Unaprjeđenje sigurnosti u mrežama pružatelja usluga

Miroslav Šimić

miroslav.simic@snt.hr

CCIE #19429

20. i 21. ožujka 2008.
Hotel Dubrovnik Palace
Dubrovnik

Welcome to the Human Network.

Agenda

- Zaštita mrežne infrastrukture
- Zaštita na rubovima mreže
- Uočavanje i sprječavanje napada

Agenda

- **Zaštita mrežne infrastrukture**
- **Zaštita na rubovima mreže**
- **Uočavanje i sprječavanje napada**

Gašenje nepotrebnih servisa

- **CDP:**

  Globalno na cijelom uređaju
  router(config)# **no cdp run**

  Na pojedinom sučelju
  router(config-if)# **no cdp enable**

- **Directed Broadcast (SMURF napad):**

  router(config-if)# **no ip directed-broadcast**
  U verziji IOS-a 11.2 i kasnijim verzijama ta je funkcionalnost isključena.

Gašenje nepotrebnih servisa

- **Finger:**
  Prije 12.1(5) i 12.1(5)T bio je uključen
  router(config)# **no service finger**
  Nakon 12.1(5) i 12.1(5)T je isključen. Ako ga treba isključiti:
  router(config)# **no ip finger**

- **Maintenance Operations Protocol (MOP)**
  router(config-if)# **no mop enabled**

- **HTTP Server**
  Isključen je. Ako ga treba isključiti:
  router(config)# **no ip http server**

Gašenje nepotrebnih servisa

- **IP BOOTP Server**

  router(config)# **no ip bootp server**

- **IP Redirects**

  router(config-if)# **no ip redirects**

- **IP Source Routing**

  router(config)# **no ip source-route**

Gašenje nepotrebnih servisa

- **PAD**

  router(config)# **no service pad**

- **Proxy ARP**

router(config-if)# **no ip proxy-arp**

- **Ident**

router(config)# **no ip identd**

- **TCP i UDP small servers**

  echo, chargen, daytime and discard services
  router(config)# **no service tcp-small-servers**
  router(config)# **no service udp-small-servers**

Implementacija korisnih alata i servisa

- Authentication, authorization, and accounting (AAA)
- Praćenje i spremanje konfiguracija
- Logiranje poruka – Syslog
- Network Time Protocol (NTP)
- Out-of-band pristup uređajima

Osnovne tehnike za zaštitu mreže

- **Input Queues**

router(config-if)# **hold-queue 1500**

- **ICMP Unreachable**

router(config-if)# **no ip unreachables**

router(config)# **ip icmp rate-limit unreachable [df] milliseconds**

router(config)# **mls rate-limit unicast ip icmp unreachable**

(SUP720 – hardware based rate limit)

- **Scheduler allocation**

router(config)# **scheduler interval 500**

router(config)# **scheduler allocate 4000 1000**

Osnovne tehnike za zaštitu mreže

- **“Skrivanje mreže”**
  MPLS VPN – MPLS Core je sakriven, korisnik ima pristup samo PE usmjerniku

  Router(config)# **no mpls ip propagate-ttl [forwarded | local]**

Kontrola prometa koji pristupa procesoru

- **Control Plane Policing - COPP**
  - –Usmjerivački protokoli
  - –Upravljački promet – telnet, SSH, SNMP
  - –Promet koji kao odredište ima IP adresu koja se nalazi na samom uređaju
  - –Razni drugi prometi – ICMP, IP Options

Kontrola prometa koji pristupa procesoru

- **Centralizirani COPP**

  router(config)# **control-plane**
  router(config-<<???>>)# **service-policy {input | output} service_policy_name**

- **COPP na distribuiranim platformama**

  12000
  router(config)# **control-plane**
  router(config-<<???>>)# **service-policy input service_policy_name**
  router(config)# **control-plane slot slot_number**
  router(config-<<???>>)# **service-policy input service_policy_name**

