc_cert(false) — отключение проверки сертификата.

Параметр	Описание
block_expired_cert	Блокирование сертификатов с истёкшим сроком действия. Доступно в правилах с действием Расшифровать: • block_expired_cert(yes) или block_expired_cert(true) — включить блокировку сертификатов с истёкшим сроком действия. • block_expired_cert(no) или block_expired_cert(false) — отключить блокировку сертификатов с истёкшим сроком действия.
block_self_signed_cert	Блокирование самоподписанных сертификатов. Доступно в правилах с действием Расшифровать: • block_self_signed_cert(yes) или block_self_signed_cert(true) — включить блокировку самоподписанных сертификатов. • block_self_signed_cert(no) или block_self_signed_cert(false) — отключить блокировку самоподписанных сертификатов.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSL (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.
service	Тип сервиса: HTTPS, SMTPTS или POP3S. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).

Параметр	Описание
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки доменных имён, для которых применяется правило инспектирования SSL. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена типа www.example.com, а не http://www.example.com/home/. Для указания списка доменов: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки читайте в разделе Настройка списков URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка инспектирования SSH

Documentation: 

Product: UserGate NGFW

Version: 7.0.1

Настройка правил SSH-инспектирования производится на уровне **security-policy ssh-inspection**. О структуре команд читайте подробнее в разделе [Настройка правил с использованием UPL](#).

Далее представлены параметры правил инспектирования SSH.

Параметр	Описание
OK PASS	Действие правила инспектирования SSH: • OK — Расшифровать. • PASS — Не расшифровывать
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования SSH. Для указания названия правила: name("SSH inspection rule example") .
desc	Описание правила. Например: desc("SSH inspection rule example configured in CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
block_ssh_shell	Блокирование удалённого запуска shell (интерпретатора командной строки, оболочки). Доступно в правилах с действием Расшифровать : • block_ssh_shell(yes) или block_ssh_shell(true) — включить блокировку. • block_ssh_shell(no) или block_ssh_shell(false) -отключить блокировку.
block_ssh_exec	Блокирование удалённого выполнения по SSH. Доступно в правилах с действием Расшифровать : • block_ssh_exec(yes) или block_ssh_exec(true) — включить блокировку. • block_ssh_exec(no) или block_ssh_exec(false) — отключить блокировку.
ssh_command	Команда linux, которую требуется передать, в формате ssh user@host 'command' Например: ssh_command("ssh root@192.168.1.1 reboot") . Редактирование команды SSH доступно в правилах с действием Расшифровать .
block_sftp	Блокирование соединения SFTP (Secure File Transfer Protocol). Доступно в правилах с действием Расшифровать : • block_sftp(yes) или block_sftp(true) — включить блокировку соединения. • block_sftp(no) или block_sftp(false) — отключить блокировку соединения.

Параметр	Описание
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSH (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей.

Настройка COB

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка системы обнаружения и предотвращения вторжений производится на уровне **security-policy intrusion-prevention**.

Правила COB настраиваются на уровне **security-policy intrusion-prevention idps-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Доступны параметры:

Параметр	Описание
PASS WARNING DENY	Действие правила COB: • PASS — не блокировать трафик. • WARNING — не блокировать трафик и записать информацию в журнал. • DENY — блокировать трафик и записать информацию в журнал.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила системы обнаружения и предотвращения вторжений. Например: name("IDPS rule example") .
desc	Описание правила. Например: desc("Intrusion prevention rule example set via CLI") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL . Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: src.ip = 02:00:00:00:00:00 .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, например, Untrusted: dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
idps_profiles	Профиля COV, которые будут использованы в данном правиле: idps_profiles("IDPS profile example"). Профили COV задаются для правил с действиями Сбросить и Журналировать. Для разрешающих правил задать профиль COV невозможно; такая реализация позволяет настроить исключения для определённого типа трафика.
idps-profiles_exclusions	Список профилей COV, сигнатуры которых будут исключены из сигнатур, указанных в профилях COV; могут быть использованы только в правилах с действием Сбросить или Журналировать: idps_profiles_exclusions("Example of IDPS profile with exclusions"). Данная возможность позволяет использовать централизованно создаваемые профили сигнатур, изменять содержимое которых администратор не может, но при этом исключить из этого профиля ряд сигнатур, которые избыточны или создают ложные срабатывания.

