

Table of Contents

Table of Contents	1
Настройка раздела Политики безопасности	2
Настройка фильтрации контента	3
Настройка веб-безопасности	7
Настройка правил инспектирования туннелей	10
Настройка инспектирования SSL	12
Настройка инспектирования SSH	15
Настройка COB	18
Настройка защиты почтового трафика	19
Настройка правил ICAP	23
Настройка ICAP-серверов	26
Настройка профилей DoS	28
Настройка правил защиты DoS	29

Настройка фильтрации контента

Documentation: ☒
Version: 7.x
Product: NGFW

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

Для создания правила контентной фильтрации используется команда:

Admin@nodename# create security-policy content-filtering <position> upl-rule

Параметры правил контентной фильтрации:

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") .

Параметр	Описание
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.
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). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
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.

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 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.
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.

Для редактирования правил контентной фильтрации используется команда:

```
Admin@nodename# set security-policy content-filtering <position> upl-rule
```

Для просмотра всех созданных правил контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering
```

Для просмотра определенного правила контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering <position>
```

Пример создания правила контентной фильтрации с использованием UPL:

```
Admin@nodename# create security-policy content-filtering 1 upl-rule PASS \
...src.zone = Trusted \
...url = lib.url("Test URL list") \
...user = known \
...rule_log(yes) \
...name("Test content-filtering rule") \
...desc("Test content-filtering rule description") \
...enabled(true)
...
Admin@nodename# show security-policy content-filtering 1
% ----- 1 --- "Content Rules" -----
PASS \
    user = known \
    url = lib.url("Test URL list") \
    src.zone = Trusted \
    desc("Test content-filtering rule description") \
    rule_log(yes) \
    enabled(true) \
    id("96b2ee34-528a-4b06-8726-69711ba639ba") \
    name("Test content-filtering rule")
```

Для удаления существующего правила контентной фильтрации используется команда:

```
Admin@nodename# delete security-policy content-filtering <position>
```

Настройка веб-безопасности

Version: 7.x

Product: NGFW

Documentation: 

Настройка веб-безопасности производится на уровне **security-policy safe-browsing**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила веб-безопасности используется команда:

```
Admin@nodename# create security-policy safe-browsing <position> upl-rule
```

Параметры правил веб-безопасности:

Параметр	Описание
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). Примеры добавления пользователей в правило: <pre>user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
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.

Для редактирования правил веб-безопасности используется команда:

```
Admin@nodename# set security-policy safe-browsing <position> upl-rule
```

Для просмотра всех созданных правил веб-безопасности используется команда:

```
Admin@nodename# show security-policy safe-browsing
```

Для просмотра определенного правила веб-безопасности используется команда:

```
Admin@nodename# show security-policy safe-browsing <position>
```

Пример создания правила веб-безопасности с помощью UPL:

```
Admin@nodename# create security-policy safe-browsing 1 upl-rule PASS \
...user = known \
...src.zone = Trusted \
...enable_adblock(yes) \
...safe_search(yes) \
...rule_log(yes) \
...name("Test safe browsing rule") \
...desc("Test safe browsing rule description") \
...enabled(true)
...
Admin@nodename# show security-policy safe-browsing 1
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  rule_log(yes) \
  enable_adblock(yes) \
  safe_search(yes) \
```

```
desc("Test safe browsing rule description") \  
enabled(true) \  
id("406a2753-750e-4830-82a8-583043e72359") \  
name("Test safe browsing rule")
```

Для удаления правила веб-безопасности используется команда:

```
Admin@nodename# delete security-policy safe-browsing <position>
```

Настройка правил инспектирования туннелей

Version: 7.x

Product: NGFW

Documentation: 

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

Для создания правила инспектирования туннелей используется команда:

```
Admin@nodename# create security-policy tunnel-inspection <position> upl-rule
```

Параметры правил инспектирования туннелей:

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.

