Table of Contents

Table of Contents 1
Настройка раздела Политики безопасности 2
- Настройка правил фильтрации контента 3
- Настройка правил веб-безопасности 7
- Настройка правил инспектирования SSL 10
- Настройка правил ICAP 13
- Настройка ICAP-серверов 16

Настройка раздела Политики безопасности

Настройка правил фильтрации контента

Product: SWG
Version: 7.5.x

Правила контентной фильтрации создаются на уровне security-policy content-filtering с помощью синтаксиса UPL. Подробнее о структуре команд — 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 просмотр веб-страницы; • DENY — блокировать веб-страницу; • WARNING — предупредить пользователя о том, что страница нежелательна для просмотра. Пользователь сам решает, отказаться от просмотра нет. Запись о просмотре страницы заносится в журнал
enabled	Включение или 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: • 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 — в разделе « Настройка сценариев»
virus_usergate	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием «Запретить»: • 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
blockpage	Выбор страницы блокировки; если страница не указана, используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например DENY("Blockpage (RU)"). Подробнее о настройке страниц блокировки — в разделе « Настройка шаблонов страниц». Вы также можете 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 — в разделе « Зоны»

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для списка IP-адресов: src.ip = lib.network() ; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов источника: src.ip = lib.url() ; в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке
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 — 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 — в разделе « Зоны»
dst.ip	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: dst.ip = lib.network() ; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: dst.ip = lib.url() ; в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке
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 — 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 — 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 укажите название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка типов контента»

Параметр	Описание
morphology	Список баз словарей морфологии, по которым будут проверяться веб-страницы. Для задания списка баз словарей морфологии: morphology = lib.morphology() ; в скобках укажите название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка морфологи»
request.header.User-Agent	User agent пользовательских браузеров, для которых будет применено правило. Для указания User agent пользовательских браузеров: request.header.User-Agent = lib.useragent() ; в скобках необходимо указать название категории User agent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка User agent 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 (адреса страниц, с которых пользователь перешел к текущему ресурсу) 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 — 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 — в разделе « Настройка календарей »
trusted_browser	Проверка подлинности браузера для предоставления доступа к ресурсам. Укажите созданное ранее подключение к серверу регистрации доверенных браузеров. Например: trusted_browser = "111". Подробнее о работе с доверенными браузерами — в разделе « Работа с доверенными браузерами »

Для редактирования правил контентной фильтрации используется команда:

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

Команда для просмотра всех созданных правил контентной фильтрации:

Admin@nodename# show security-policy content-filtering

Команда для просмотра определенного правила контентной фильтрации:

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")

Команда для удаления существующего правила контентной фильтрации:

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

Настройка правил веб-безопасности

Product: SWG
Version: 7.5.x

Правила веб-безопасности создаются на уровне security-policy safe-browsing с помощью синтаксиса UPL. Подробнее о структуре команд — 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: • 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 — в разделе « Настройка списков URL»
enable_injector	Встраивание кода в веб страницы: • enable_injector(yes) или enable_injector(true); • enable_injector(no) или enable_injector(false)
custom_injector	Встраиваемый код
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 — 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 — 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 — в разделе «Настройка списков URL»
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке
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 — в разделе0« Настройка LDAP-коннектора»). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках укажите название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Команда для редактирования правил веб-безопасности:

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

Команда для просмотра всех созданных правил веб-безопасности:

Admin@nodename# show security-policy safe-browsing

Команда для просмотра определенного правила веб-безопасности:

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")
```

Команда для удаления правила веб-безопасности:

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

Настройка правил инспектирования SSL

Product: SWG
Version: 7.5.x

Правила инспектирования SSL создаются на уровне security-policy ssl-inspection с помощью синтаксиса UPL. Подробнее о структуре команд — 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 — 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 — в разделе « Настройка профилей SSL»
rule_log	Запись в журнал информации о трафике при срабатывании правила: • 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, выдан 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	Блокировка 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 — в разделе «Настройка LDAP-коннектора»). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
src.zone	Зона источника трафика. Для указания зоны источника, например Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны»
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов источника: src.ip = lib.url(); в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке
dst.ip	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: dst.ip = lib.network(); в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: dst.ip = lib.url(); в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке
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 укажите название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки — 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 укажите название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки — в разделе « Настройка списков URL»
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках укажите название группы календарей. Подробнее о настройке календарей — в разделе « Настройка календарей»

Команда для редактирования правил инспектирования SSL:

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

Команда для просмотра параметров всех созданных правил инспектирования SSL:

Admin@nodename# show security-policy ssl-inspection

Команда для просмотра параметров определенного правила инспектирования SSL:

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")
```

Команда для удаления правила инспектирования SSL:

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

Настройка правил ICAP

Product: SWG
Version: 7.5.x

Правила ICAP создаются на уровне security-policy icap-rules с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила ICAP используется команда:

Admin@nodename# create security-policy icap-rules [reqmod | respmod] <position> upl-rule

Создание ICAP-правил раздельно для режимов REQMOD и RESPMOD доступно в версии 7.5.1 и выше.

