

Table of Contents

Table of Contents	1
Политики безопасности	2
Применение профилей COV/L7 для трафика DNAT	3
Создание и применение профилей COV	12

KnowledgeBase: ☒
Product: NGFW
Version: 7.1.x
Technology: IDPS

Начиная с версии ПО 7.1.0 профили COB и приложений (L7) применяются в разрешающих правилах межсетевого экрана.

Правила DNAT срабатывают до правил межсетевого экрана. Таким образом, для анализа трафика, прошедшего трансляцию DNAT с помощью COB или L7, необходимо в разрешающем правиле из зоны Untrusted в защищаемую зону или к публикуемому серверу добавить профили COB и/или приложений.

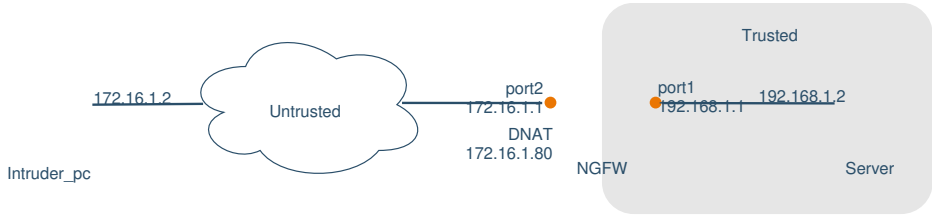
После попадания под разрешающее правило с профилями COB и/или приложений, трафик начинает анализироваться с помощью сигнатур профилей. При срабатывании сигнатур профиля будет выполнено действие, настроенное в профиле и произведена соответствующая запись в системном журнале, если была включена опция журналирования.

Если ни одна из сигнатур в профиле COB не сработала, то трафик пропускается дальше.

В профиле приложений в явном виде настраивается действие для неидентифицированного трафика. Если ни одна из сигнатур профиля приложений не сработала, выполняется настроенное действие для неидентифицированного трафика.

Рассмотрим пример применения профилей COB/L7 для трафика DNAT.

Схема тестовой сети выглядит следующим образом:



У межсетевого экрана UserGate (NGFW) настроены две зоны — Trusted и Untrusted. Интерфейс port1 в зоне Trusted имеет IP-адрес 192.168.1.1, интерфейс port2 в зоне Untrusted — IP-адрес 172.16.1.1. За межсетевым экраном в зоне Trusted находится сервер с IP-адресом 192.168.1.2. Сервер публикуется в зону Untrusted через DNAT с IP-адресом 172.16.1.80. Из зоны Untrusted к серверу обращается атакующий компьютер Intruder_pc с IP-адресом 172.16.1.2.

Настройка NGFW

На NGFW необходимо создать правило DNAT, правило межсетевого экрана и профили COB/приложений, содержащих необходимый набор сигнатур.

Создание правила DNAT

Для публикации сервера из зоны Trusted в зону Untrusted необходимо создать правило DNAT.

В свойствах правила необходимо указать тип трансляции адреса (DNAT), внешний IP-адрес с которым публикуется в зону Untrusted сервер (SNAT IP), включить журналирование для отображения событий в журнале трафика:

В качестве зоны источника трафика указать зону Untrusted:

В качестве адреса назначения указать публикуемый IP-адрес сервера (172.16.1.80):

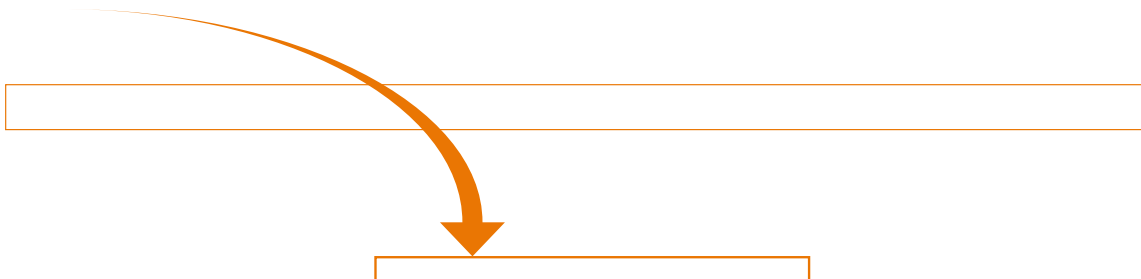
В качестве адреса назначения DNAT указать IP-адрес сервера в зоне Trusted:

Создание профиля COB

В библиотеке элементов создадим профиль COB *IDPS for DNAT*, который будет использоваться в данном примере. Добавим в этот профиль тестовую сигнатуру *BlackSun Test* с id 999999:



Во вкладке профиля **Совпавшие сигнатуры** переопределим действие на срабатывание этой сигнатуры. Действие по умолчанию **Пропустить** заменим на **Отбросить**:



Настройка правила межсетевого экрана

Создадим разрешающее правило межсетевого экрана, указав в качестве зоны источника трафика — зону Untrusted, а в качестве адреса назначения — адрес сервера 192.168.1.2.

В свойствах правила необходимо указать действие правила (**Разрешить**), включить журналирование для отображения событий в журнале трафика:

В качестве адреса назначения указать IP-адрес сервера 192.168.1.2:



Проверка работы

Пример 1. Без применения профилей COB/L7

Для начала проверим работу схемы без применения профилей COB/L7.

На сервере для эмуляции работы запустим встроенный пакет python:

```
server:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

На компьютере Intruder_pc создадим файл *bs.txt* и поместим в него строку со словом "*blacksun*", на которую реагирует соответствующая тестовая сигнатура COB:

```
intruder_pc:~$ echo "blacksun" > bs.txt
```

Передадим содержимое файла в утилиту *nc*, которая установит TCP-сессию с http-сервером по порту 8000 и отправит ему данную строку:

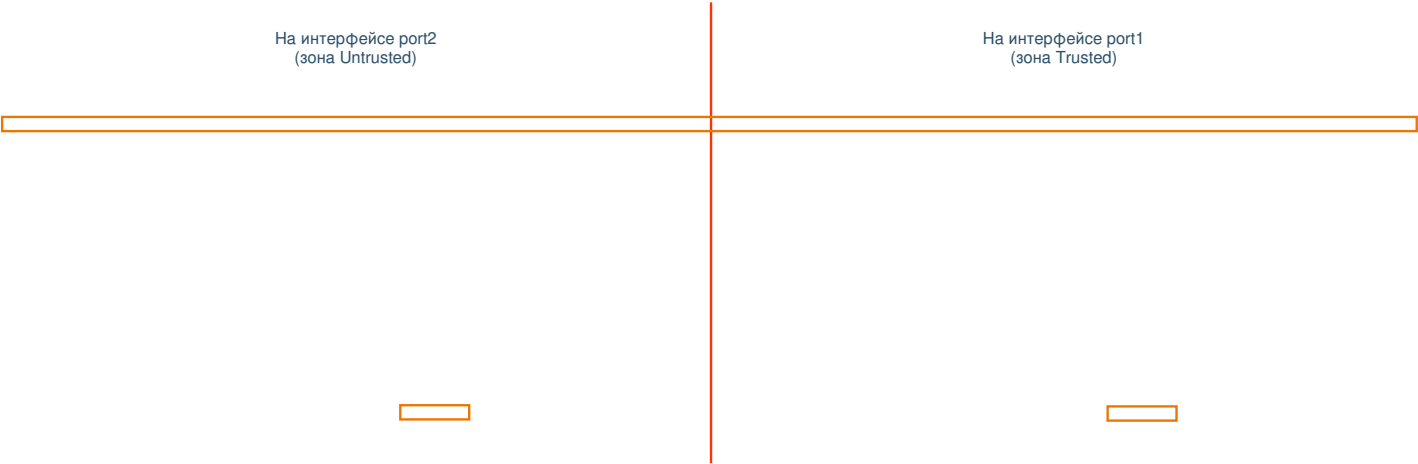
```
intruder_pc:~$ cat bs.txt | nc 172.16.1.80 8000
```

Intruder_pc получит ответ от сервера:

```
intruder_pc:~$ cat bs.txt | nc 172.16.1.80 8000
<!DOCTYPE HTML>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Error response</title>
  </head>
  <body>
    <h1>Error response</h1>
    <p>Error code: 400</p>
    <p>Message: Bad request syntax ('blacksun').</p>
```

```
<p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
</body>
</html>
```

В файле трассировки трафика можно увидеть, что сегмент со строкой "blacksun" успешно дошел до публикуемого сервера:



Срабатывание правил DNAT и межсетевого экрана отображается в журнале трафика NGFW:

Пример 2. С применением в правиле МЭ профиля COB

Добавим в созданное ранее правило межсетевого экрана профиль COB:



Для этого в свойствах правила межсетевого экрана на вкладке **Общие** необходимо указать созданный ранее профиль COB *IDPS for DNAT*:

```
Снова установим сессию со стороны Intruder_pc:
intruder_pc:~$ cat bs.txt | nc 172.16.1.80 8000
■
Ответ от сервера в этом случае не пришел.
```

В файле трассировки трафика можно увидеть, что сегмент со строкой *"blacksun"* был заблокирован NGFW. В трафике зоны Trusted его нет, а в трафике зоны Untrusted видны повторяющиеся попытки передать данный сегмент:



Срабатывание правил DNAT и межсетевого экрана отображается в журнале трафика *NGFW*:

В журнале COB отображается срабатывание профиля COB, который был включен в правило МЭ:

Пример 3. С применением в правиле МЭ профилей COB и L7

В данном примере к DNAT-трафику будут применены как профиль COB, так и профиль приложений (L7). При этом для демонстрации работы обоих профилей одновременно профиль приложений будет детектировать используемое приложение и пропускать его трафик, а профиль COB будет блокировать.

Создадим профиль приложений (профиль L7), который будет добавлен в наше правило межсетевого экрана.

Предварительно создадим тестовую пользовательскую сигнатуру приложения для детектирования нашего приложения (протокол TCP, порт 8000):



При создании профиля приложений добавим в него созданную сигнатуру *TCP 8000* (id = 1050002) и установим действие **Отбросить** для приложений, которые не были определены в этом профиле:

Действие на срабатывание сигнатуры по умолчанию останется **Пропустить**:

Добавим в созданное ранее правило межсетевого экрана профиль приложений *L7 for DNAT*:



Для этого в свойствах правила межсетевого экрана на вкладке **Общие** необходимо указать созданный ранее профиль приложений *L7 for DNAT*:

Снова установим сессию со стороны Intruder_pc:

```
intruder_pc:~$ cat bs.txt | nc 172.16.1.80 8000
```

■

Ответ от сервера в этом случае не пришел.

В файле трассировки трафика наблюдается то же, что и в [Примере 2](#) — сегмент со строкой *"blacksun"* был заблокирован NGFW. В трафике зоны Trusted его нет, а в трафике зоны Untrusted видны повторяющиеся попытки передать данный сегмент:

На интерфейсе port2
(зона Untrusted)

На интерфейсе port1
(зона Trusted)

Срабатывание правил DNAT и межсетевого экрана отображается в журнале трафика *NGFW*. Здесь же отображено срабатывание сигнатуры профиля приложений (приложение определено как *TCP 8000*) и выполнено действие, определенное в профиле (**Пропустить**):

В журнале COB отображается срабатывание профиля COB — трафик отброшен:

Product: NGFW
Version: 7.1.x
Technology: IDPS

Пример создания и применения профиля COB.

Создание профиля COB

Для создания профиля COB необходимо выполнить следующие шаги:

1. В веб-консоли администратора NGFW перейдите в раздел **Настройки → Библиотеки → Профили COB** и нажмите кнопку **Добавить** на панели инструментов.
2. В открывшемся окне **Свойства профиля COB** на вкладке **Общие** укажите название профиля.
3. В блоке **Фильтры** нажмите кнопку **Добавить** на панели инструментов.

4. В открывшемся окне **Свойства фильтра** настраиваются параметры фильтрации сигнатур COB из библиотеки сигнатур. Для примера выберите следующее:

- Нажав кнопку **Все**, выберите параметры **Высокий** и **Очень высокий**.
- Нажав кнопку **Еще**, выберите **Операционная система сигнатуры**, **Протокол**, **Категория**.
- Нажав кнопку **Операционная система сигнатуры**, выберите **Linux**.
- Нажав кнопку **Протокол**, выберите **HTTP**.
- Нажав кнопку **Категория**, выберите **exploit, injection**.

5. Нажмите на кнопку **Расширенный** на панели инструментов и проверьте строку получившегося фильтра:
threat IN ('medium','high','very high') AND (protocol = 'http') AND (category IN ('exploit','injection')) AND (os = 'Linux')

6. Нажмите на кнопку **Сохранить** для создания фильтра.

7. В одном профиле может быть несколько фильтров одновременно. Для создания дополнительного фильтра нажмите кнопку **Добавить** в блоке **Фильтры**. Сигнатуры можно искать по номеру их идентификатора. Для примера в открывшемся окне **Свойства фильтра** нажмите **Расширенный** на панели инструментов и в строке поиска сигнатур напишите:

id = 9001

Должна отобразиться сигнатура "DNSmasq RR Record Heap Buffer Overflow" с идентификатором 9001. Нажмите на кнопку **Сохранить** для создания фильтра.

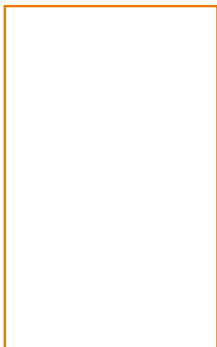


8. Проверьте, что в окне **Свойства профиля СОВ** в блоке **Фильтры** теперь отображаются оба созданных фильтра.

9. На вкладке **Совпавшие сигнатуры** будут отображаться сигнатуры, выбранные с помощью созданных ранее фильтров этого профиля. Для каждой из этих сигнатур можно переопределить параметры действия, журналирования и трассировки. Для этого необходимо выбрать сигнатуру указателем мыши, нажать правую кнопку в поле **Действие** и выбрать в контекстном меню **Переопределить**. В окне переопределения параметров сигнатуры выберите необходимые параметры.

Если необходимо одинаковым образом переопределить параметры всех совпавших сигнатур, нажмите на кнопку **Выделить все** на панели инструментов, затем нажмите на кнопку **Переопределить** там же на панели инструментов и далее выберите необходимые параметры для сигнатур.

Нажмите на кнопку **Сохранить** для закрытия окна **Переопределение сигнатуры** и применения параметров.
Убедитесь в том, что в интерфейсе в соответствующих полях изменились значения параметров для всех сигнатур.



10. Нажмите на кнопку **Сохранить** для создания профиля COB.

Применение профиля COB

Чтобы применить созданный профиль COB, его необходимо добавить в разрешающее правило межсетевого экрана. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур такого профиля будет произведено действие, настроенное в профиле и произведена соответствующая запись в Журнале COB, если была включена опция журналирования.

1. Для применения профиля в веб-консоли администратора NGFW перейдите в раздел **Настройки → Политики сети → Межсетевой экран**, выберите разрешающее правило межсетевого экрана и нажмите **Редактировать** в панели инструментов.

2. В открывшемся окне **Свойства правила межсетевого экрана** на вкладке **Общие** в поле **Профиль COB** выберите созданный ранее профиль.



3. Нажмите на кнопку **Сохранить**, чтобы применить изменение правила.