  Sup 720
  router(config)# **mls qos**
  router(config)# **control-plane**
  router(config-<<???>>)# **service-policy input service_policy_name**
  router(config)# **mls qos protocol arp police bps**

Kontrola prometa koji pristupa procesoru

- **Receive Access Control List**

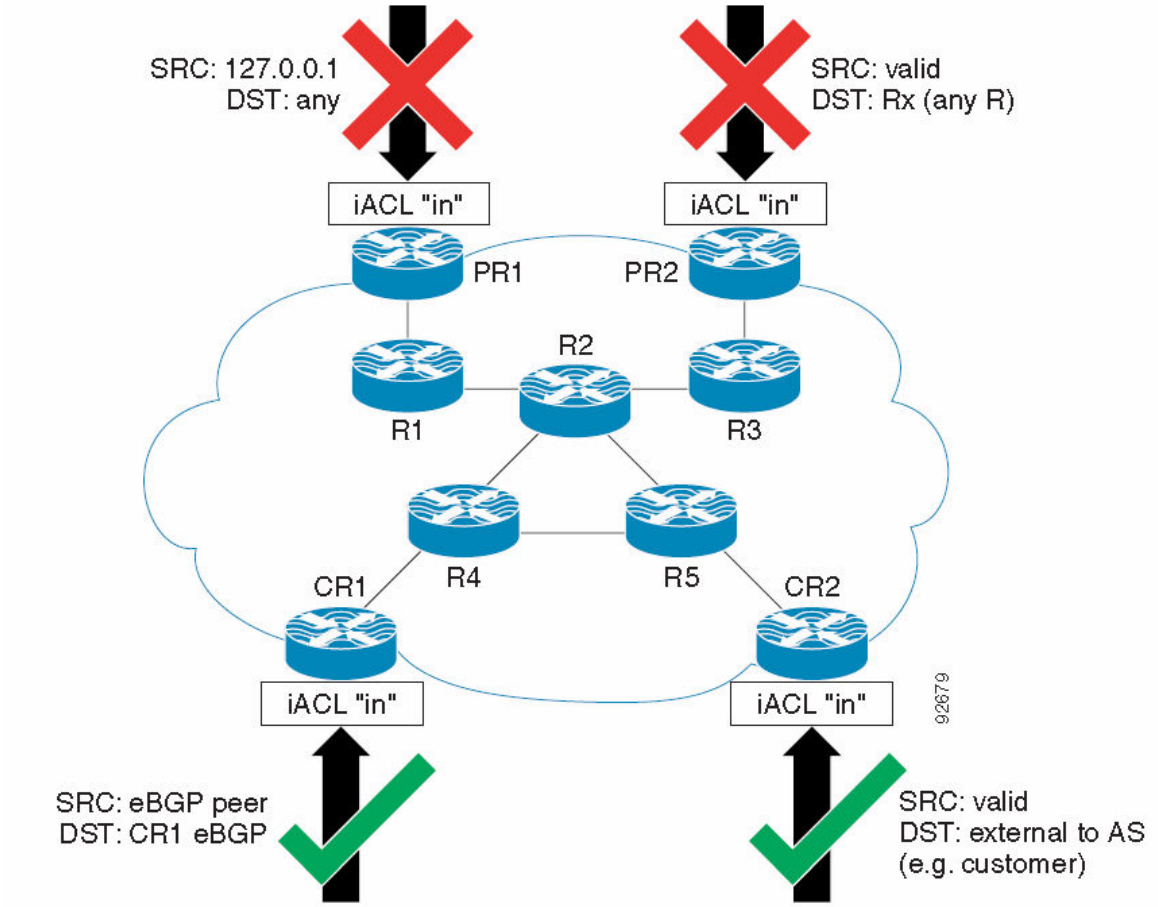
  router(config)# **ip receive access-list num**

Agenda

- Zaštita mrežne infrastrukture
- **Zaštita na rubovima mreže**
- Uočavanje i sprječavanje napada