Для редактирования правил инспектирования туннелей используется команда:

```
Admin@nodename# set security-policy tunnel-inspection <position> upl-rule
```

Для просмотра всех созданных правил инспектирования туннелей используется команда:

```
Admin@nodename# show security-policy tunnel-inspection
```

Для просмотра определенного правила инспектирования туннелей используется команда:

```
Admin@nodename# show security-policy tunnel-inspection <position>
```

Пример создания правила инспектирования туннелей:

```
Admin@nodename# create security-policy tunnel-inspection 1 upl-rule PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...service = ipsec_null \
...name("Test tunnel-inspection rule") \
...desc("Test tunnel-inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy tunnel-inspection 1
% ----- 1 -----
PASS \
  src.zone = Untrusted \
  dst.zone = Trusted \
  service = ipsec_null \
  desc("Test tunnel-inspection rule description") \
  enabled(true) \
  id("051cf677-3d36-4d5c-968f-73c3421c2b28") \
  name("Test tunnel-inspection rule")
```

Для удаления правила инспектирования туннелей используется команда:

```
Admin@nodename# delete security-policy tunnel-inspection <position>
```

Настройка инспектирования SSL

Version: 7.x

Product: NGFW

Documentation: 

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

Для создания правила инспектирования SSL используется команда:

```
Admin@nodename# create security-policy ssl-inspection <position> upl-rule
```

Параметры правил инспектирования SSL:

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). Примеры добавления пользователей в правило: <pre>user = known user = "user" user = "testd.local\user1" user = ("user", "testd.local\user1")</pre>
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, SMTPS 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.

Для редактирования правил инспектирования SSL используется команда:

```
Admin@nodename# set security-policy ssl-inspection <position> upl-rule
```

Для просмотра параметров всех созданных правил инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection
```

Для просмотра параметров определенного правила инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection <position>
```

Пример создания правила инспектирования SSL:

```
Admin@nodename# create security-policy ssl-inspection 1 upl-rule OK \
...user = unknown \
...ssl_profile("Default SSL profile") \
...rule_log(yes) \
...name("Decrypt all test rule") \
...desc("Description for decrypt all rest rule") \
...enabled(true)
...
Admin@nodename# show security-policy ssl-inspection 1
% ----- 1 -----
OK \
  user = unknown \
  desc("Description for decrypt all rest rule") \
  rule_log(yes) \
  ssl_profile("Default SSL profile") \
  enabled(true) \
  id("134b7274-01ee-47db-9fc1-a2f06b340b94") \
  name("Decrypt all test rule")
```

Для удаления правила инспектирования SSL используется команда:

```
Admin@nodename# delete security-policy ssl-inspection <position>
```

Настройка инспектирования SSH

Version: 7.x

Product: NGFW

Documentation: 

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

Для создания правила инспектирования SSH используется команда:

```
Admin@nodename# create security-policy ssh-inspection <position> upl-rule
```

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). Примеры добавления пользователей в правило: <pre>user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
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.

Для редактирования правил инспектирования SSH используется команда:

```
Admin@nodename# set security-policy ssh-inspection <position> upl-rule
```

Для просмотра всех созданных правил инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection
```

Для просмотра определенного правила инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection <position>
```

Пример создания правила инспектирования SSH с использованием UPL:

```
Admin@nodename# create security-policy ssh-inspection 1 upl-rule OK \
...service = ("Any TCP") \
...block_ssh_shell(yes) \
...block_sftp(yes) \
...rule_log(yes) \
...name("Test SSH inspection rule") \
...desc("Test SSH inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy ssh-inspection 1
% ----- 1 -----
OK \
  service = "Any TCP" \
  block_ssh_shell(yes) \
  block_sftp(yes) \
  desc("Test SSH inspection rule description") \
  rule_log(yes) \
  enabled(true) \
  id(d703f390-896f-47c2-91bd-69c6d37aa6d2) \
  name("Test SSH inspection rule")
```

Для удаления правила инспектирования SSH используется правило:

```
Admin@nodename# delete security-policy ssh-inspection <position>
```

Настройка COB

Version: 7.x

Product: NGFW

Documentation: ☒

Настройка параметров [управления загрузкой](#) системы обнаружения и предотвращения вторжений производится на уровне security-policy intrusion-prevention.

```
Admin@nodename# set security-policy intrusion-prevention <parameter>
```

