DDoS Black-holing with ExaBGP in a Provider Network

by Matthias Cramer
matthias.cramer@iway.ch

At the beginning there is a DDoS

You have a Server/Costumer in your Network which is under a DDoS attack.
First you need to have the tools to find out the attacked IP. Attacker is out of interest in a DDoS situation. We use Netflow/sFlow data from our Core Equipment and analyse it with the help of nfsen/nfdump.
If you know the IP you can start trying filtering at L3 L4 on the customer Firewall or with ACL's on the core. If that helps you are lucky. But probably not for long.

Your upstream Transit Links get full

The attack has changed. Now it is a bandwidth heavy attack. This is normal when the Attacker sees that the Site comes back on line while still under attack.
So what now ? Call your upstream to black hole the traffic ? I'm sort of. We do it the automatic way.
Most of the Transit Carriers have BGP community's in place to black hole a /32 prefix. In the past this was a pita to configure this. With a exaBGP server in Place it is a matter of a few minutes

The Provider Network

The BGP and exaBGP Config

At the end there is mostly happyness

Now your Network is happy again. The only thing you have to deal with is the customer that is offline now because you black holed him. But usually he is not entirely innocent...

To see if the DDoS has stopped. Just stop the exaBGP announcements... And see if traffic comes or not. If not we have a big success. Else wait another few minutes/hours...

Questions ?

iway.ch

iway.ch
QUALITY INTERNET SERVICES

Prezi

DDoS Black-holing with ExaBGP in a Provider Network

by Matthias Cramer
matthias.cramer@iway.ch

At the beginning there is a DDoS

You have a Server/Customer in your Network which is under a DDoS attack. First you need to have the tools to find out the attacked IP. Attacker is not of interest in a DDoS situation. We use NetFlow/sFlow data from our Core Equipment and analyse it with the help of nfsen/nfdump. If you know the IP you can start trying filtering at L3 L7 on the customer Firewall or with ACL's on the core. If that helps you are lucky. But probably not for long.

Your upstream Transit Links get full

The attack has changed. Now it is a bandwidth heavy attack. This is normal when the Attacker sees that the Site comes back on line while still under attack.
So what now ? Call your upstream to black hole the traffic ? Yes, sort of. We do it the automatic way. Most of the Transit Carriers have BGP community's in place to black hole a /32 prefix. In the past this was a pita to configure this. With a exaBGP server in place it is a matter of a few minutes

The Provider Network

The BGP and exaBGP Config

[illegible]

At the end there is mostly happyness

Now your Network is happy again. The only thing you have to deal with is the customer that is offline now because you black holed him. But usually he is not entirely innocent..

To see if the DDoS has stopped. Just stop the exaBGP announcements.. And see if traffic comes or not. If not we have a big success. Else wait another few minutes/hours..

Questions ?