Zaštita na rubovima mreže

- **Infrastructure Protection Access Control Lists – iACL**



Zaštita na rubovima mreže

1. Dio

! Deny your infrastructure space as a source of external packets
access-list 101 deny ip your_public_infrastructure_block any
! Deny src addresses of 0.0.0.0 and 127/8 (special useIPv4 addresses)
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
! Deny RFC1918 space from entering AS
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.15.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any

Zaštita na rubovima mreže

2. dio

! Permit eBGP session
access-list 101 permit tcp host bgp_peer host local_ip eq 179
access-list 101 permit tcp host bgp_peer eq 179 host local_ip
! Permit OSPF
access-list 101 permit ospf host ospf_neighbour host 224.0.0.5
! Permit DR multicast address, if needed
access-list 101 permit ospf host ospf_neighbour host 224.0.0.6
access-list 101 permit ospf host ospf_neighbour host local_ip

3. dio

! Deny all other access to infrastructure
access-list 101 deny ip any your_public_infrastructure_block

4. dio

! Permit transit traffic (ISP).

access-list 101 permit ip any any

Zaštita na rubovima mreže

- **Filtriranje prometa od korisnika**

```
! Permit eBGP session
access-list 101 permit tcp host bgp_peer host local_ip eq 179
access-list 101 permit tcp host bgp_peer eq 179 host local_ip
! Permit OSPF
access-list 101 permit ospf host ospf_neighbour host 224.0.0.5
! Permit DR multicast address, if needed
access-list 101 permit ospf host ospf_neighbour host 224.0.0.6
access-list 101 permit ospf host ospf_neighbour host local_ip
! Deny access to infrastructure
access-list 101 deny ip any your_public_infrastructure_block
! Permit transit traffic (ISP).
access-list 101 permit ip user_address_block any
! Deny any other traffic.
access-list 101 deny ip any any
```

Agenda

- Zaštita mrežne infrastrukture
- Zaštita na rubovima mreže
- **Uočavanje i sprječavanje napada**