Доступны параметры:

Параметр	Описание
flow-control	Включение/отключение функции flow control (доступно в версии 7.4.0 и выше): - on — функция включена; - off — функция отключена.
mode	Включение/отключение режима умного сканирования (сканируется часть проходящих пакетов сессии в пределах установленного лимита): - on — режим включен; - off — режим отключен.
limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Посмотреть установленные настройки можно с помощью команды:

```
Admin@nodename# show security-policy intrusion-prevention
```

По умолчанию функция flow control и режим умного сканирования включены; проверяются первые 200 КБ каждой сессии.

[Профили COB](#) создаются в библиотеке элементов и добавляются в [правила межсетевого экрана](#) для активации системы обнаружения и предотвращения вторжений.

Настройка правил защиты почтового трафика

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила защиты почтового трафика используется следующая команда:

Admin@nodename# create security-policy mail-security <position> upl-rule

Параметры правил защиты почтового трафика:

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") .
rule_log	Запись в журнал информации о срабатывании правила защиты почтового трафика. 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.
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) .

Параметр	Описание
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 .
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). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
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 .

Параметр	Описание
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 .

Для редактирования правила защиты почтового трафика используется команда:

```
Admin@nodename# set security-policy mail-security <position> upl-rule
```

Для просмотра параметров всех созданных правил защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security
```

Для просмотра параметров определенного правила защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security <position>
```

Пример создания правила защиты почтового трафика:

```
Admin@nodename# create security-policy mail-security 1 upl-rule WARNING \
...src.zone = Untrusted \
...service = (SMTP, POP3, SMTPS, POP3S) \
...mark_hdr(Subject) \
...mark("[SPAM]") \
...antispam_usergate(yes) \
...rule_log(yes) \
...name("Test SMTP and POP3 filtering") \
...desc("Test SMTP and POP3 filtering description") \
...enabled(true)
...
Admin@nodename# show security-policy mail-security 1
% ----- 1 -----
WARNING \
  src.zone = Untrusted \
  service = (SMTP, POP3, SMTPS, POP3S) \
  rule_log(yes) \
  desc("Test SMTP and POP3 filtering description") \
  mark_hdr(Subject) \
  mark("[SPAM]") \
  antispam_usergate(yes) \
  enabled(true) \
  id("7d86d348-9619-4097-94d1-bad4f3e85554") \
  name("Test SMTP and POP3 filtering")
```

Для удаления правила защиты почтового трафика используется команда:

```
Admin@nodename# delete security-policy mail-security <position>
```

Настройка антиспама

Параметры антиспама настраиваются на уровне **security-policy mail-security-antispam**.

Для настройки параметров антиспама используется следующая команда:

```
Admin@nodename# set security-policy mail-security-antispam <parameters>
```

Параметры настройки антиспама:

Параметр	Описание
batv-enabled	on/off . Включение/выключение защиты BATV (Bounce Address Tag Validation), предотвращающей рассылку спам-сообщений в виде возвратных сообщений.
dnsbl-servers	Указание списка DNSBL-серверов для проверки SMTP-трафика.
dnsbl-black-list	Список запрещенных серверов в дополнение к тем, что есть в списках DNSBL. Возможно добавление списка по GeoIP, или списка IP-адресов.
dnsbl-white-list	Список серверов, исключенных из DNSBL проверки. Возможно добавление списка по GeoIP, или списка IP-адресов.

Для просмотра параметров антиспама используется следующая команда:

```
Admin@nodename# show security-policy mail-security-antispam <parameters>
```

Возможен просмотр всех настроек антиспама целиком (по нажатию Enter), или отдельно белого/черного списков DNSBL при указании параметров **dnsbl-white-list** или **dnsbl-black-list**.

Для удаления параметров антиспама используется следующая команда:

```
Admin@nodename# delete security-policy mail-security-antispam <parameters>
```

Возможно удаление серверов DNSBL, белого/черного списков DNSBL.