iway.ch

iway.ch
QUALITY INTERNET SERVICES

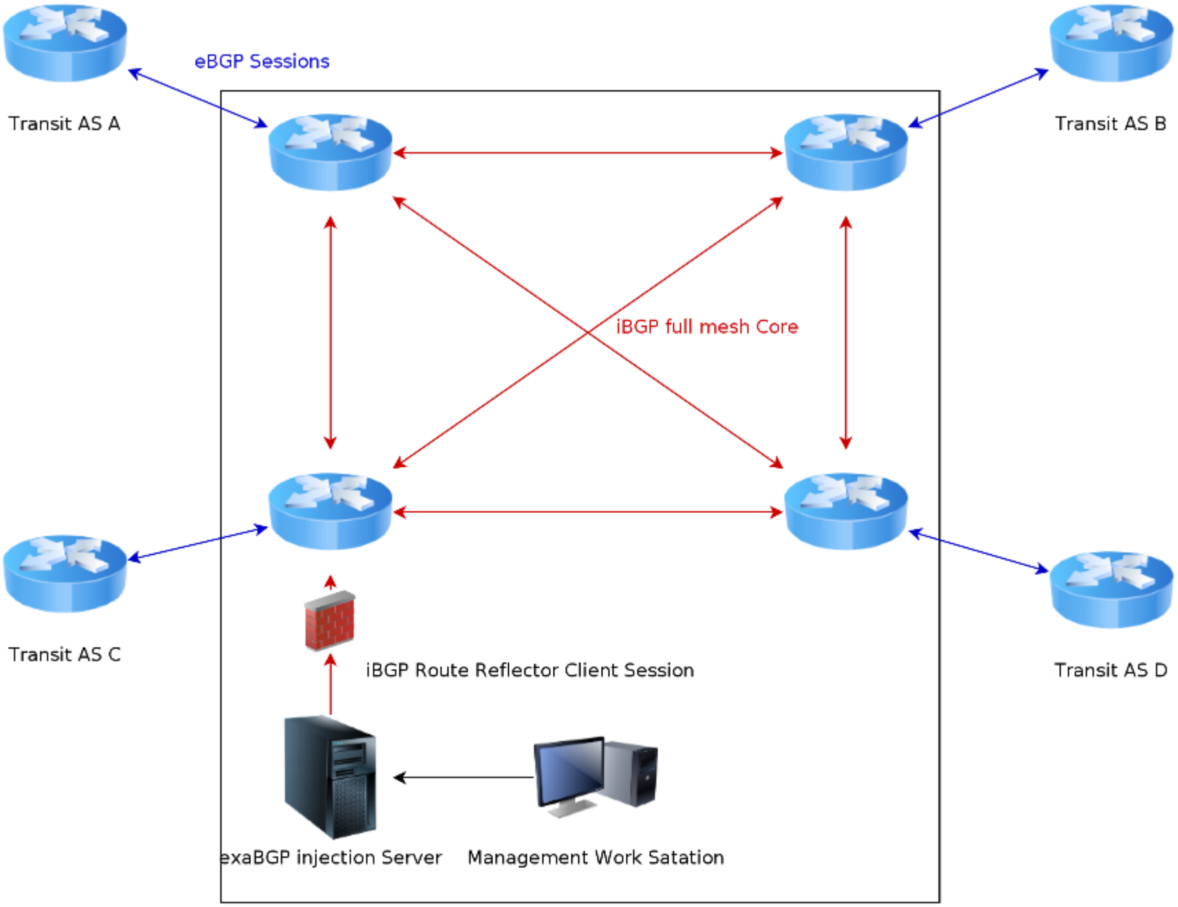
At the beginning there is a DDoS

You have a Server/Customer in your Network which is under a DDoS attack.
First you need to have the tools to find out the attacked IP. Attacker is not of interest in a DDoS situation. We use Netflow/sFlow data from our Core Equipment and analyze it with the help of nfsen/nfdump.
If you have the IP you can start trying filtering at L3-L7 on the customer Firewall or with ACL's on the core. If that helps you are lucky. But probably not for long...

