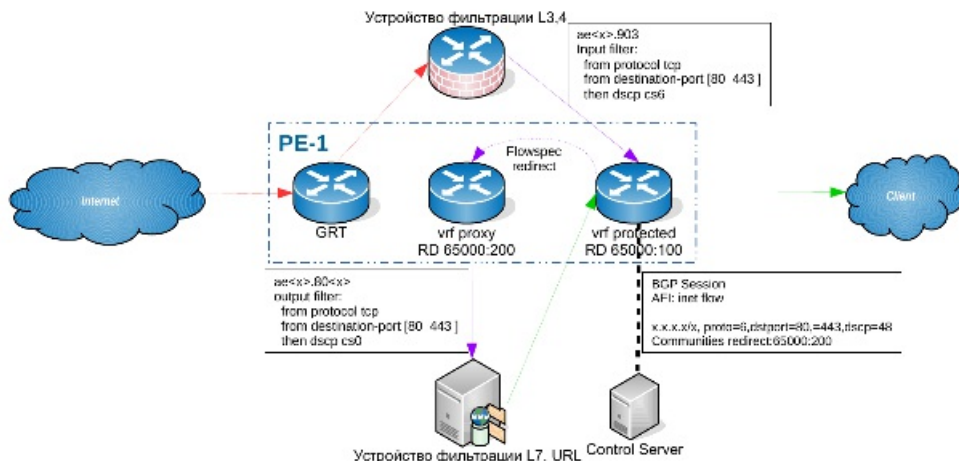


Перенаправление трафика на фильтрацию (URL, Layer 7, etc.) с применением BGP FlowSpec

Реализация на сети технологий MPLS и VPN позволяет реализовать гибкую схему управляемого перенаправления трафика на узлы фильтрации Layer7, URL, etc. Узлы фильтрации могут быть интегрированы в общую геораспределенную сеть ISP, оператора защиты от DDoS или, в зависимости от особенностей топологии сети, может быть реализована централизованная схема фильтрации.

Схема типового узла приведена ниже:



В схеме без фильтрации по L7 трафик из WAN поступает через форвардинг таблицы default.inet.0 на устройство фильтрации трафика по Layer 3 и Layer 4. Очищенный трафик направляется в сеть клиента через vrf protected.

Для перенаправления трафика на L7 фильтрацию создан новый routing-instances proxy с RD 65000:200, в котором маршрутная информация распространяется между всеми маршрутизаторами в сети, в iBGP включена кроме AFI inet-vpn-unicast дополнительно AFI inet-vpn-flow в MP-BGP, позволяющая передавать информацию FlowSpec в соответствующем vrf.

```
PE-1> show bgp neighbor 192.168.1.2 | match "NLRI for this session: |Table|Received prefixes:| Accepted prefixes:"
```

NLRI for this session: inet-unicast **inet-vpn-unicast** l2vpn inet6-labeled-unicast **inet-vpn-flow**

Table **proxy.inet.0** Bit: b0000

Received prefixes: 4

Accepted prefixes: 4

Table **protected.inetflow.0** Bit: c0000

Received prefixes: 1

Accepted prefixes: 1

Конфигурация routing-instances proxy приведена ниже:

```
PE-1>show configuration routing-instances proxy
```

```
instance-type vrf;
interface ae0.800;
interface ae0.801;
interface ae0.924;
route-distinguisher 65000:200;
vrf-target {
import target:65000:200;
export target:65000:200;
}
vrf-table-label;
routing-options {
static {
route 0.0.0.0/0 {
next-table protected.inet.0;
preference 200;
}
}
```

```

}
flow {
term-order standard;
}
}
protocols {
bgp {
import default-proxy;
export reject-all;
group Redirect {
type external;
passive;
peer-as 65501;
multipath;
neighbor 10.0.2.202 {
local-address 10.0.2.201;
}
neighbor 10.0.2.206 {
local-address 10.0.2.205;
}
}
}
}
}

```

В конфигурации протокола BGP routing-instances proxy указаны два neighbors устройств фильтрации по Layer7 для обеспечения избыточности одного узла.

Перенаправление трафика на L7 фильтрацию осуществляется следующим образом:
С Control Server (сервер управления), имеющего поднятую eBGP-сессию с family inet flow в routing-instances protected анонсируется по FlowSpec маршрут с соответствующими атрибутами для перенаправления трафика из routing-instances protected в routing-instances proxy. Пример ниже:

```

192.168.200.1*,proto=6,dstport=80,dscp=48/term:1
*[BGP/170] 4d 19:59:37, localpref 100, from 10.22.2.2
AS path: 65501 I, validation-state: unverified
Fictitious

```

Данный анонс распространяется по всем маршрутизаторам сети по inet-vpn-flow.

