Experiment 4a - BGP Security

DE-CIX Academy

Version 1.2 - Students Copy

1 Introduction

In this series of experiments we protect our BGP setup against malicious BGP announcements and other various threats from the Internet.

2 Network Setup

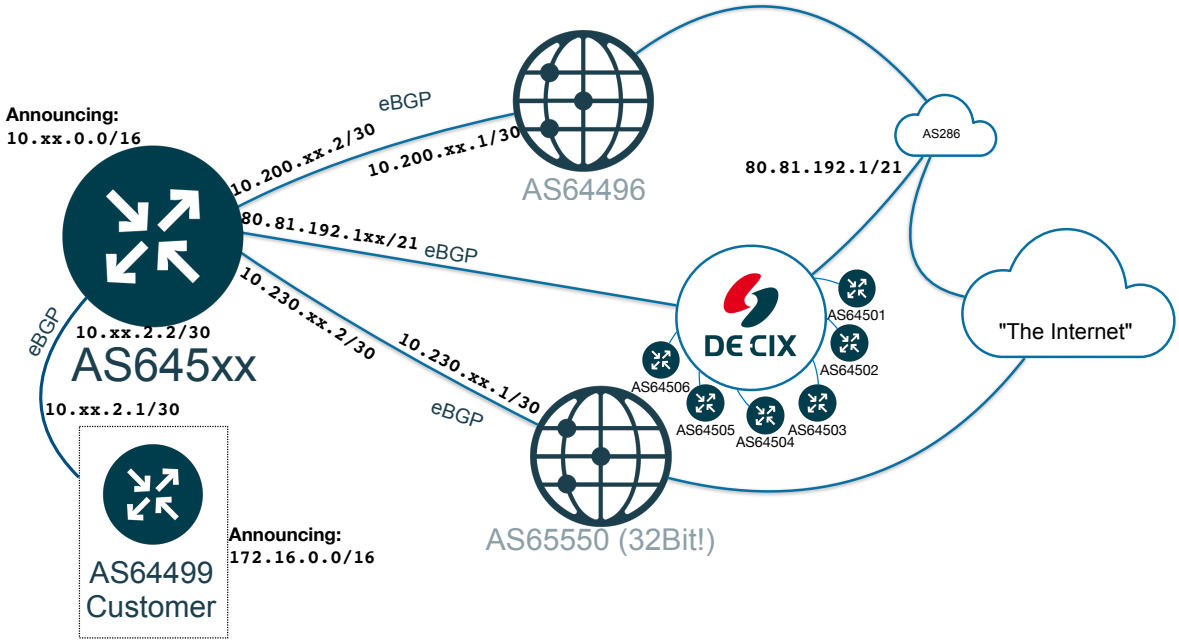


Figure 1: Network Setup

Figure 1 shows the network topology for this experiment. Two upstreams, one customer and everybody peers with each other.

3 Security Measures

3.1 Maximum Prefix

To configure maximum prefix use the *maximum-prefix* statement for either a single peer or a peer-group in address-family context:

neighbor *<ip address> | <peergroup-name>* maximum-prefix *<threshold> <warning-percentage>* restart *<restart-time>*
defines a maximum prefix for either *<ip address>* (can be IPv4 or IPv6) or a whole peer group:

<threshold> is the number of prefixes you allow from this peer or peer group. If more are received the BGP session is shut down.

<warning-percentage> is optional - if this percentage of <*threshold*> prefixes are received the router loggs a warning message.

restart *<restart time>* is also optional (but recommended); if it is missing the BGP session stays down until manual intervention (using a *clear* command). It configures the number of minutes after which the BGP session is made active again.

3.2 MD5 Session Passwort

This is usually done for each individual peer (it would only make sense doing this for a peer-group in case of iBGP). You put the password *outside* of any address-family context:

neighbor *<ip address> | <peergroup-name>* password *<some password>* this configures an MD5 password on the TCP session to the neighbor. Be aware this becomes active immediately so the BGP session will drop. The neighbor has to configure the same password.

Keep in mind that you need a functioning and maintained password management if you use session passwords in production. Usually the effort is not worth it and TTL security (see next section) can achieve the same.

3.3 TTL security

To ensure that a BGP peer is a specific number of hops away (usually in eBGP exactly one hop) the TTL counter of IP packets can be used. For a hop of one: if packets are sent with a TTL of 255 and not received with TTL of 255 they are discarded. For a hop of two, 255 and 254 as TTL are allowed and so on.

