

PROJEKT BGP BLACKHOLING PL

Łukasz Bromirski
lukasz@bromirski.net

bgp@networkers.pl

Projekt BGP Blackholing PL

<http://networkers.pl/bgp-blackholing>

- **Problem ataków DoS/DDoS**
- **Projekt BGP Blackholing PL**
co zrobić żeby się dołączyć?
- **Zastosowania BGP Blackholing w Twojej sieci**
- **Materiały**
- **Q&A**

PROBLEM DDoS



Typowy DDoS

<http://networkers.pl/bgp-blackholing>

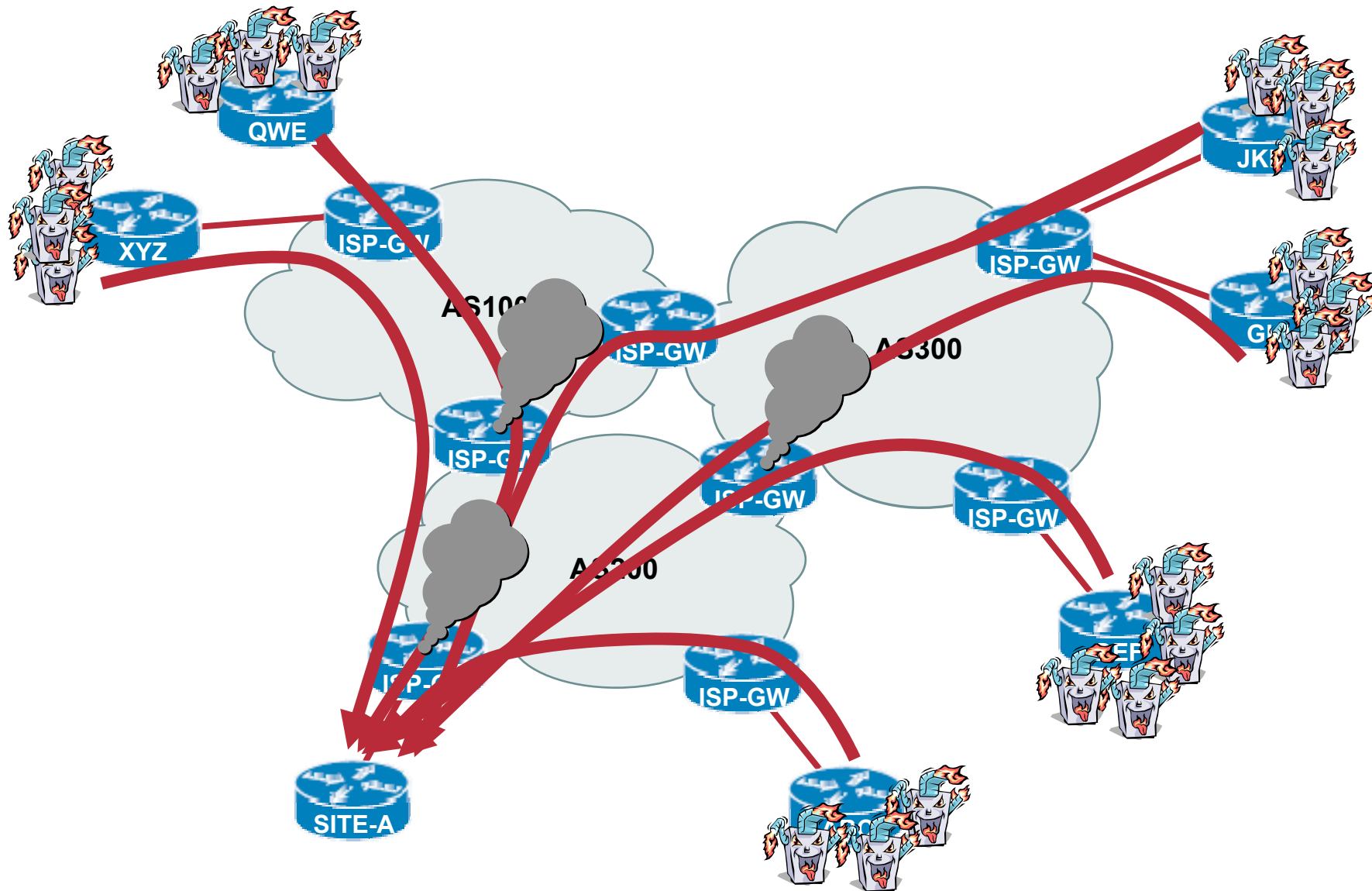
- **Setki/tysiące** trojanów-zombie (**BOTNET***)
- **Setki tysięcy** pakietów na sekundę
- **Wielusetmegabitowy/gigabitowy** strumień śmieci
- **Zatyka sukcesywnie kolejne wąskie gardła:**
 - styk(i) z Internetem źródła
 - styk(i) z Internetem atakowanego
 - sieć ISP
 - styki ISP z innymi ISP
 - „kto popsuł Internet?”

