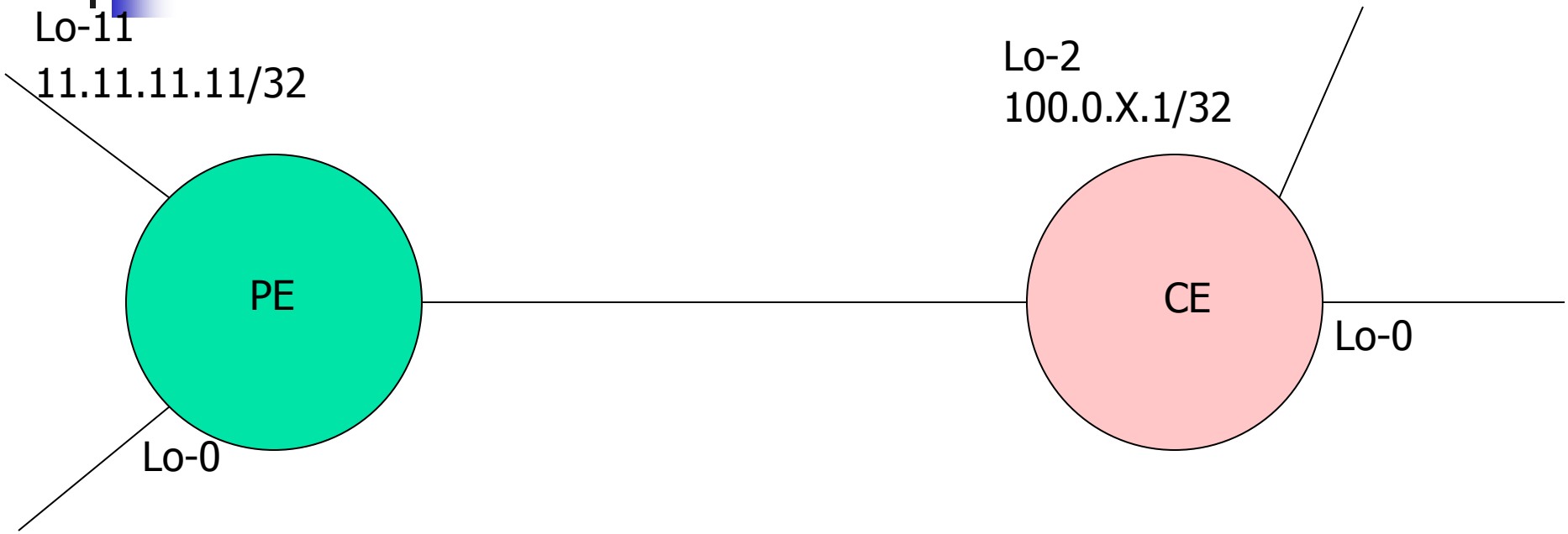
ISP and NSP Security Workshop

APRICOT 2013

Source based RTBH

S/RTBH



Destination Based RTBH

- Requires knowledge of the target (victim) address/network.
- Willingly sacrifices (black-holes) the communication of the target with the rest of the world.
- Relies on BGP to "signal" black-hole from trigger to one or more enforcers – usually edge routers in the network.
- Uses unreachable next-hop to drop packets to the destination

Source Based RTBH

- Requires knowledge of the attack sources
- Attack sources are unable to communicate with the entire protected infrastructure, not only the intended victims.
- Relies on BGP to "signal" black-hole from trigger to one or more enforcers- usually edge routers in the network.
- Uses Unicast Reverse Path Forwarding(uRPF) to drop packets.

PE Configuration

- Configure the Loopback-11 with the ip address.
- 11.11.11.11 255.255.255.255
- Eg.
  - PE(config)# interface loopback11
  - PE(config-if)#ip address 11.11.11.11 255.255.255.255

Announced the loopback-11 via BGP

Eg. Router bgp <ASN>

PE(config-router)network 11.11.11.11 mask 255.255.255.255

CE Configuration

- remove the community from 100.0.<router-id>.1/32 and add the trigger for 11.11.11.11/32.
- Add the route-map

```
ip community-list standard RTBH-Trigger permit 666:666

route-map RTBH-Trigger permit 10
 match tag 666
 set community 666:666
!
route-map RTBH-Trigger permit 99
!

route-map UseRTBH permit 10
 match community RTBH-Trigger
 set ip next-hop 192.0.2.1
!
route-map UseRTBH permit 99
```

CE Configuration

Eg.

CE-router#

router bgp <ASN>

no network 100.0.X.1 mask 255.255.255.255 route-map Loopback2-RTBH

network 100.0.X.1 mask 255.255.255.255

redistribute static route-map RTBH-Trigger

!

ip route 11.11.11.11 255.255.255.255 Null0 tag 666

Check the Victim Source

```
PE#sh ip bgp 11.11.11.11
BGP routing table entry for 11.11.11.11/32, version 25
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
     1         2
  81
    192.0.2.1 from 10.0.18.6 (192.168.31.1)
      Origin incomplete, metric 0, localpref 100, valid, external
      Community: 666:666
  Local
    0.0.0.0 from 0.0.0.0 (10.0.18.251)
      Orig
```

Ping with Source loopback11 from PE

PE#ping 100.0.X.1 source lo11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 100.0.X.1, timeout is 2 seconds:

Packet sent with a source address of 11.11.11.11

.....

Success rate is 0 percent (0/5)

Ping with Source loopback0 from PE

PE#ping 100.0.X.1 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.X.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.18.251
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/101/232 ms
PE#

Debug on CE and re-run the ping.

CE:

access-list 100 permit icmp any any echo

access-list 100 permit icmp any any echo-reply

CE-Router#debug ip packet 100

PE#ping 100.0.X.1 source lo11 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 100.0.X.1, timeout is 2 seconds:
Packet sent with a source address of 11.11.11.11
.
Success rate is 0 percent (0/1)
PE#

CE#debug ip packet 100
IP packet debugging is on for access list 100
Router31#
*Feb 21 12:37:14.959: IP: tableid=0, s=11.11.11.11 (Ethernet1/0), d=100.0.X.1 (Loopback2), routed via RIB
*Feb 21 12:37:14.959: IP: s=11.11.11.11 (Ethernet1/0), d=100.0.X.1, len 100, rcvd 4
*Feb 21 12:37:14.963: IP: tableid=0, s=100.0.X.1 (local), d=11.11.11.11 (Null0), routed via RIB
*Feb 21 12:37:14.967: IP: s=100.0.X.1 (local), d=11.11.11.11 (Null0), len 100, sending
CE#

Use uRPF

PE

interface Ethernet X/X

description Link to CE-X e X/X

ip address X.X.X.Y 255.255.255.252

ip verify unicast source reachable-via any

PE#ping 100.0.X.1 source lo11 repeat 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 100.0.X.1, timeout is 2 seconds:
Packet sent with a source address of 11.11.11.11
.
Success rate is 0 percent (0/1)
PE#