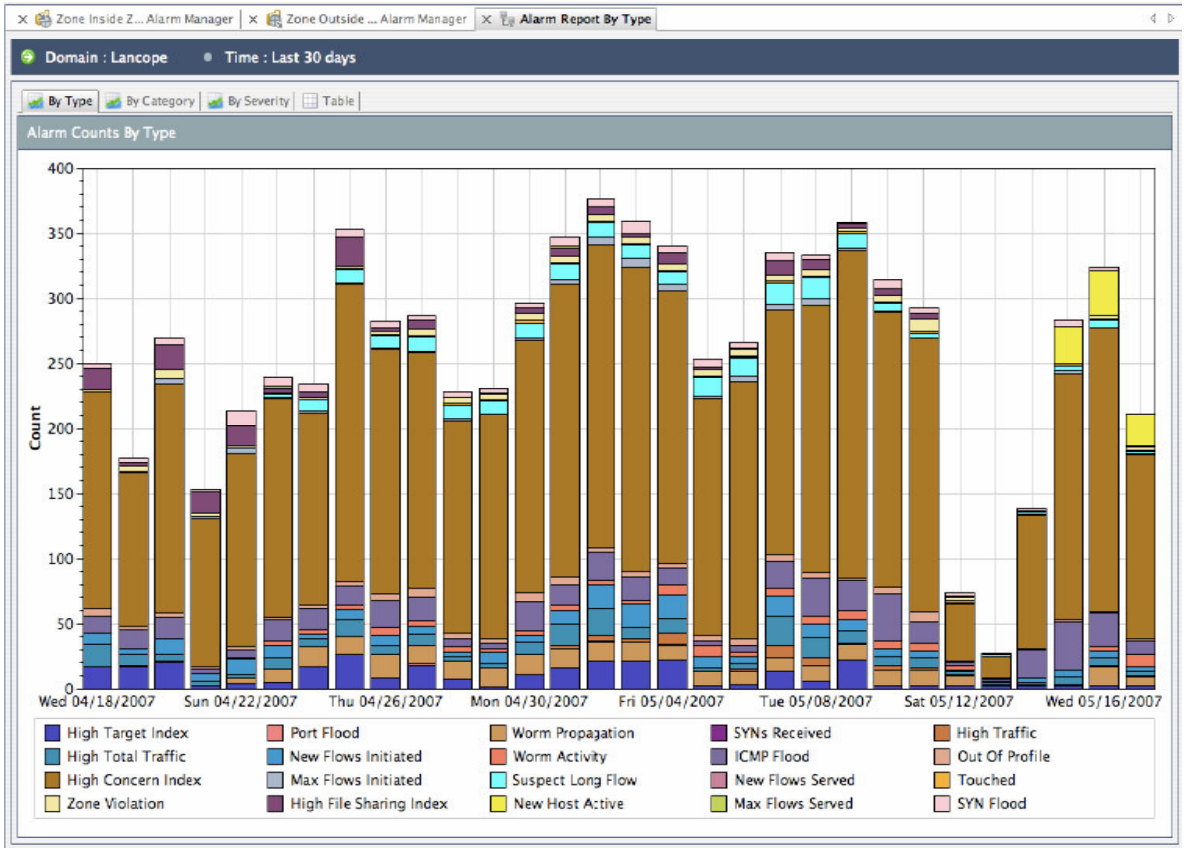
Uočavanje i sprječavanje napada

- **ACL**

```
Extended IP access list 169
        permit icmp any any echo (2 matches)
        permit icmp any any echo-reply (21374 matches)
        permit udp any any eq echo
        permit udp any eq echo any
        permit tcp any any established (150 matches)
        permit tcp any any (15 matches)
        permit ip any any (45 matches)
```

