

Combridge IP/BGP policy

IP Transit Global

1. Introduction:	2
2. Signalling communities:	3
2.1 AS Path Prepending	3
2.2 Restrict Route Propagation	3
2.3. Blackholing	3
2.3.1 Automatic (customer initiated) DoS filtering:	4
2.3.2 Manual (customer initiated) DoS filtering	4
3. Informational Communities	4
4. Traffic monitoring tool for customer	5
5. Looking glass	5
6. Escalation levels:	5

1. Introduction:

The Combridge is operating under AS5483 Internet network ("AS5483", AS SET:AS-MATAV).

We are offering two types of BGP sessions:

a) default BGP (advertised ~ 50 networks)

We are providing to customer /30 Ip range for interconnection.

b) full BGP.

Connection with a routereflector

Neighbor Ip address:145.236.224.176

Spec. Comm.: ebgp-multihop 5

Observations:

- Combridge does not accept (and advertise) routes more specific than/24
- Combridge filter the incoming updates based on the route objects found in the ripe database.
- The customer may ask for updating the filters if he adds new networks.
- The customer has to maintain proper ripe route entries.
- The customer should inform the provider about advertising of new AS

BGP Security policy

- Combridge do not accept routes that are not in the ripe db
- Combridge do not accept default route
- Combridge do not advertise default information by default
- Combridge do not accept/advertise private ip addresses
- Combridge do not filter outgoing traffic by default
- If DoS attack is coming from the customers network, the provider may set incoming filters, and notify customer.

We are providing the following BGP community based routing services to IP transit customer networks.

A customer network can use these communities to influence routing decisions and manipulate traffic streams within AS5483. There are two general categories of communities:

- Signalling communities that are sent by a customer network to request certain routing services from AS5483.
- Informational communities that AS5483 sends to provide additional information about routes that is not available via other BGP attributes.

2. Signalling communities:

2.1 AS Path Prepending

community	action
5483:6004	prepend 3x to bix
5483:6005	prepend 3x to ronix
5483:6007	prepend 3x to romtelecom
5483:6008	prepend 3x to UPC
5483:6011	prepend 3x to Interlan
5483:6012	prepend 3x to Fastlink
5483:6013	prepend 3x to Primetelecom
5483:6014	prepend 3x to Newcom
5483:6015	prepend 3x to Netserv
5483:6016	prepend 3x to Direct One
5483:6001	prepend 3x to dt
5483:6003	prepend 3x to level-3
5483:6006	prepend 3x to interroute
5483:6009	prepend 3x to google
5483:6010	prepend 3x to Globalcrossing

2.2 Restrict Route Propagation

community	action
5483:6101	don't advertise to dt
5483:6103	don't advertise to level-3
5483:6106	don't advertise to Interroute
5483:6109	don't advertise to google
5483:6110	don't advertise to Globalcrossing

2.3. Blackholing

2.3.1 Automatic (customer initiated) DoS filtering:

A customer network may request blackholing to defend against Denial of Service (DoS) and Distributed DoS attacks. Blackholing results in AS5483 discarding all traffic to the particular address space

Customer may send updates marked with community 5483:10000 (for /32 routes) to provider.

The customer may advertise only networks that are inside of his address space. blackholing remains active until customer advertises the specific network w/ community.

Ex:

```
!
ip prefix-list <filter-out> permit <ip address>
!
route-map <to-peer> permit 10
match ip address prefix-list <filter-out>
set community 5483:10000 additive
route-map <to-peer> permit 20
!
! in bgp config:
...
neighbor <peer> route-map <to-peer> out
...
!
```

2.3.2 Manual (customer initiated) DoS filtering

Customer may notify provider's NOC about being attacked and ask for applying outgoing filters.

The filters remain until customer asks for removal.

3. Informational Communities

As information to customer networks, AS5483 indicates on the routes it advertises whether the route is imported from a customer, peer or upstream provider.

Community Value	Description
5483:4001	routes from DTAG
5483:4003	routes from Level-3
5483:4004	routes from BIX
5483:4006	routes from PP romania
5483:4009	routes from Interroute
5483:4012	all international upstreams providers only, without BIX
5483:4013	routes from Combridge customers
5483:4014	routes from T-Mobile
5483:4015	routes from EKG
5483:4016	routes from Globalcrossing
5483:4017	routes from Primetelecom

Customer may use below example for settings:

```
ip community-list standard cmb-customers permit 5483:4013 route-map example-in
description from-Combridge
match community cmb-customers set local preference xxx route-map example-in
desc international set local preference yyy
```

xxx and yyy depends on customer configuration toward the other directions.

4. Traffic monitoring tool for customer

Customer should provide a public IP address to have access to the monitoring tool.
<http://monitor.combridge.ro:8181>

5. Looking glass

<http://netwiz.net.telekom.hu/lg/>

6. Escalation levels:

Technical problem :	
---------------------	--

Department	Helpdesk	24h/24h	Between 00:00 si 24:00,
Phone	+4031 0800 000 +4021 3120 396		
Fax	+4031 0800 201		
Mobile	+4075 1291 695		
E-Mail	support@combridge.ro		
Escalation level:			
<i>Level 2</i>	Level2 team Tel.: +40 31 0800 000 Fax.: +40 31 0800 201 Email: level2@combridge.ro	7days /week	Between 09:00 si 24.00
<i>Level 3</i>	Andrei Nedelcu Technical Manager Network Operation Tel.: +40 31 0800 224 Fax.: +40 31 0800 201 Mob: +40 741 249 954 Email: andrei.nedelcu@combridge.ro	<i>Working hours</i>	Between 09:00 si 18.00
<i>Level 4</i>	Endre Magyari Technical Director Tel.: +40 31 0800 202 Fax.: +40 31 0800 201 Mob: +40 744 794 735 Email: magyari.endre@combridge.ro	<i>Working hours</i>	Between 09:00 si 18.00
<i>Level 5</i>	Levente Csenteri Executive Director Tel: +40 31 0800 200 Fax: +40 31 0800 201 Mob. RO: + 40 744 666514 Mob. HU: + 36 30 9541225 Email: csenteri.levente@combridge.ro	<i>Working hours</i>	Between 09:00 si 18.00