Настройка правил ICAP

Documentation: ☒

Product: NGFW

Version: 7.x

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила ICAP используется команда:

```
Admin@nodename# create security-policy icap-rules <position> upl-rule
```

Параметры правил ICAP:

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). Примеры добавления пользователей в правило: <pre>user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
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: 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.
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, ...).

Для редактирования правила ICAP используется команда:

```
Admin@nodename# set security-policy icap-rules <position> upl-rule
```

Для просмотра параметров всех созданных ICAP правил используется команда:

```
Admin@nodename# show security-policy icap-rules
```

Для просмотра параметров определенного правила ICAP:

```
Admin@nodename# show security-policy icap-rules <position>
```

Пример создания правила ICAP:

```
Admin@nodename# create security-policy icap-rules 1 upl-rule PASS \  
...src.zone = Trusted \  
...http.method = (GET, POST) \  
...profile("ICAP server1") \  
...name("Test ICAP rule") \  
...desc("Test ICAP rule description") \  
...enabled(true)  
...
```

```
Admin@nodename# show security-policy icap-rules 1
```

```
% ----- 1 -----
```

```
PASS \  
src.zone = Trusted \  
http.method = (GET, POST) \  
desc("Test ICAP rule description") \  
profile("ICAP server1") \  
enabled(true) \  
id("80a7dca6-96f7-42c8-baad-8716be8d3b93") \  
name("Test ICAP rule")
```

Для удаления правила ICAP используется команда:

```
Admin@nodename# delete security-policy icap-rules <position>
```

Настройка ICAP-серверов

Product: NGFW
Documentation: ☒
Version: 7.x

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

Структура команды для создания ICAP-сервера:

```
Admin@nodename# create security-policy icap-server <parameter>
```

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. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу.
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-path	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Reqmod.
respmod-path	Использовать режим Respmo: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Respmo.
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@nodename# set security-policy icap-server <server-name> <parameter>
```

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

Структура команды для отображения информации об ICAP-сервере:

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

Структура команды для удаления ICAP-сервера:

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

Настройка профилей DoS

Documentation: 

Product: NGFW

Version: 7.x

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

Структура команды для создания профиля DoS:

```
Admin@nodename# create security-policy dos-profile <parameter>
```

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.
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.
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.
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 редактирования существующих профилей DoS:

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

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

Структура команды для удаления профиля:

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

Структура команды для отображения информации о профиле DoS:

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

Настройка правил защиты DoS

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка правил защиты от DoS атак производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Структура команды для создания правила защиты от DoS атак:

```
Admin@nodename# create security-policy dos-rules <position> upl-rule <parameters>
```

Параметры правил защиты от DoS атак:

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 .

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 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). Примеры добавления пользователей в правило: <pre>user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
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.

Структура команды для редактирования правила защиты от DoS атак:

```
Admin@nodename# set security-policy dos-rules <position> upl-rule <parameters>
```

Структура команды для просмотра правил защиты от DoS атак:

```
Admin@nodename# show security-policy dos-rules
Admin@nodename# show security-policy dos-rules <position>
```

Пример создания правила защиты от DoS атак с помощью UPL:

```
Admin@nodename# create security-policy dos-rules 1 upl-rule WARNING \
```

```

...src.zone = Untrusted \
...dst.zone = DMZ \
...service = (HTTP, HTTPS) \
...profile("Test DoS profile") \
...rule_log(session) \
...name("Test DoS rule") \
...desc("Test DoS rule description") \
...enabled(true)
...
Admin@nodename# show security-policy dos-rules 1
% ----- 1 -----
WARNING \
src.zone = Untrusted \
dst.zone = DMZ \
service = (HTTP, HTTPS) \
desc("Test DoS rule description") \
rule_log(session) \
profile("Test DoS profile") \
enabled(true) \
id("68da2f83-59ae-4a7d-b595-f6ff31bf34c6") \
name("Test DoS rule")

```

Структура команды для удаления правила защиты от DoS атак:

```
Admin@nodename# delete security-policy dos-rules <position>
```