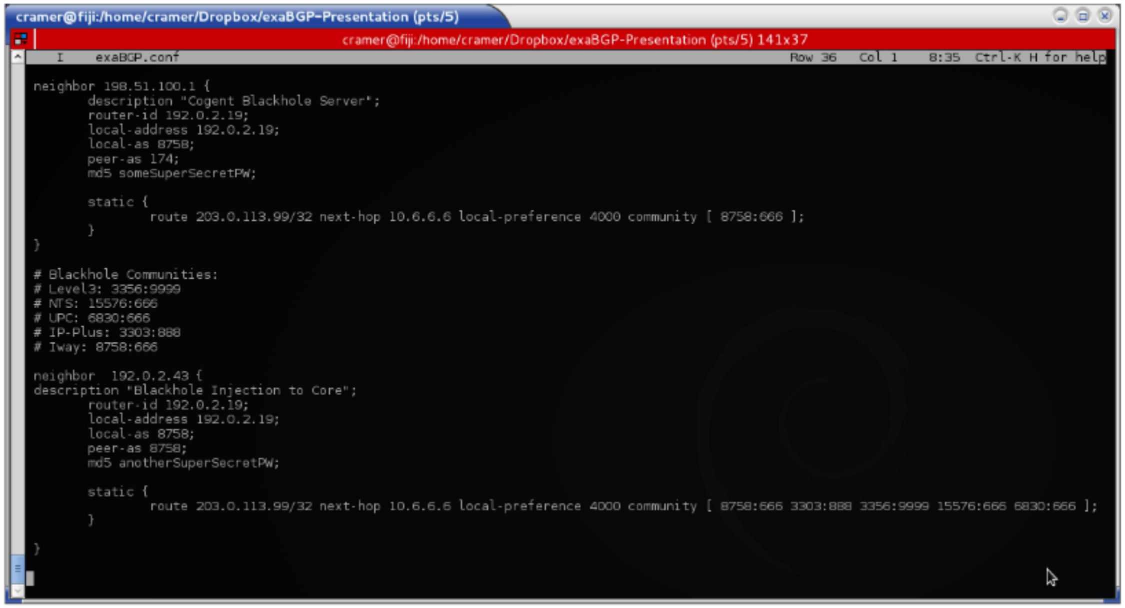
Your upStream TranSit LinkS get full

The attack has changed. Now it is a bandwidth heavy attack. This is normal when the Attacker sees that the Site comes back on line while still under attack.
So what now ? Call your upstream to black hole the traffic ? Yes, sort of. We do it the automatic way.
Most of the Transit Carriers have BGP community's in place to black hole a /32 prefix. In the past this was a pita to configure this. With a exaBGP server in Place it is a matter of a few minutes