Только в CLI доступна настройка режима умного сканирования (сканирование только первых байт каждой сессии). Настройка режима производится на уровне **security-policy intrusion-prevention settings**. Для настройки используется команда:

```
Admin@UGOS# set security-policy intrusion-prevention settings
```

Доступны параметры:

Параметр	Описание
intelligent-mode	Включение/отключение режима умного сканирования: • on. • off.
intelligent-limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Для просмотра состояния режима:

```
Admin@UGOS# show security-policy intrusion-prevention settings
```

По умолчанию режим умного сканирования включен; проверяются первые 200 КБ каждой сессии.

Настройка сценариев

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка сценариев происходит на уровне **security-policy scenarios** с использованием UPL (подробнее об UserGate Policy Language читайте в разделе [Настройка правил с использованием UPL](#)).

Для задания условий сценариев и их объединения используются определения (definitions). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слэша (как при использовании многострочного ввода).

Для создания/изменения условий сценариев используется функция **def scenario_cond**, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
scenario_conditions
end
```

Параметры, используемые для задания разных типов условий, будут рассмотрены в следующих разделах.

Далее, после указания условий, указываются общие свойства сценария, представленные в таблице ниже:

Наименование	Описание
OK	Действие для создания сценария.
scenario_cond	Пользовательское имя определения, содержащего список условий сценария: scenario_cond = condition_example .
enabled	Включить/отключить использование сценария: • enabled(true); • enabled(false).
name	Задать имя сценария: name("Example scenario name") .
desc	Задать описание сценария: desc("Description for scenario created as an example") .
trigger	Применение: • trigger(one_user) — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; • trigger(all_users) — при срабатывании сценария, правило, в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила.
duration	Задать период активности сценария; указывается в минутах.
operation_mode	Задать режим активации сценария: • operation_mode(all) — сценарий работает, если выполнятся все условия; • operation_mode(any) — сценарий работает, если выполнится хотя бы одно из условий.

Примечание При обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием **Объём трафика**. Сценарий будет применён ко всем пользователям в течение минуты; ограничение объёма трафика: 1 ГБ/день:

```
Admin@UGOS# create security-policy scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(2GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
```

...

Для изменения, например, объема трафика:

```
Admin@UGOS# set security-policy scenarios 3 upl-rule \  
...def scenario_cond scenario_cond_test  
...traffic_limit(2GB) \  
...period(day) \  
...scond_type(traffic)  
...end  
...OK \  
...scenario_cond = scenario_cond_test
```

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
category	Категории или группы категорий сайтов: <code>category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME)</code> .
scond_type	Тип условия: <code>scond_type(url_category)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(virus_detection)</code> .

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
application	Категории приложений или группы приложений: <code>application = lib.applicationgroup(APP_GROUP)</code> или <code>application = lib.applicationgroup(all)</code>; <code>application = lib.category(APPS_CATEGORY_NAME)</code>.
scond_type	Тип условия: <code>scond_type(app)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа COB

Параметры условия типа **COB**:

Наименование	Описание

Наименование	Описание
ips_tl	Уровень угрозы: • ips_tl(very_low) - очень низкий; • ips_tl(low) - низкий; • ips_tl(medium) - средний; • ips_tl(high) - высокий; • ips_tl(very_high) - очень высокий.
scond_type	Тип условия: scond_type(ips) .

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
response.header.Content-Type	Тип контента: response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST) .
scond_type	Тип условия: scond_type(mime_type) .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Условие типа Размер пакета

Для создания и настройки условия типа **Размер пакета** используются следующие параметры:

Наименование	Описание
packet_size	Размер пакета, при превышении которого выполняется условие; указывается следующим образом: • packet_size(1) - размер пакета 1 байт; • packet_size(1KB) - размер пакета 1 Кбайт; • packet_size(1MB) - размер пакета 1 Мбайт; • packet_size(1GB) - размер пакета 1 Гбайт.
scond_type	Тип условия: scond_type(net_packet_size) .

Условие типа Сессий с одного IP

При настройке условия типа **Сессий с одного IP** используются:

Наименование	Описание
scond_type	Тип условия: scond_type(sessions_per_ip) .
sessions_limit	Максимальное количество сессий, разрешённых с одного IP-адреса: sessions_limit() .

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(traffic) .
traffic_limit	Ограничение объёма трафика: • traffic_limit(1) - 1 байт трафика; • traffic_limit(1KB) - 1 Кбайт трафика; • traffic_limit(1MB) - 1 Мбайт трафика; • traffic_limit(1GB) - 1 Гбайт трафика.
period	Период времени: • period(minute) - минута; • period(hour) - час; • period(day) - день; • period(week) - неделя; • period(month) - месяц.

Условие типа Проверка состояния

Для настройки условия типа **Проверка состояния** предназначены параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(health_check) .
health_check_method	Метод проверки: • health_check_method(ping) - ping; • health_check_method(dns) - DNS-запрос; • health_check_method(get) - HTTP-метод GET.
url.address	Адрес, на который будут выполняться ping и DNS-запрос: url.address = "1.1.1.1" .
url.domain	FQDN для проверки состояния путём выполнения DNS-запроса или URL для метода HTTP GET: url.domain = "example.ru" .
gateway	Название используемого шлюза: gateway() . Важно! Шлюз должен быть предварительно создан.
health_result	Результат выполнения проверки: • health_result(positive) - положительный; • health_result(negative) - отрицательный.
health_request_timeout	Тайм-аут подключения (в секундах): health_request_timeout() .
health_answer_timeout	Время ожидания ответа на запрос HTTP GET (в секундах): health_answer_timeout() .

Наименование	Описание
health_type_request	Тип DNS-запроса: • health_type_request(a). • health_type_request(aaaa). • health_type_request(cname). • health_type_request(ns). • health_type_request(ptr).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval().
max_event_count	Количество срабатываний: max_event_count().

Настройка правил защиты почтового трафика

Product: UserGate NGFW

Version: 7.0.1

Documentation: 

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать:

Параметр	Описание
PASS WARNING DENY("with error") DENY	Действие правила защиты почтового трафика: • PASS — Пропустить — пропустить трафик без изменения. • WARNING — Маркировать — маркировать почтовые сообщения специальным тэгом в теме письма или дополнительном поле. • DENY("with error") — Блокировать с ошибкой — блокировать письмо и сообщать об ошибке доставки письма серверу SMTP (для SMTP(S)-трафика) или клиенту (для POP3(S)-трафика). • DENY — Блокировать без ошибки — блокировать письмо без уведомления о блокировке.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила защиты почтового трафика. Например: name("Mail security rule example") .
desc	Описание правила. Например: desc("Mail security rule example configured in CLI") .
antispam_usergate	Проверка почтового трафика антиспамом UserGate (задаётся для правил с действием Маркировать , Блокировать с ошибкой или Блокировать без ошибки): • antispam_usergate(yes) или antispam_usergate(true) — включить проверку. • antispam_usergate(no) или antispam_usergate(false) — отключить проверку.
dnsbl	Антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику в правилах с действием Маркировать , Блокировать с ошибкой или Блокировать без ошибки : • dnsbl(yes) или dnsbl(true) — использовать антиспам-проверку. • dnsbl(no) или dnsbl(false) — отключить использование антиспам-проверки. 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 и вирусы.
mark_hdr	Заголовок. Поле куда помещать тег маркировки; задаётся для правил с действием Маркировать : mark_hdr(Subject) .
mark	Текст тега, который маркирует письмо; задаётся для правил с действием Маркировать , например, mark("Text for marking emails") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты почтового трафика (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
envelope_from	Почтовый адрес отправителя письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_from = "Sender email group". Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.
envelop_to	Почтовый адрес адресата письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_to = "Receiver email group". Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.

Настройка правил ICAP

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать:

Параметр	Описание
PASS OK	Действие правила ICAP: • PASS — Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • OK — Переслать — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера (стандартный режим работы большинства ICAP-серверов). • OK ... ignore — Переслать и игнорировать — переслать данные ICAP-сервер и игнорировать ответ от ICAP-сервера (вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика); ignore указывается среди свойств правила.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила ICAP. Для указания названия правила: name("ICAP rule example") .
desc	Описание правила. Например: desc("ICAP rule example set via CLI") .
profile	ICAP-серверы, куда UserGate будет пересылать запросы; указывается в формате: profile("Example ICAP server") . О настройке серверов ICAP через CLI читайте в разделе Настройка ICAP-серверов .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
user	Пользователи и группы пользователей, для которых применяется правило ICAP (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка: <pre>response.header.Content-Type = lib.mime();</pre> в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.
category	Список категорий или категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET.
service	Тип сервиса: HTTP, SMTP или POP3. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).

Настройка ICAP-серверов

Documentation: 

Product: UserGate NGFW

Version: 7.0.1

Настройка ICAP-серверов производится на уровне **security-policy icap-server**.

Структура команды для создания ICAP-сервера:

