

Table of Contents

Table of Contents	1
Экспорт и импорт настроек	2
Экспорт и импорт политик UserGate через CLI	3
Импорт настроек из файлов конфигурации кластера NGFW	5

Product: NGFW
Version: 7.x

Импорт доступен в следующих разделах:

- Сеть: правила DNS;
- Пользователи и устройства: правила captive-портала;
- Политики сети: правила межсетевого экрана, NAT и маршрутизации, пропускной способности;
- Политики безопасности: правила фильтрации контента, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, защиты почтового трафика, ICAP, защиты DoS, системы обнаружения и предотвращения вторжений, сценарии;
- Глобальный портал: правила веб-портала и reverse-прокси;
- VPN: серверные и клиентские правила.

Указанные выше правила настраиваются с использованием UserGate Policy Language (UPL), подробную информацию о котором вы можете найти в соответствующем [разделе](#) руководства администратора.

Рассмотрим экспорт и импорт правил на примере правил межсетевого экрана. На NGFW созданы следующие правила:

Мешевой экран

+

Добавить

✎

Редактировать

✖

Удалить

↔

Переместить

📄

Копировать

🔌

Включить

🔌

Отключить

📄

Скопировать ID правила

🔍

Открыть логи

🔄

Сбросить счётчики

Все

▼

Принуд

✓

🔍

🔍

#	С...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...
1	(...)	web1	🚫 Запретить	🖨 Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
2	(...)	web2	🚫 Запретить	🖨 DMZ	Любой	🖨 Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
3	(...)	web3	✅ Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
4	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—

Примечание Правила созданы для демонстрации примера.

Примечание После выполнения импорта все существующие правила раздела будут заменены на импортированные.

1. Для редактирования правила могут быть сохранены в файл конфигурации или скопированы из интерфейса командной строки. В обоих вариантах используется подключение к интерфейсу командной строки по SSH.

Для сохранения правил в файл, например, **fw_config.cfg**, выполните следующую команду:

```
ssh Admin@IP_ADDRESS -p 2200 show network-policy firewall >fw_config.cfg
```

где Admin - имя администратора;

IP ADDRESS - адрес интерфейса UserGate.

Введите пароль учетной записи администратора, файл со списком правил будет сохранён на вашем устройстве.

Для копирования правил из интерфейса командной строки подключитесь к CLI по SSH:

ssh Admin@IP ADDRESS -p 2200

где Admin - имя администратора;

IP ADDRESS - адрес интерфейса UserGate.

Подключение по SSH необходимо для возможности копирования правил.

Примечание Команды выполняются в режиме конфигурации.

Для перехода в режим конфигурации используйте следующую команду:

```
Admin@UGOS> configure
```

Отобразите в CLI правила раздела, которые необходимо выгрузить:

```
Admin@UGOS# show network-policy firewall
```

ПримечаниеИспользуйте *Tab* или *?* для просмотра текущих возможных значений или автодополнения.

Также действия над правилами могут быть выполнены после перехода на уровень раздела, в таком случае не нужно указывать уровень для каждой команды:

```
Admin@UGOS# edit network-policy firewall
```

```
[ network-policy firewall ]
Admin@UGOS# show
```

Результат выполнения команды:

```
network-policy firewall ]
Admin@UGOS> show

% ----- 1 -----
DENY \
    src.zone = Trusted \
    enabled(true) \
    id(ba1abe50-f492-4e12-8a12-86df83ba0481) \
    name(web1)
% ----- 2 -----
DENY \
    src.zone = DMZ \
    dst.zone = Untrusted \
    enabled(true) \
    id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
    name(web2)
% ----- 3 -----
PASS \
    enabled(true) \
    id("4e537010-322e-45e8-a1e1-7390f2300bce") \
    name(web3)
```

2. Скопируйте правила для редактирования: используйте, например, текстовый редактор.

Примечание Не копируйте строку с позицией первого правила.

Отредактируйте необходимые параметры правила. Для примера изменим названия правил на **cli1**, **cli2** и **cli3**, соответственно:

```
DENY \
  src.zone = Trusted \
  enabled(true) \
  id(ba1abe50-f492-4e12-8a12-86df83b40a81) \
  name(cjl1)
```

```
% ----- 2 -----
DENY \
  src.zone = DMZ \
  dst.zone = Untrusted \
  enabled(true) \
  id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
  name(cli2)
% ----- 3 -----
PASS \
  enabled(true) \
  id("4e537010-322e-45e8-a1e1-7390f2300bce") \
  name(cli3)
```

3. Импортируйте правила. Выделите и скопируйте правила в редакторе. Перейдите в CLI, введите команду **import upl-rule** и вставьте скопированные правила:

```
[ network-policy firewall ]
Admin@UGOS# import upl-rule DENY \
...  src.zone = Trusted \
...  enabled(true) \
...  id(ba1abe50-f492-4e12-8a12-86df83b40a81) \
...  name(cli1)
... % ----- 2 -----
... DENY \
...  src.zone = DMZ \
...  dst.zone = Untrusted \
...  enabled(true) \
...  id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
...  name(cli2)
... % ----- 3 -----
... PASS \
...  enabled(true) \
...  id("4e537010-322e-45e8-a1e1-7390f2300bce") \
...  name(cli3)
...
[ network-policy firewall ]
Admin@UGOS#
```