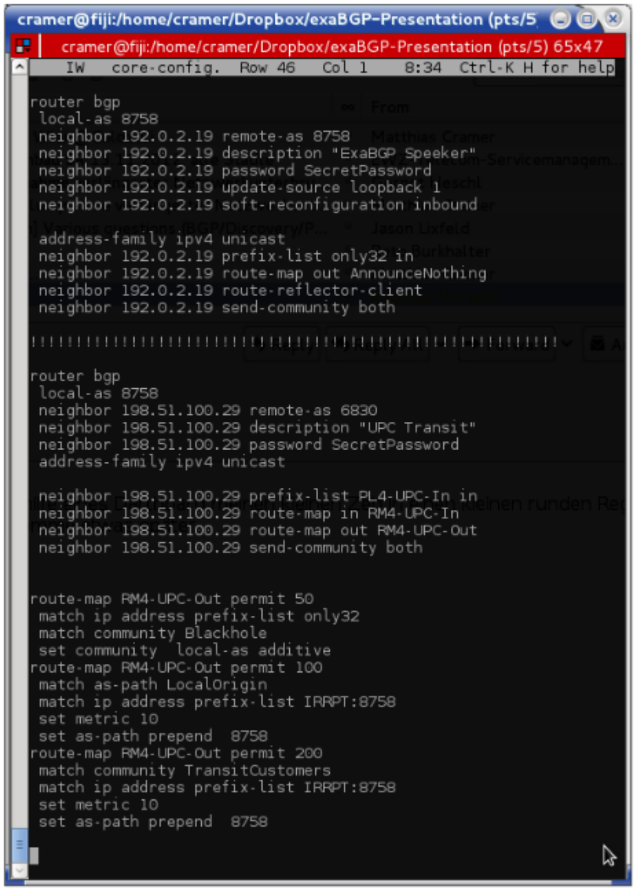
The Provider Network



The BGP and exaBGP Config

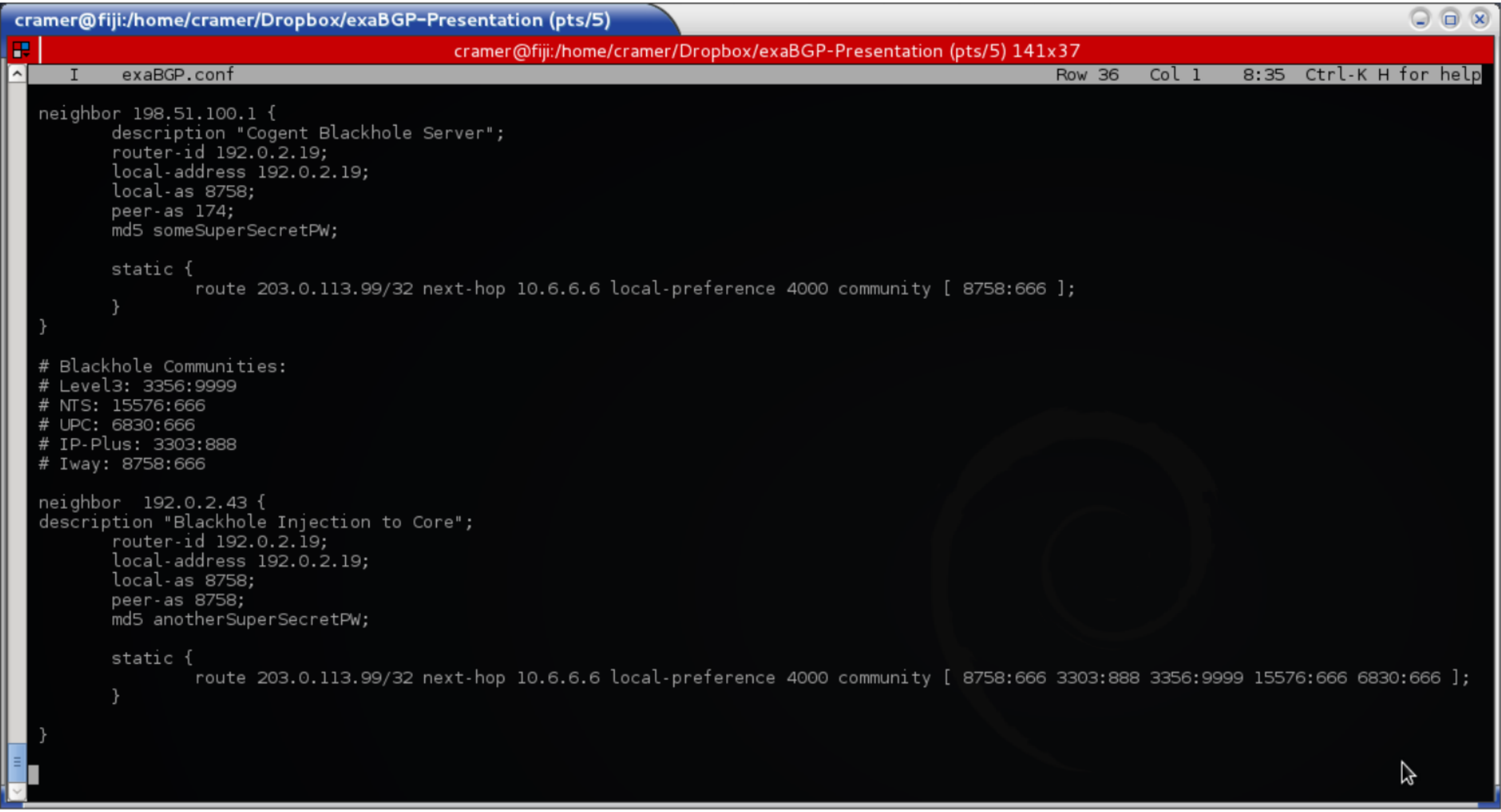

cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5)
cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5) 141x37

```
  I    exaBGP.conf                                    Row 36   Col 1    8:35  Ctrl-K H for help

neighbor 198.51.100.1 {
        description "Cogent Blackhole Server";
        router-id 192.0.2.19;
        local-address 192.0.2.19;
        local-as 8758;
        peer-as 174;
        md5 someSuperSecretPW;

        static {
                route 203.0.113.99/32 next-hop 10.6.6.6 local-preference 4000 community [ 8758:666 ];
        }
}

# Blackhole Communities:
# Level3: 3356:9999
# NTS: 15576:666
# UPC: 6830:666
# IP-Plus: 3303:888
# Iway: 8758:666

neighbor  192.0.2.43 {
description "Blackhole Injection to Core";
        router-id 192.0.2.19;
        local-address 192.0.2.19;
        local-as 8758;
        peer-as 8758;
        md5 anotherSuperSecretPW;

        static {
                route 203.0.113.99/32 next-hop 10.6.6.6 local-preference 4000 community [ 8758:666 3303:888 3356:9999 15576:666 6830:666 ];
        }

}
```


cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5
cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5) 65x47

