Informacja dla klientów pozwalająca na zrozumienie zagrożeń cyberbezpieczeństwa

W celu zapewnienia optymalnej konfiguracji kompatybilnej z wymaganiami technicznymi węzła EPIX wraz z niezbędnymi zabezpieczeniami uczestnik powinien posiadać odpowiednią konfigurację interfejsów, sesji BGP oraz vlanów zgodnie z poniższymi zaleceniami.

1. RPF – Reverse Path Filter (powinno być wyłączone na interfejsie)

2. W porcie powinien być widoczny tylko jeden mac address routera klienta

3. Interfejs powinien mieć wyłączony promisc mode

4. IP spoofing jest niedozwolony w vlanie openpeeringowym (prosimy o odfiltrowanie ruchu wychodzącego w kierunku vlana openpeeringowego z ograniczeniem do własnych klas adresowych)

5. Router musi mieć wyłaczone IPv6 RA na interfejsie.

6. Ruch typu link-local nie jest dozwolony, za wyjątkiem ruchu ARP oraz IPv6 ND

7. Akceptowane MTU na vlanach openpeeringowych wynosi 1500.

8. Sieci należące do openpeeringu nie są rozgłaszane przez BGP
– dlatego aby mieć dostęp np. do zapytań icmp z sieci która nie jest siecią openpeeringową jako źródło zapytania należy po swojej stronie odpowiednio rozgłosić sieć typu connected z routera do wewnątrz własnej sieci.

9. Dozwolone ethertype w openpeeringu:
– 0x0800 – IPv4
– 0x0806 – ARP
– 0x86dd – IPv6

10. Filtrowany i niedozwolony ruch w ramach dopuszczonych ethertype:
– IRDP
– ICMP redirects
– IEEE 802 Spanning Tree
– Discovery protocols: CDP, EDP, LLDP
– VLAN/trunking protocols: VTP, DTP
– Protokoły routingu oparte na rozgłoszeniach broadcastowych takie jak (e.g. OSPF, ISIS, IGRP, EIGRP)
– BOOTP/DHCP
– PIM-SM
– PIM-DM
– DVMRP
– ICMPv6 ND-RA
– UDLD
– L2 Keepalives
– Multicast (za wyjątkiem IPv6 ND)

11. W przypadku naduzyć celowego lub niecelowego działania które doprowadzi np. do:
BGP hijack

Amplifikacji DNS
Floodów różnego rodzaju jak np. (Broadcast, Multicast flood)
HTTP flood
Amplifikacji NTP
UDP flood
ICMP flood
Naduzyć związanych z wykorzystaniem SSDP
Amplifikacji Memcached

EPIX może wyłączyć port uczestnika openpeeringu.

Zalecana konfiguracja (Linux router):

Wyłączenie ip redirects / proxy arp / reverse path filtering

for i in /proc/sys/net/ipv4/conf/*/accept_redirects; do echo 0 > $i; done
for i in /proc/sys/net/ipv4/conf/*/send_redirects; do echo 0 > $i; done
for i in /proc/sys/net/ipv4/conf/*/accept_source_route; do echo 0 > $i; done
for i in /proc/sys/net/ipv4/conf/*/proxy_arp; do echo 0 > $i; done
for i in /proc/sys/net/ipv4/conf/*/secure_redirects; do echo 1 > $i; done
for i in /proc/sys/net/ipv4/conf/*/bootp_relay; do echo 0 > $i; done
for i in /proc/sys/net/ipv4/conf/*/arp_filter; do echo 1 > $i; done
for i in /proc/sys/net/ipv4/conf/*/arp_ignore; do echo 1 > $i; done
for i in /proc/sys/net/ipv4/conf/*/arp_announce; do echo 2 > $i; done
for i in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 0 > $i; done

Uwaga:

for i in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 0 > $i; done
W przypadku takiego ustawienia stajemy się poddatni na “ip spoofing” – dlatego powyższe ustawienie powinno być zabezpieczone dodatkowo firewallem (np. iptables chain FORWARD)
Innym ustawieniem które zapewni nam ochronę przed “ip spoofingiem” jest (RP Filter w Loose Mode):
for i in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 2 > $i; done
* powyższe ustawienia zależą od konfiguracji Waszego routera oraz wymagaja precyzyjnej wiedzy dotyczącej tego jak wyglada ip routing na routerze.

W przypadku systemu Linux należy także zwiększyć parametry dotyczące maksymalnej ilości wpisów w arp-cache:
sysctl -w net.ipv4.neigh.default.gc_thresh1=1024
sysctl -w net.ipv4.neigh.default.gc_thresh2=2048
sysctl -w net.ipv4.neigh.default.gc_thresh3=4096

sysctl -w net.ipv6.neigh.default.gc_thresh1=1024
sysctl -w net.ipv6.neigh.default.gc_thresh2=2048
sysctl -w net.ipv6.neigh.default.gc_thresh3=4096

IPv6 Router Advertisement
net.ipv6.conf.default.accept_ra=0
net.ipv6.conf.all.accept_ra=0

Dla poszczególnych interfejsów na których zestawione są sesje BGP do openpeeringu:
net.ipv6.conf.vlan4090.accept_ra=0
net.ipv6.conf.vlan992.accept_ra=0
– numery interfejsów i vlanów mogą się różnić w zależności od sposobu odbierania danej usługi

Zalecana konfiguracja (Cisco)

Parametry konfiguracji globalne:
no service dhcp
no ip bootp server
no service config
no cdp run

Parametry konfiguracji interfejsu na którym terminowany jest openpeering:

no ip redirects
no ip proxy-arp
no cdp enable
no ip directed-broadcast
no mop enable
duplex full
no keepalive
ipv6 nd suppress-ra

Dodatkowo w przypadku sesji BGP do openpeeringu wymagane jest ustawienie ‘no bgp-enforce-first-as” dla sesji BGP z routerami RS