Configuration commands:

neighbor *<ip address> | <peergroup-name>* ttl-security hops *<hopnumber>* - this allows the neighbor to be maximum <*hopnumber*> hops away. TTL security needs to be configured on both sides of a BGP session.

A Initial Router Configuration

(instead of XX insert your router number)

```
hostname rXX
!
ip route 10.XX.0.0/16 Null0
!
interface loopback0
 ip address 10.XX.1.1/32
!
router bgp 645XX
 neighbor customer peer-group
 neighbor peering peer-group
 neighbor upstream peer-group
 neighbor 10.XX.2.1 remote-as 64499
 neighbor 10.XX.2.1 peer-group customer
 neighbor 80.81.192.1 remote-as 286
 neighbor 80.81.192.1 peer-group peering
 neighbor 80.81.192.102 remote-as 64502
 neighbor 80.81.192.102 peer-group peering
 ...
 neighbor 10.200.XX.1 remote-as 65550
 neighbor 10.200.XX.1 peer-group upstream
 neighbor 10.230.XX.1 remote-as 64496
 neighbor 10.230.XX.1 peer-group upstream
 !
 address-family ipv4 unicast
  network 10.XX.0.0/16 route-map own-networks
  neighbor customer next-hop-self
  neighbor customer soft-reconfiguration inbound
```

```
  neighbor customer route-map customer-in in
  neighbor customer route-map customer-out out
  neighbor peering next-hop-self
  neighbor peering soft-reconfiguration inbound
  neighbor peering route-map peering-in in
  neighbor peering route-map peering-out out
  neighbor upstream next-hop-self
  neighbor upstream soft-reconfiguration inbound
  neighbor upstream route-map upstream-in in
  neighbor upstream route-map upstream-out out
 exit-address-family
!
bgp community-list expanded announce-to-customer permit _645XX:4[1357]000
bgp community-list expanded announce-to-peering permit _645XX:4[2367]000
bgp community-list expanded announce-to-upstream permit _645XX:4[4567]000
bgp community-list expanded my-communities permit _645XX:.*
bgp large-community-list expanded my-largecommunities permit _645XX:.*:.*
!
route-map upstream-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map upstream-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
 on-match next
!
route-map upstream-in permit 100
 set community 645XX:41000 additive
 set extcommunity rt 645XX:21000
 set large-community 645XX:2:1000 additive
 set local-preference 10
!
route-map peering-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map peering-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
 on-match next
!
route-map peering-in permit 100
 set community 645XX:41000 additive
 set extcommunity rt 645XX:23000
 set large-community 645XX:2:3000 additive
 set local-preference 1000
!
route-map customer-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map customer-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
```

```
 on-match next
!
route-map customer-in permit 100
 set community 645XX:47000 additive
 set extcommunity rt 645XX:24000
 set large-community 645XX:2:4000 additive
 set local-preference 10000
!
route-map customer-out permit 100
 match community announce-to-customer
!
route-map peering-out permit 100
 match community announce-to-peering
!
route-map upstream-out permit 100
 match community announce-to-upstream
!
route-map own-networks permit 100
 set community 645XX:47000
!
line vty
!
end
```