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. Ппереслать 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 или 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, на которые UserGate SWG будет пересылать запросы; указывается в формате: profile("ICAP server1", "ICAP server2"). О настройке профилей серверов ICAP через CLI — 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 — в разделе « Зоны»
src.ip	Добавление списков IP-адресов или доменов источника. Для списка IP-адресов: src.ip = lib.network() ; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов источника: src.ip = lib.url() ; в скобках укажите название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = (BR, RU)). Коды названий стран доступны по ссылке

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 — в разделе «Настройка LDAP-коннектора»). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
dst.ip	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: dst.ip = lib.network() ; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: dst.ip = lib.url() ; в скобках укажите название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = (BR, RU)). Коды названий стран доступны по ссылке
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка: response.header.Content-Type = lib.mime() ; в скобках укажите название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — 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 укажите название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки — в разделе «Настройка категорий URL». Для указания категории URL: category = "URL category name" . Пример: category = (lib.category(cat1), "Web-based Email")
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url() ; в скобках укажите название списка URL. Подробнее о создании и настройке списков URL — в разделе « Настройка списков URL »
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например GET: http.method = GET
service	Тип сервиса. Чтобы указать сервис: service = "service name" . Например: service = http
before_content_filter	Параметр, определяющий порядок применения правил ICAP и контентной фильтрации (доступно в версии 7.5.1 и выше). Может применяться в сценариях, когда пользователь обращается к ресурсу, запрещенному политикой контентной фильтрации (например, при скачивании файла), чтобы такие запросы могли блокироваться до передачи на ICAP-сервер. Управлять приоритетом выполнения правил контентной фильтрации и ICAP можно для обоих стеков правил (REQMOD и RESPMOD). Порядок применения правил: • before_content_filter(true) — ICAP-правила ➔ Правила контентной фильтрации; • before_content_filter(false) — Правила контентной фильтрации ➔ ICAP-правила

Команда для редактирования правила ICAP:

```
Admin@nodename# set security-policy icap-rules [reqmod | respmod] <position> upl-rule
```

Команда для просмотра параметров всех созданных правил ICAP:

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

Команда для просмотра параметров определенного правила ICAP:

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

Пример создания правила ICAP:

```
Admin@nodename# create security-policy icap-rules reqmod 2 upl-rule PASS \
...src.zone = Trusted \
...http.method = GET \
...profile("ICAP server1") \
...name("Test ICAP rule") \
...desc("Test ICAP rule description") \
...before_content_filter(false) \
...enabled(true)
...
Admin@nodename# show security-policy icap-rules reqmod 2
% ----------------- 1 -----------------
PASS \
    src.zone = Trusted \
    http.method = GET \
    desc("Test ICAP rule description") \
    profile("ICAP server1") \
    enabled(true) \
    before_content_filter(false) \
    name("Test ICAP rule")
```

Команда для удаления правила ICAP:

```
Admin@nodename# delete security-policy icap-rules [reqmod | respmod] <position>
```

Настройка ICAP-серверов

Product: SWG
Version: 7.5.x

Профили ICAP-серверов настраиваются на уровне security-policy icap-server.

Для создания профиля ICAP-сервера используется команда:

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

Параметры ICAP-сервера.

Параметр	Описание
name	Имя ICAP-сервера
description	Описание ICAP-сервера
ip	IP-адрес ICAP-сервера
port	TCP-порт ICAP-сервера; значение по умолчанию: 1344
max-msg-size	Максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу
check-icap	Интервал времени в секундах, через который UserGate SWG посылает запрос на ICAP-сервер для проверки его доступности
bypass	Если эта опция включена, то устройство UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен
balance-max-connections	Максимальное количество соединений с сервером, которые могут быть установлены одновременно
balance-weight	Числовое значение, определяющее относительный вес сервера при балансировке трафика. Запросы распределяются пропорционально заданным весам. Значение 0 исключает сервер из пула балансировки
reqmod-path	Настройка работы режима REQMOD: • <text> — указание пути в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер; • off — отключить использование режима REQMOD
respmod-path	Настройка работы режима RESPMOD: • <text> — указание пути в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер; • off — отключить использование режима RESPMOD
user-header	Передача имени пользователя на ICAP-сервер: • <text> — указать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер; • off — не отправлять имя пользователя на ICAP-сервер
user-encode	Кодирование имени пользователя в Base64. Может потребоваться, если имена пользователей содержат символы национальных алфавитов. • on — включить; • off — отключить

Параметр	Описание
ip-header	Передача IP-адреса пользователя на ICAP-сервер: • <text> — заголовок, который будет использоваться для отправки IP-адреса пользователя на ICAP-сервер; • off — не отправлять IP-адрес пользователя на ICAP-сервер
mac-header	Передача MAC-адреса пользователя на ICAP-сервер: • <text> — заголовок, который будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер.; • off — не отправлять MAC-адрес пользователя на ICAP-сервер

Команда для обновления существующего профиля ICAP-сервера:

Admin@nodename# set security-policy icap-server <server-name> <parameter>

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

Команда для отображения информации о профиле ICAP-сервера:

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

Команда для удаления профиля ICAP-сервера:

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