4. Проверьте изменения в CLI:

```
[ network-policy firewall ]
Admin@UGOS# show

% ----- 1 -----
DENY \
  src.zone = Trusted \
  enabled(true) \
  id("082ed6ed-20b6-4c93-921a-047eb9ff40a4") \
  name(cli1)
% ----- 2 -----
DENY \
  src.zone = DMZ \
  dst.zone = Untrusted \
  enabled(true) \
  id(f5f08dbd-019f-490a-8cfa-342c34a348fa) \
  name(cli2)
% ----- 3 -----
PASS \
  enabled(true) \
  id(b5ad3589-98d4-4911-8cf2-9590d0f3f4ea) \
  name(cli3)
```

или веб-интерфейсе:

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

Сбросить счётчики

Все

Принуд

✓

#	С...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...	
1	(...)	cli1	Запретить	Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...	
2	(...)	cli2	Запретить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...	
3	(...)	cli3	Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...	
4	(...)	Default block	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—	

Импорт настроек из файлов конфигурации кластера NGFW

Product: NGFW
Version: 7.x

Внимание! Лицензионные ключи версий 6 и 7 несовместимы. Перед обновлением до версии 7 необходимо запросить у менеджера ключ.

Администратор UserGate NGFW имеет возможность импортировать настройки узлов кластера NGFW из сохраненного ранее файла экспорта настроек кластера. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Экспорт настроек является кластерной функцией, т.е. экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.

Процедура импорта настроек узлов кластера NGFW включает в себя следующие основные шаги:

- 1. Экспорт настроек узлов исходного кластера NGFW.
- 2. Импорт настроек мастер-узла нового кластера.
- 3. Импорт настроек резервного узла нового кластера.

Важно! Импорт настроек кластера предназначен для восстановления настроек после переустановки ОС с нуля. Не рекомендуется проводить импорт полной конфигурации на работающем кластере (например, для проверки).

Импорт настроек мастер-узла приведёт к перезагрузке. В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится с импортированными настройками, кроме настроек кластера конфигурации (настройки кластера отказоустойчивости будут импортированы). Мастер-узел перестанет "видеть" резервный узел. Резервный узел нужно будет добавить в кластер конфигурации заново.

Импорт настроек резервного узла приведёт к перезагрузке. В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки. Внутреннее имя узла будет соответствовать импортированному имени старого резервного узла.

Экспорт настроек узлов кластера NGFW

1. Для экспорта настроек узлов исходного кластера NGFW в веб-консоли администратора любого из узлов кластера перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек**, нажмите **Экспорт** и выберите **Экспортировать все настройки**.

2. Сохраните созданный файл экспорта настроек узлов кластера.

Импорт настроек мастер-узла кластера

Важно! При импорте конфигурации NGFW с версий 7.X, при наличии в правилах доменных пользователей/групп, обязательно должен быть доступен LDAP-сервер для валидации пользователей, иначе правила будут импортированы без условия «Пользователи».

1. В веб-консоли узла, на который необходимо перенести настройки мастер-узла кластера, перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**:

2. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта настроек узлов кластера:

3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**:

4. Выберите будущую роль узла в кластере (в данном случае **Мастер-узел**) и название узла из файла экспорта. Нажмите **Старт**:

5. Узел перейдет в режим перезагрузки:

В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем применятся импортированные настройки конфигурации и узел загрузится с настройками мастер-узла из файла экспорта, включая импортированное название старого узла.

ПримечаниеИмпорт настроек не восстанавливает информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать NGFW с помощью имеющегося ПИН-кода.

Импорт настроек мастер-узла завершен.

Импорт настроек резервного узла кластера

Импорт настроек резервного узла кластера состоит из следующих основных этапов:

- 1. Первичная инициализация узла без добавления его в кластер и активации лицензии.
- 2. Импорт всех настроек резервного узла. Узел уйдёт в перезагрузку, в процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки.
- 3. Добавление узла в кластер конфигурации.
- 4. Импорт только сетевых настроек узла.

Подробнее о шагах импорта настроек резервного узла кластера:

- 1. Выполните первичную инициализацию узла согласно процедуре в разделе [«Первоначальная настройка»](#).
- 2. Импортируйте настройки резервного узла.
 - 2.1. В веб-консоли узла, на который необходимо перенести настройки резервного узла кластера, перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**:



- 2.2.. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта настроек узлов кластера:



- 2.3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**:



- 2.4. Выберите будущую роль узла в кластере (в данном случае **Slave-узел**) и название узла из файла экспорта. Нажмите **Старт**:



2.5. Узел перейдет в режим перезагрузки:

В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки. Внутреннее имя узла будет соответствовать выбранному имени старого резервного узла — это необходимо, чтобы кластер отказоустойчивости собрался корректно. Само отображение имени можно будет изменить в веб-интерфейсе на вкладке **Настройки** → **UserGate** → **Управление устройством** → **Кластер конфигурации**.

3. Добавьте узел в кластер конфигурации.

Необходимо произвести первоначальную установку узла как дополнительного узла в кластере:



4. Импортируйте сетевые настройки узла.

4.1. После добавления узла в кластер в качестве резервного узла необходимо импортировать только сетевые настройки резервного узла из файла экспорта. Для этого в веб-консоли узла перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**.



Выберите **Импортировать только сетевые настройки** и нажмите **Выбрать узлы**.

4.2. Выберите название резервного узла и нажмите **Старт**:



4.3. Резервный узел импортирует сетевые настройки из файла конфигурации.

Если лицензия на узле не отображается активной, можно ускорить процесс импорта лицензии с мастер-узла, нажав **Проверить лицензию** в Дашборде резервного узла.

Импорт настроек узлов кластера завершен.