Конфигурация протокола BGP маршрутизатора для FlowSpec с Control Server приведена ниже:

```

PE-1> show configuration routing-instances protected protocols bgp group Servers neighbor 10.22.2.2
description "Proxy FlowSpec";
passive;
import Import_proxy_flowspec;
family inet {
flow {
prefix-limit {
maximum 200;
teardown;
}
no-validate Redirect-to-proxy;
}
}
export reject-all;
peer-as 65501;

```

Параметр no-validate позволяет FlowSpec маршрутам быть активными без валидации данных анонсов в inet.0. Примененное к neighbor policy осуществляет match по передаваемому FlowSpec community и перенаправляет трафик в routing-instances proxy. Пример конфигурации policy и community приведен ниже:

```

PE-1> show configuration policy-options policy-statement Redirect-to-proxy
term 1 {
from community redirect;
to instance proxy;
then accept;
}

```

```

}
term 2 {
then accept;
}
{master}
PE-1> show configuration policy-options community redirect
members redirect:65000:200;
{master}

```

Далеко не положительной особенностью является общий forwarding для всех instances, участвующих во FlowSpec, что приводит к постоянному циклическому форвардингу пакетов между instances, где они "умирают" по TTL. Решением данной проблемы стало раскраска трафика маркерами dscp на выходе устройств фильтрации Layer3,4 и сброс этих маркеров для трафика на выходе vrf proxy. Данное решение реализовано применением интерфейсных firewall filters и анонсом во FlowSpec match dscp, совпадающего с раскраской dscp на выходе устройств фильтрации Layer3,4. Примеры обоих фильтров приведены ниже:

```

PE-1> show configuration firewall filter mark_dscp_proxy
term 1 {
from {
protocol tcp;
destination-port [ 80 483 ];
}
then {
accept;
dscp cs6;
}
}
term 2 {
then accept;
}

```

```

PE-1> show configuration firewall filter clear_dscp
term 1 {
from {
protocol tcp;
destination-port [ 80 483 ];
}
then {
accept;
dscp cs0;
}
}
term 2 {
then accept;
}
{master}

```

Для маршрутизации трафика на фильтры Layer7 с каждым из них поднята BGP-сессия, в которой всеми фильтрами анонсируется маршрут 0.0.0.0/0, являющийся анукаст и основным маршрутом в таблице:

```

PE-2> show route table proxy.inet.0 0/0 exact
roxy.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0 *[BGP/170] 5d 20:56:48, localpref 100, from 192.168.1.4
AS path: 65501 I, validation-state: unverified
> to 10.10.48.1 via ae0.1062, label-switched-path PRIORITY-PE2-PE4
to 10.10.48.1 via ae0.1062, label-switched-path BE-PE2-PE4
to 10.10.68.1 via ae0.1064, label-switched-path PRIORITY-PE2-PE4
[BGP/170] 5d 21:01:12, localpref 100, from 192.168.1.3
AS path: 65501 I, validation-state: unverified
> to 10.10.48.1 via ae0.1062, label-switched-path PRIORITY-PE2-PE3
to 10.10.48.1 via ae0.1062, label-switched-path BE-PE2-PE3
to 10.10.68.1 via ae0.1064, label-switched-path PRIORITY-PE2-PE3
[BGP/170] 5d 21:32:11, localpref 100, from 192.168.1.1
AS path: 65501 I, validation-state: unverified

```

```
> to 10.10.68.1 via ae0.1064, label-switched-path PRIORITY-PE2-PE1  
to 10.10.48.1 via ae0.1062, label-switched-path PRIORITY-PE2-PE1-1  
to 10.10.68.1 via ae0.1064, label-switched-path BE-PE2-PE1  
to 10.10.48.1 via ae0.1062, label-switched-path PRIORITY-PE2-PE1  
to 10.10.68.1 via ae0.1064, label-switched-path PRIORITY-PE2-PE1-1  
[Static/200] 5d 20:54:19  
to table protected.inet.0
```

В данном vrf существует статический маршрут 0.0.0.0/0 с более высоким preference 200, и с next-table protected.inet.0, который служит byrass-маршрутом в случае каких-либо проблем с устройствами фильтрации Layer7.