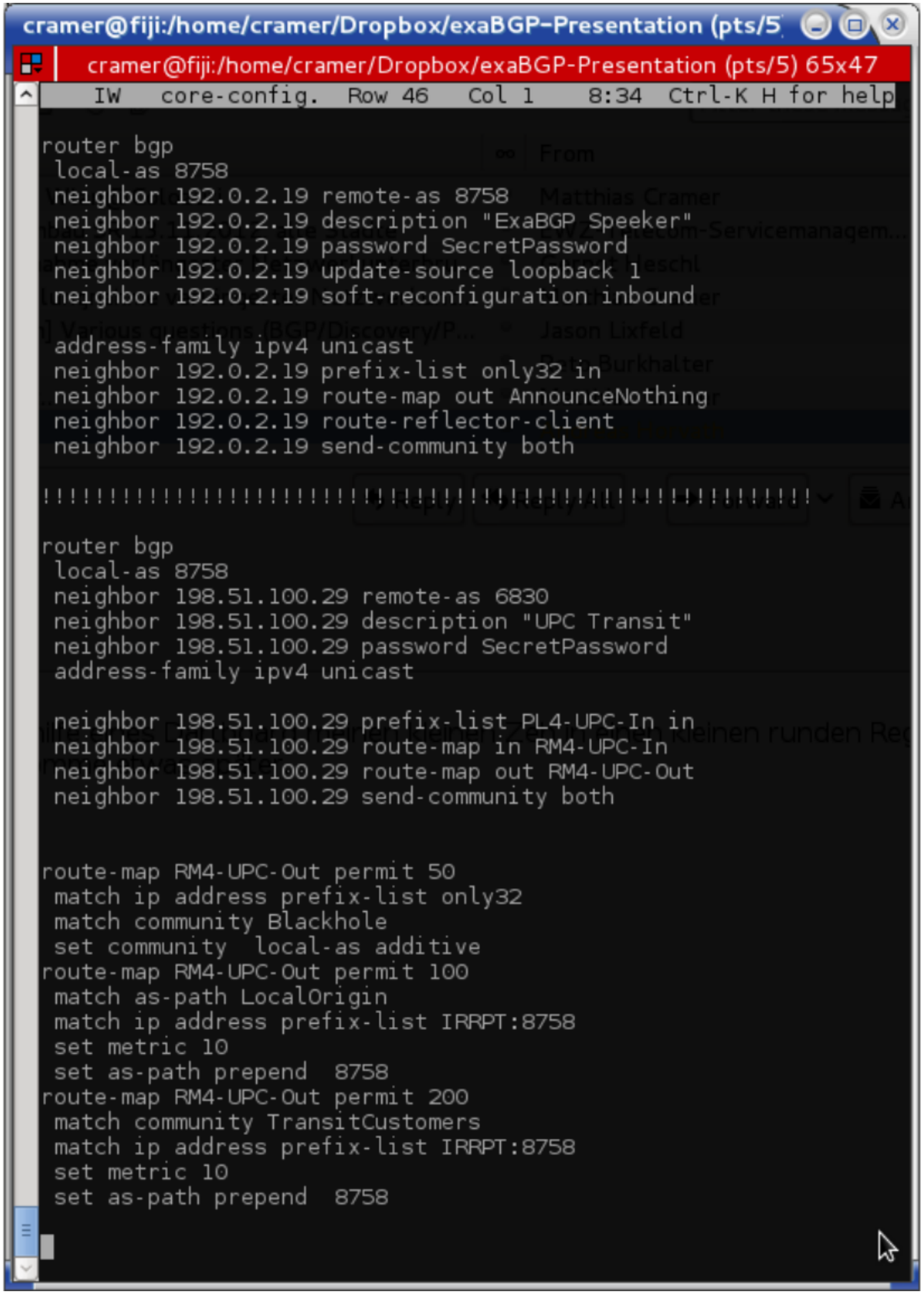
```
    IW   core-config.  Row 46   Col 1    8:34  Ctrl-K H for help

router bgp
 local-as 8758
 neighbor 192.0.2.19 remote-as 8758
 neighbor 192.0.2.19 description "ExaBGP Speeker"
 neighbor 192.0.2.19 password SecretPassword
 neighbor 192.0.2.19 update-source loopback 1
 neighbor 192.0.2.19 soft-reconfiguration inbound

 address-family ipv4 unicast
 neighbor 192.0.2.19 prefix-list only32 in
 neighbor 192.0.2.19 route-map out AnnounceNothing
 neighbor 192.0.2.19 route-reflector-client
 neighbor 192.0.2.19 send-community both

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

router bgp
 local-as 8758
 neighbor 198.51.100.29 remote-as 6830
 neighbor 198.51.100.29 description "UPC Transit"
 neighbor 198.51.100.29 password SecretPassword
 address-family ipv4 unicast

 neighbor 198.51.100.29 prefix-list PL4-UPC-In in
 neighbor 198.51.100.29 route-map in RM4-UPC-In
 neighbor 198.51.100.29 route-map out RM4-UPC-Out
 neighbor 198.51.100.29 send-community both


route-map RM4-UPC-Out permit 50
 match ip address prefix-list only32
 match community Blackhole
 set community  local-as additive
route-map RM4-UPC-Out permit 100
 match as-path LocalOrigin
 match ip address prefix-list IRRPT:8758
 set metric 10
 set as-path prepend  8758
route-map RM4-UPC-Out permit 200
 match community TransitCustomers
 match ip address prefix-list IRRPT:8758
 set metric 10
 set as-path prepend  8758
```