```
Admin@UGOS# create security-policy icap-server
```

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя ICAP-сервера.
description	Задать описание ICAP-сервера.
ip	Задать IP-адрес ICAP-сервера.
port	Задать TCP-порт ICAP-сервера; значение по умолчанию: 1344.
max-msg-size	Определить максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
check-icap	Задать период проверки доступности сервера ICAP.
bypass	Если эта опция включена, то UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен.
reqmod-service	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Reqmod.
respmod-service	Использовать режим Respmode: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Respmode.
user-header	Установить отсылку имени пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. • off — не отсылать имя пользователя на ICAP-сервер.
user-encode	Установить кодировку имени пользователя в Base64: • on. • off.
ip-header	Установить отсылку IP-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. • off — не отсылать IP-адрес пользователя на ICAP-сервер.

Параметр	Описание
mac-header	Установить отсылку MAC-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. • off — не отсылать MAC-адрес пользователя на ICAP-сервер.

Структура команды для обновления существующего ICAP-сервера:

```
Admin@UGOS# set security-policy icap-server <server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового ICAP-сервера.

Структура команды для удаления ICAP-сервера:

```
Admin@UGOS# delete security-policy icap-server <server-name>
```

Структура команды для отображения информации об ICAP-сервере:

```
Admin@UGOS# show security-policy icap-server <server-name>
```

Настройка правил защиты DoS

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил защиты DoS производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Параметр	Описание
PASS WARNING DENY	Действие правила защиты DoS: • PASS — разрешить трафик; защита от DoS атак не применяется. • WARNING — применить профиль защиты от DoS атак. • DENY — безусловно блокировать трафик.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила защиты DoS. Например: name("DoS rule example") .
desc	Описание правила. Например: desc("DoS rule example configured in CLI") .
profile	Профиль защиты DoS. Выбор профиля доступен только для правил с действием Защитить (WARNING) . Для указания профиля: profile("DoS profile example") . О создании и настройке профилей защиты читайте в разделе Настройка профилей DoS .
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .

Параметр	Описание
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты DoS (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: src.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка профилей DoS

Documentation: 

Product: UserGate NGFW

Version: 7.0.1

Настройка профилей DoS производится на уровне **security-policy dos-profile**.

Структура команды для создания профиля DoS:

```
Admin@UGOS# create security-policy dos-profile
```

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя профиля.
description	Задать описание профиля.
aggregate	Установить суммирование количества пакетов, проходящих в секунду для всех IP адресов или подсчёт индивидуально для каждого IP-адреса.
dos-protection-syn	Настройка защиты от сетевого флуда для протокола TCP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
dos-protection-udp	Настройка защиты от сетевого флуда для протокола UDP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
dos-protection-icmp	Настройка защиты от сетевого флуда для протокола ICMP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
max-sessions	Установить ограничение количества сессий: • <num> — задать число сессий. • off — отключить ограничение числа сессий.

Структура команды для обновления существующих профилей DoS:

```
Admin@UGOS# set security-policy dos-profile <profile-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды добавления нового профиля DoS.

Структура команды для удаления профиля:

```
Admin@UGOS# delete security-policy dos-profile <profile-name>
```

Структура команды для отображения информации о профиле DoS:

```
Admin@UGOS# show security-policy dos-profile <profile-name>
```