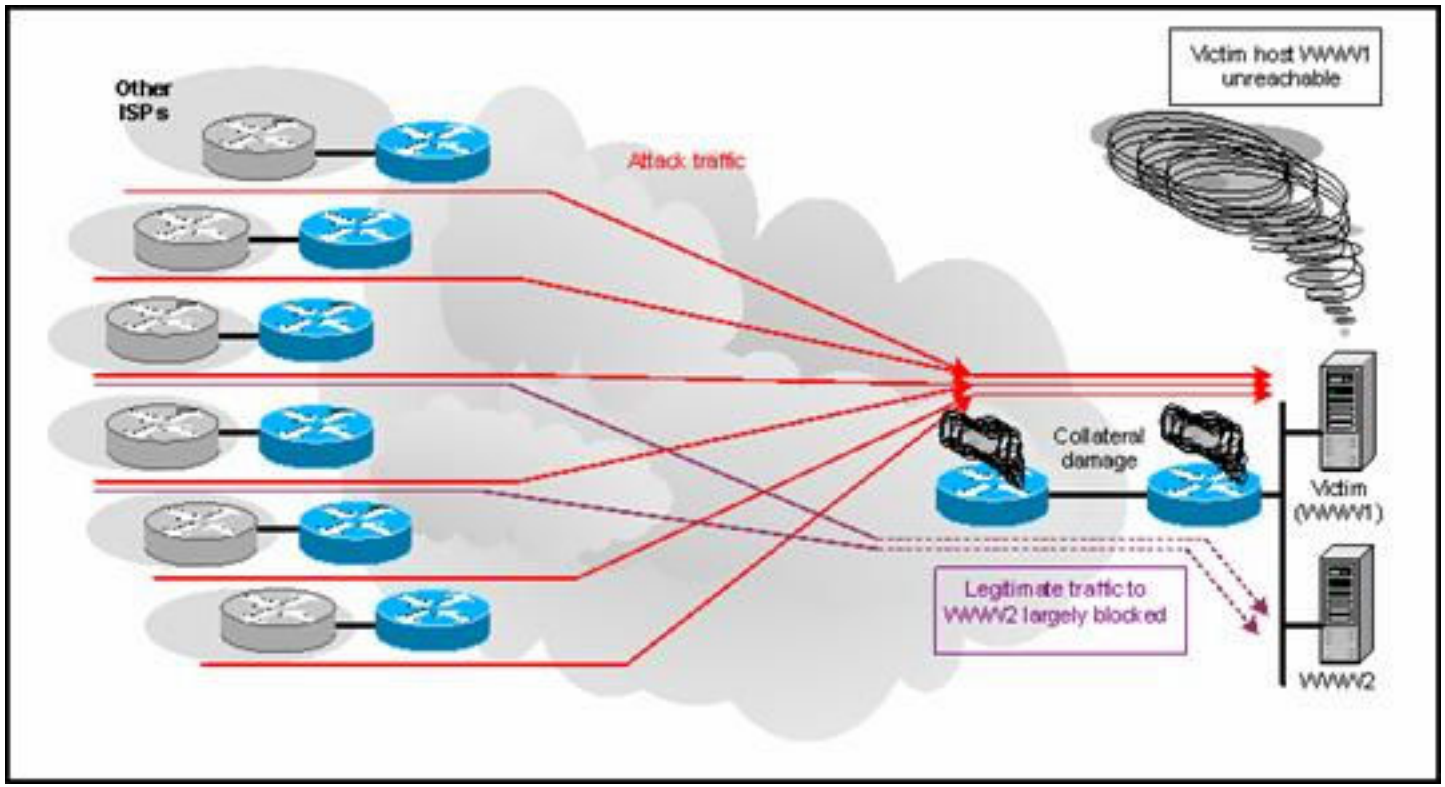
Uočavanje i sprječavanje napada

- **Netflow**



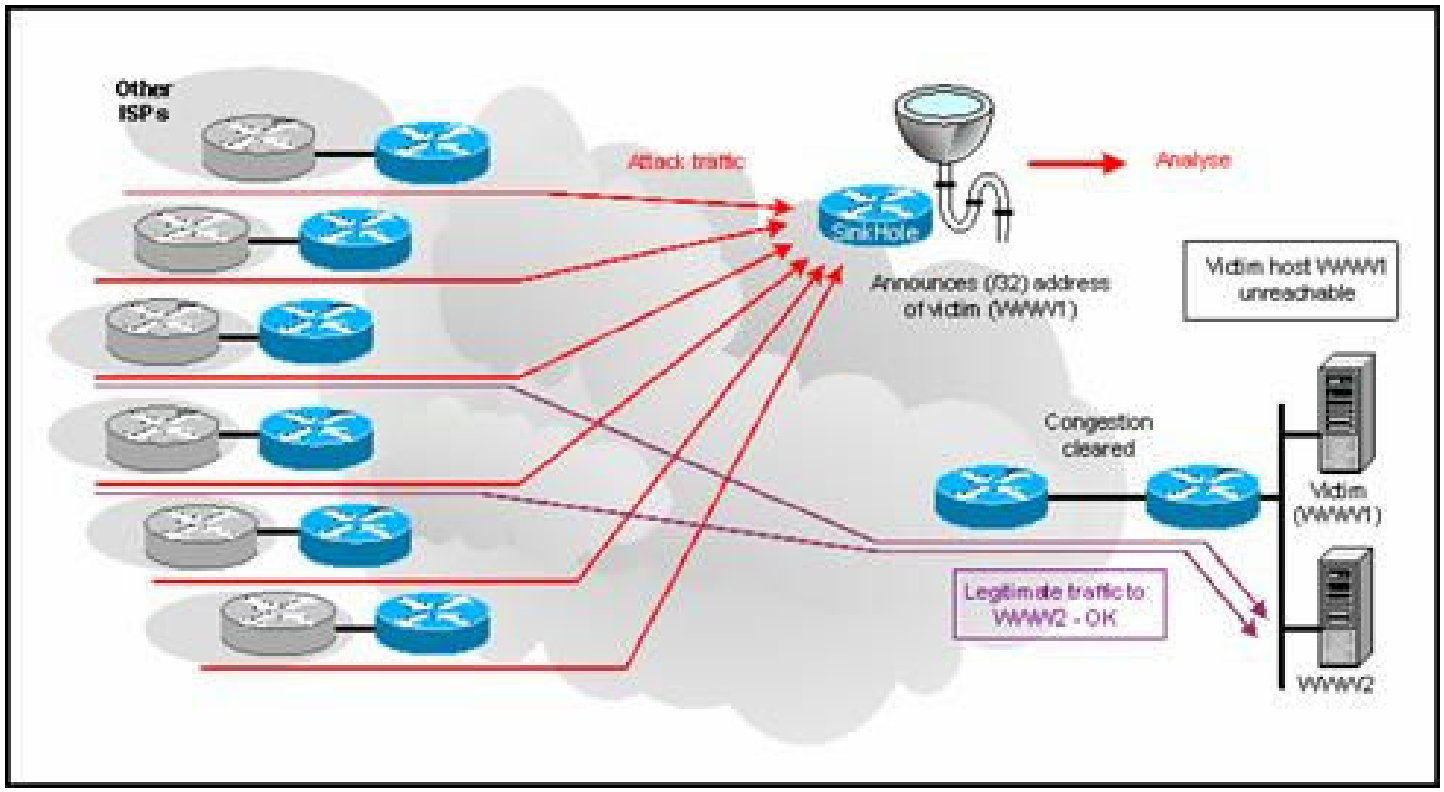
Uočavanje i sprječavanje napada