B Final Router Configuration

```
hostname rXX
!
ip route 10.XX.0.0/16 Null0
!
interface loopback0
 ip address 10.XX.1.1/32
!
router bgp 645XX
 neighbor customer peer-group
 neighbor peering peer-group
 neighbor upstream peer-group
 neighbor 10.XX.2.1 remote-as 64499
 neighbor 10.XX.2.1 peer-group customer
 neighbor 80.81.192.1 remote-as 286
 neighbor 80.81.192.1 peer-group peering
 neighbor 80.81.192.102 remote-as 64502
 neighbor 80.81.192.102 peer-group peering
 neighbor 80.81.192.102 ttl-security hops 1
 neighbor 80.81.192.102 password somepasswordhere
 ...
 neighbor 10.200.XX.1 remote-as 65550
 neighbor 10.200.XX.1 peer-group upstream
 neighbor 10.230.XX.1 remote-as 64496
 neighbor 10.230.XX.1 peer-group upstream
 !
 address-family ipv4 unicast
  network 10.XX.0.0/16 route-map own-networks
  neighbor customer next-hop-self
  neighbor customer soft-reconfiguration inbound
  neighbor customer route-map customer-in in
  neighbor customer route-map customer-out out
```

```
  neighbor peering next-hop-self
  neighbor peering soft-reconfiguration inbound
  neighbor peering route-map peering-in in
  neighbor peering route-map peering-out out
  neighbor peering maximum-prefix 100 80 restart 1
  neighbor upstream next-hop-self
  neighbor upstream soft-reconfiguration inbound
  neighbor upstream route-map upstream-in in
  neighbor upstream route-map upstream-out out
 exit-address-family
!
bgp community-list expanded announce-to-customer permit _645XX:4[1357]000
bgp community-list expanded announce-to-peering permit _645XX:4[2367]000
bgp community-list expanded announce-to-upstream permit _645XX:4[4567]000
bgp community-list expanded my-communities permit _645XX:.*
bgp large-community-list expanded my-largecommunities permit _645XX:.*:.*
!
route-map upstream-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map upstream-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
 on-match next
!
route-map upstream-in permit 100
 set community 645XX:41000 additive
 set extcommunity rt 645XX:21000
 set large-community 645XX:2:1000 additive
 set local-preference 10
!
route-map peering-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map peering-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
 on-match next
!
route-map peering-in permit 100
 set community 645XX:41000 additive
 set extcommunity rt 645XX:23000
 set large-community 645XX:2:3000 additive
 set local-preference 1000
!
route-map customer-in permit 50
 match community my-communities
 set comm-list my-communities delete
 on-match next
!
route-map customer-in permit 60
 match large-community my-largecommunities
 set large-comm-list my-largecommunities delete
 on-match next
```

```
!
route-map customer-in permit 100
 set community 645XX:47000 additive
 set extcommunity rt 645XX:24000
 set large-community 645XX:2:4000 additive
 set local-preference 10000
!
route-map customer-out permit 100
 match community announce-to-customer
!
route-map peering-out permit 100
 match community announce-to-peering
!
route-map upstream-out permit 100
 match community announce-to-upstream
!
route-map own-networks permit 100
 set community 645XX:47000
!
line vty
!
end
```

C Slides

Setting Maximum-Prefix

- You can set *max-prefix*
  - for a whole *peer-group* or
  - for each individual BGP peer
- you have to set it separately for each *address family* (in our case IPv4 and IPv6)

```
configure

router bgp 645xx
 address-family ipv4
  neighbor peering maximum-prefix 100 80 restart 1
```

Parameters here are:

- shut down session when more then **100** IPv4 prefixes are received
- give a warning at **80%** (= 80 prefixes in this case)
- wait **1 minute** before re-establishing the session

Show commands:

- **show bgp ipv4 summary**
  in case max prefix is triggered the session is down with status *PfxCT*

BGP Session Password

- Talk to your neighbor
- agree upon a password
- configure the password on the BGP session between you

```
configure

router bgp 645xx
 neighbor 80.81.192.1yy password some-password-here
```

Show commands:

- **show bgp ipv4 summary**
- **show bgp ipv4 neighbor 80.81.192.1yy** - should show “Peer Authentication Enabled” at the end

TTL Security

- Using TTL security BGP TCP packets only a configurable number of hops away will be allowed.
- This parameter has to be configured on both peers.

```
configure

router bgp 645xx
  neighbor 80.81.192.1yy ttl-security hops 1
```

Show commands:

- **show bgp ipv4 summary**
- **show bgp ipv4 neighbor 80.81.192.1yy** - should show "*External BGP neighbor may be up to 1 hops away*"

IXP LAN Announcement - Demonstration

- Never accept BGP announcements of prefixes representing IXP LANs you are connecting to
- Even more important: No more-speficic announcements inside these LANs.

Show commands:

- **show ip route 80.81.192.0**
- **show ip route 80.81.192.1**
- **show bgp ipv4 summary**

RFD (Route Flap Dampening)

- Dampening stops further propagation of flapping routes
- Try default values first

```
router bgp 645xx
  bgp dampening
```

Show commands:

- show bgp ipv4 unicast dampening parameters
- show bgp ipv4 unicast dampening dampened-paths
- show bgp ipv4 unicast dampening flap-statistics
- show bgp ipv4 129.13.0.0/16
- show bgp ipv4 192.0.2.0/24
- show bgp ipv4 community 645*xx*:23000

RFD with adjusted parameters

- Default parameters are too aggressive
- Start dampening later (threshold at least 6000)

```
router bgp 645xx
  bgp dampening 10 750 12000 45
```

Do a "*show bgp ipv4 unicast dampening parameters*" and match values to the configured values above.

Show commands:

- show bgp ipv4 unicast dampening parameters
- show bgp ipv4 unicast dampening dampened-paths
- show bgp ipv4 unicast dampening flap-statistics
- show bgp ipv4 129.13.0.0/16
- show bgp ipv4 192.0.2.0/24
- show bgp ipv4 community 645*xx*:23000