* <http://swatit.org/bots/index.html>

Typowy DDoS

Jak to się dzieje?

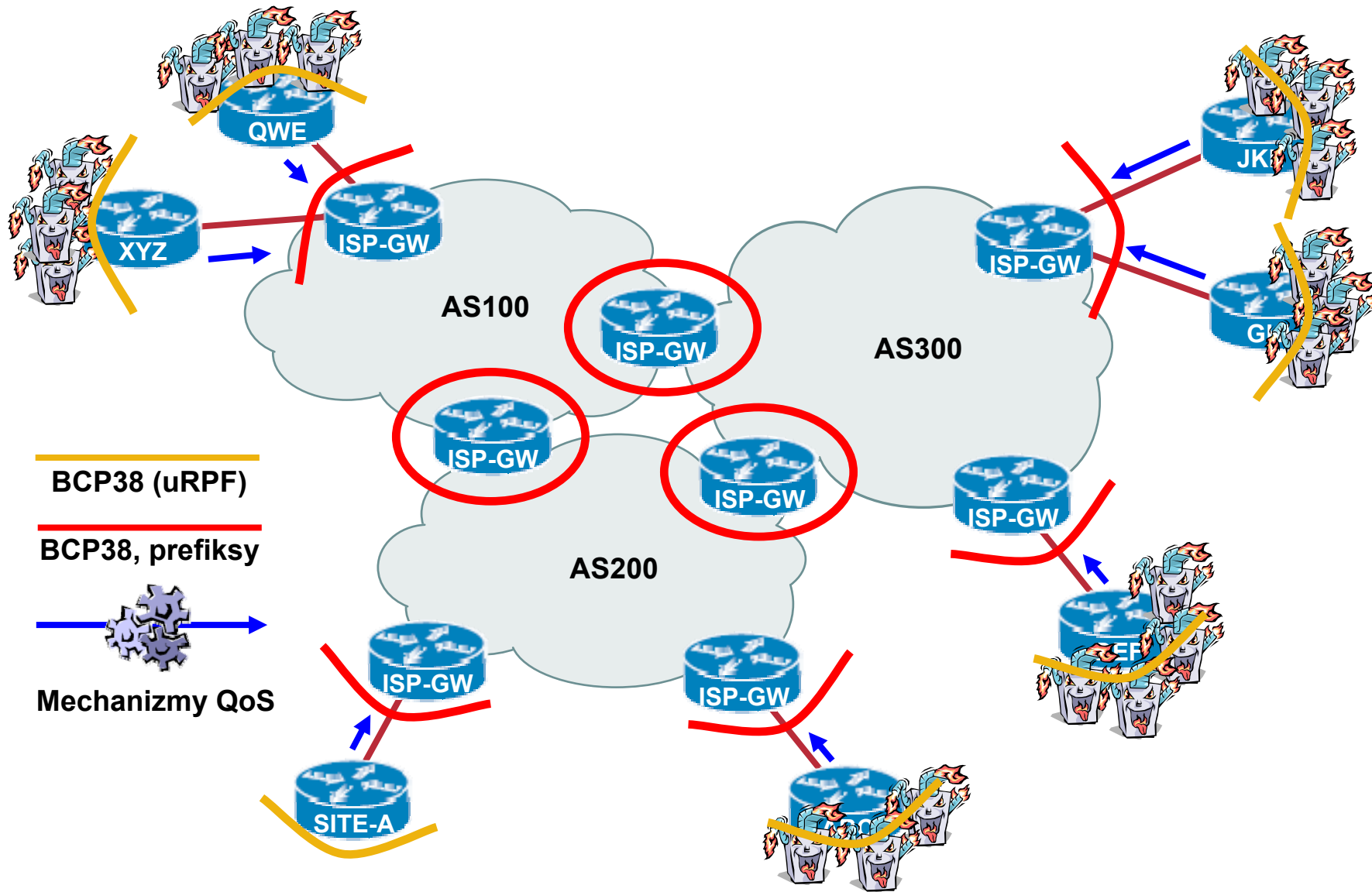
<http://networkers.pl/bgp-blackholing>



Typowy DDoS

Co ja mogę zrobić dla zwiększenia bezpieczeństwa?

<http://networkers.pl/bgp-blackholing>



Czego brakuje do walki z DoS/DDoS?

<http://networkers.pl/bgp-blackholing>

- **Wszelkiego rodzaju filtry wymagają interwencji ręcznej przy dowolnej zmianie ich zawartości**
 - bogon list – casus 83/8**
 - spoofed source – realnie brak możliwości**
 - atakowany host/podsieć – filtry zakładane lokalnie (efektywnie nic to nie zmienia)**
- **Rozwiązania dedykowane zwykle wymagają osobnej infrastruktury, którą trzeba utrzymywać**
 - ...i która może stać się celem ataku**
- **Wykorzystanie mechanizmów routingu daje możliwość wyjścia z filtrowaniem poza swoją sieć...**

PROJEKT BGP BLACKHOLING PL



BGP blackholing PL

O czym mówimy?

<http://networkers.pl/bgp-blackholing>

- Grupa entuzjastów różnego rodzaju zagadnień sieciowych
- Grupa route-serwerów
 - prefiksy bogon (nieprzydzielone przez IANA* i zarezerwowane)
 - opcja akceptowania prefiksów rozgłaszanych przez członków projektu
- Regulamin dostępny na WWW projektu
- Projekt oparty o dobrą wolę i wolny czas
 - brak jakichkolwiek gwarancji
- Analogia do projektu grupy Cymru
 - <http://www.cymru.com/BGP/bogon-rs.html>