- Sink Holes



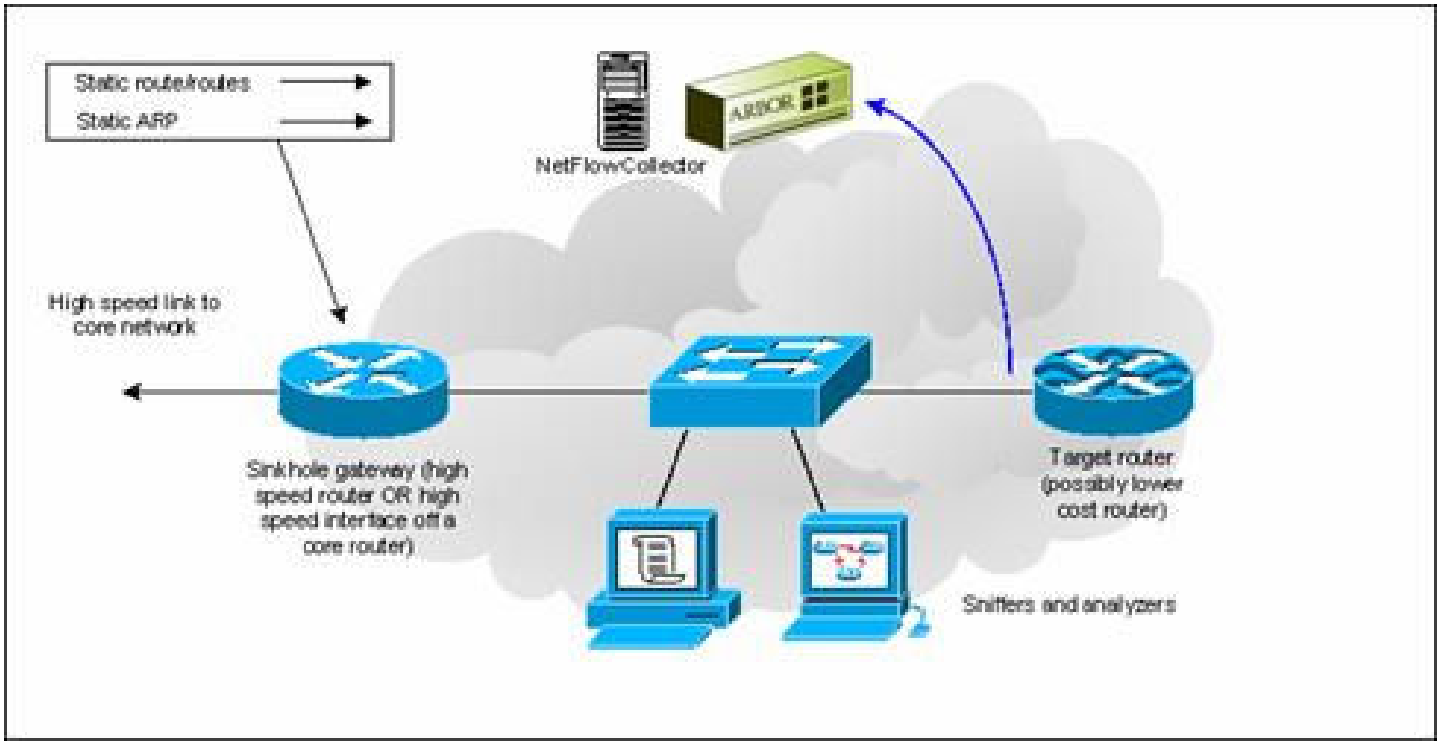
Uočavanje i sprječavanje napada

- Sink Holes



Uočavanje i sprječavanje napada

- **Sink Holes**



Uočavanje i sprječavanje napada

- **Sink Holes**

```
! Static route to 96.0.0.0 /3 network
ip route 96.0.0.0 63.255.255.255 192.0.2.200
!
...
!
ip arp 192.0.2.200 00.00.0c.12.34.56 arpa
!
```

