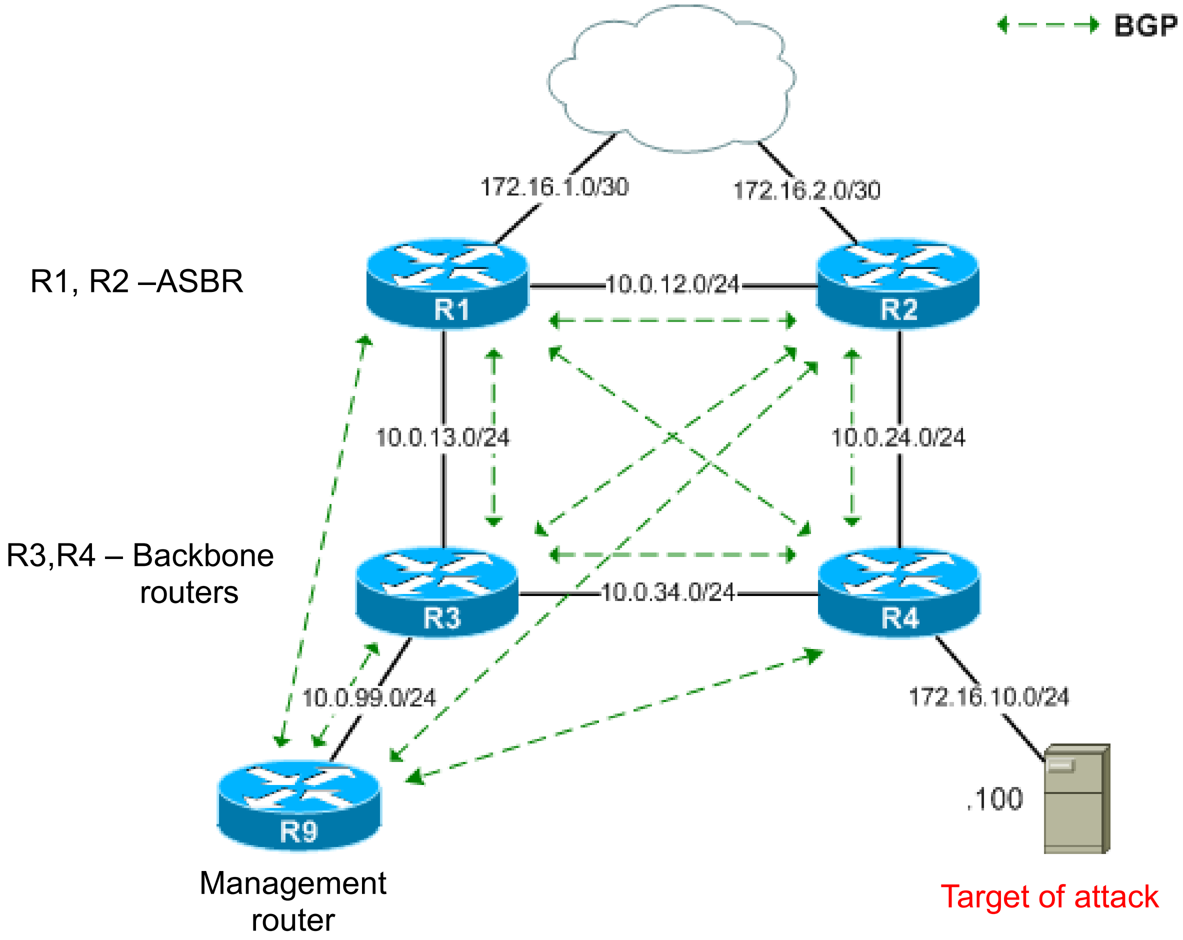
____________________ ____________________

Date Name

Application of BGP-4 - using RTBH



Instructions

1. Cable the network as shown in the diagram.
2. Implement BGP as shown.

Objectives

1. Prepare and activate defence against DDoS attack against internal target using RTBH.

Prologue

- We anticipate sacrificing the target in advance.
- We will save the rest of the network, especially the infrastructure.
- Preliminary preparation of defense - starting points.
  - Routers configuration.
  - Static paths, including the tag parameter, can be distributed via BGP4.
- Defence activation in case of attack.
  - Detected IP address of the attack victim.

  - A static routing record (path) is created manually, diverting traffic instead of destination to an black hole (Null0) on a management router.
  - This path is immediately distributed (injected) to all ASBRs using BGP4.

Hints

1. Black hole preparation.
   - Create a static route in all ASBRs, for example.
     ```
     R1 (config) # ip route 192.0.2.1 255.255.255.255 Null0
     ```
   - Data sent to 192.0.2.1/32 will be forwarded to Null0, i.e. discarded immediately.
   - The particular address is not important (the range selected for Test-Net is selected here, see RFC 3330).
2. Create a route-map on a management router for future redistribution of tagged static route with modified next hop address value.
3. Enable redistribution of static path to BGP4 using route map on a management router.

Attack occured!

1. Create static route pointing to the attack target management router, next hop will be Null0.
2. That route cannot be directly propagated to ASBRs due to the formally incorrect item of the Null0 next hop. Therefore, tag (i.e. 666) should be added to ensure that the route map redistributes that route with the modified next hop address.

Conclusions

- Unfortunately, the victim is now unavailable.
- The infrastructure is protected against overload.