The BGP and exaBGP Config


cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5)
cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5) 141x37

```
   I    exaBGP.conf                                                                                        Row 36    Col 1     8:35  Ctrl-K H for help

neighbor 198.51.100.1 {
        description "Cogent Blackhole Server";
        router-id 192.0.2.19;
        local-address 192.0.2.19;
        local-as 8758;
        peer-as 174;
        md5 someSuperSecretPW;

        static {
                route 203.0.113.99/32 next-hop 10.6.6.6 local-preference 4000 community [ 8758:666 ];
        }
}

# Blackhole Communities:
# Level3: 3356:9999
# NTS: 15576:666
# UPC: 6830:666
# IP-Plus: 3303:888
# Iway: 8758:666

neighbor  192.0.2.43 {
description "Blackhole Injection to Core";
        router-id 192.0.2.19;
        local-address 192.0.2.19;
        local-as 8758;
        peer-as 8758;
        md5 anotherSuperSecretPW;

        static {
                route 203.0.113.99/32 next-hop 10.6.6.6 local-preference 4000 community [ 8758:666 3303:888 3356:9999 15576:666 6830:666 ];
        }

}
```

```
ol 1     8:35  Ctrl-K H for help

356:9999 15576:666 6830:666 ];
```


cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5
cramer@fiji:/home/cramer/Dropbox/exaBGP-Presentation (pts/5) 65x47

```
    IW   core-config.  Row 46    Col 1      8:34  Ctrl-K H for help

router bgp
 local-as 8758
 neighbor 192.0.2.19 remote-as 8758
 neighbor 192.0.2.19 description "ExaBGP Speeker"
 neighbor 192.0.2.19 password SecretPassword
 neighbor 192.0.2.19 update-source loopback 1
 neighbor 192.0.2.19 soft-reconfiguration inbound

 address-family ipv4 unicast
 neighbor 192.0.2.19 prefix-list only32 in
 neighbor 192.0.2.19 route-map out AnnounceNothing
 neighbor 192.0.2.19 route-reflector-client
 neighbor 192.0.2.19 send-community both

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

router bgp
 local-as 8758
 neighbor 198.51.100.29 remote-as 6830
 neighbor 198.51.100.29 description "UPC Transit"
 neighbor 198.51.100.29 password SecretPassword
 address-family ipv4 unicast

 neighbor 198.51.100.29 prefix-list PL4-UPC-In in
 neighbor 198.51.100.29 route-map in RM4-UPC-In
 neighbor 198.51.100.29 route-map out RM4-UPC-Out
 neighbor 198.51.100.29 send-community both


route-map RM4-UPC-Out permit 50
 match ip address prefix-list only32
 match community Blackhole
 set community  local-as additive
route-map RM4-UPC-Out permit 100
 match as-path LocalOrigin
 match ip address prefix-list IRRPT:8758
 set metric 10
 set as-path prepend  8758
route-map RM4-UPC-Out permit 200
 match community TransitCustomers
 match ip address prefix-list IRRPT:8758
 set metric 10
 set as-path prepend  8758
```

At the end there is mostly happyness

Now your Network is happy again. The only thing you have to deal with is the customer that is offline now because you black holed him. But usually he is not entirely innocent...

To see if the DDoS has stopped. Just stop the exaBGP announcements... And see if traffic comes or not. If not we have a big success. Else wait another few minutes/hours...

Questions ?

iway.ch

QUALITY INTERNET SERVICES