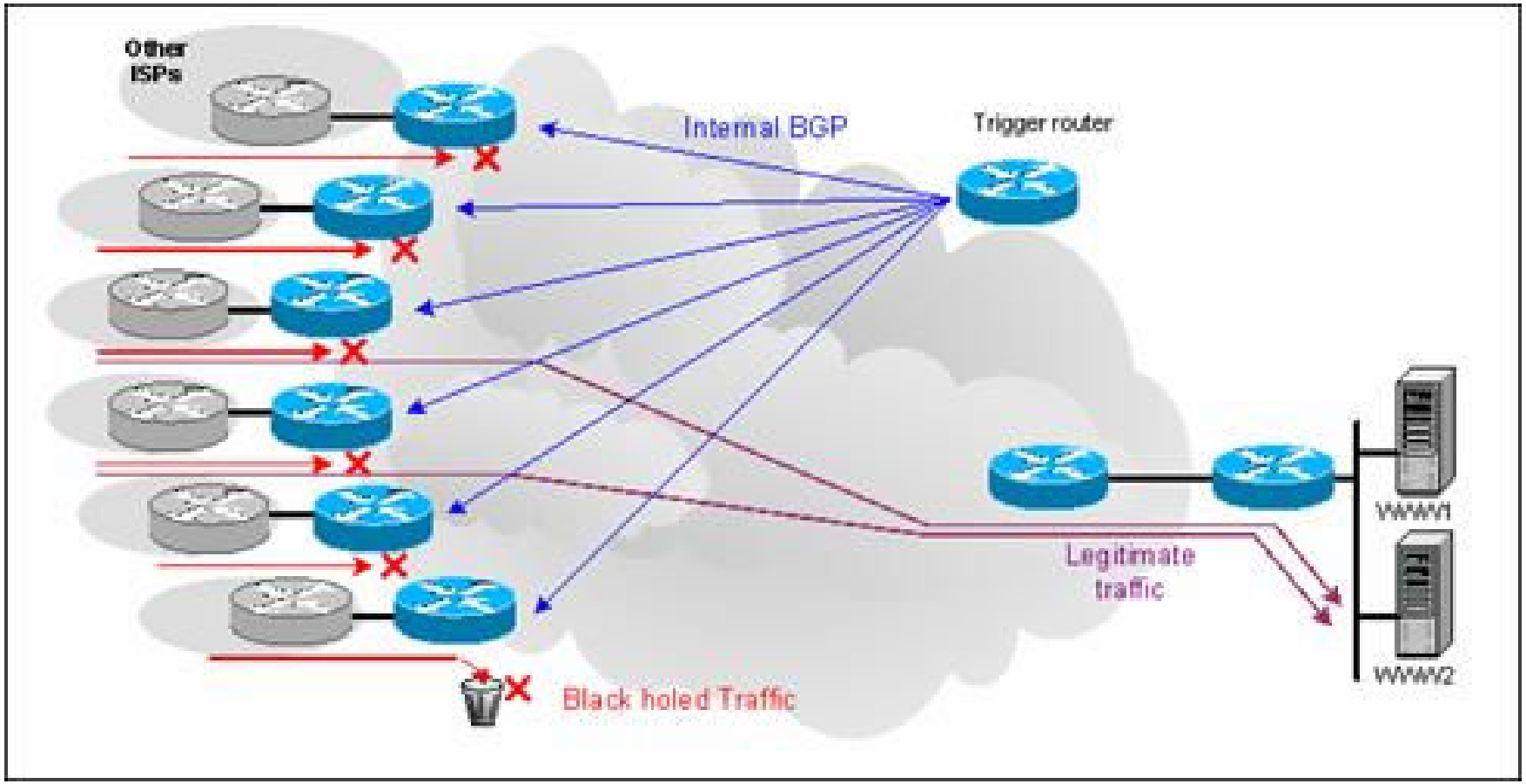
Uočavanje i sprječavanje napada

- **Black Holes**

  ip route 171.xxx.xxx.1 255.255.255.255 Null0

Uočavanje i sprječavanje napada

- Remote trigered Black Hole



Uočavanje i sprječavanje napada

- **Remote trigered Black Hole –**
  preusmjeravanje po odredišnoj adresi

Svi ruteri:
ip route 192.0.2.0 255.255.255.0 Null0

Uočavanje i sprječavanje napada

- **Remote trigered Black Hole –**

  preusmjeravanje po odredišnoj adresi

Ruter sa kojega se oglašava ruta:

```
 router bgp 999
...
redistribute static route-map STATIC-TO-BGP
!
route-map STATIC-TO-BGP permit 10
match tag 66
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export 999:000
!
Route-map STATIC-TO-BGP permit 20
!
ip route 171.xxx.xxx.1 255.255.255.255 Null0 Tag 66
!
```

Uočavanje i sprječavanje napada

- **Remote trigered Black Hole –**
  preusmjeravanje po source adresi (Unicast Reverse Path Forwarding (uRPF) Loose mode)

Svi ruteri:

```
!
interface FastEthernet2/0
ip address 192.xxx.xxx.50 255.255.255.0
ip verify unicast source reachable-via any
...
speed 100
full-duplex
!
```

Uočavanje i sprječavanje napada

- **Remote trigered Black Hole –**

  preusmjeravanje po source adresi

Ruter sa kojega se oglašava ruta:

```
 router bgp 999
...
redistribute static route-map STATIC-TO-BGP
!
route-map STATIC-TO-BGP permit 10
match tag 66
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export 999:000
!
Route-map STATIC-TO-BGP permit 20
!
ip route 171.xxx.xxx.1 255.255.255.255 Null0 Tag 66
!
```

Uočavanje i sprječavanje napada

- Cisco Traffic Anomaly Detector Module
- Cisco Anomaly Guard Module

Miroslav Šimić, dipl. ing.
miroslav.simic@snt.hr
CCIE #19429

www.snt-world.com