 - my dodatkowo umożliwiamy rozgłaszanie własnych prefiksów

<http://www.iana.org/assignments/ipv4-address-space>

BGP blackholing PL

Czego będę potrzebował?

<http://networkers.pl/bgp-blackholing>

- **Cisco IOS**

oprogramowanie z BGP – IP Plus, ew. SP Services

<http://www.cisco.com/go/fn>

- **BSD/Linux**

Quagga (na BSD z patchem dla Null0*)

Dla OpenBSD/FreeBSD: OpenBGPd

- **Pozostałe platformy/systemy**

...zapytaj dostawcę – zwykle osobna licencja

* <http://lukasz.bromirski.net/projekty/quagga-null0.diff>

BGP blackholing PL

Czego będę potrzebował?

<http://networkers.pl/bgp-blackholing>

- Quagga/Zebra – patch do poprawnej obsługi **Null0**

```
--- quagga-0.99.1/zebra/zebra_rib.c
+++ quagga-0.99.1-blackhole/zebra/zebra_rib.c
@@ -405,6 +405,8 @@
     {
         SET_FLAG (nexthop->flags, NEXTHOP_FLAG_RECURSIVE);
         nexthop->rtype = newhop->type;
+         if (newhop->type == NEXTHOP_TYPE_BLACKHOLE)
+             nexthop_blackhole_add (rib);
         if (newhop->type == NEXTHOP_TYPE_IPV4 ||
             newhop->type == NEXTHOP_TYPE_IPV4_IFINDEX)
             nexthop->rgate.ipv4 = newhop->gate.ipv4;
```

* <http://lukasz.bromirski.net/projekty/quagga-null0.diff>

DOŁĄCZENIE DO BGP BLACKHOLING PL



BGP blackholing

Konfiguracja – z lotu ptaka

<http://networkers.pl/bgp-blackholing>

- **Zestawiamy sesje eBGP z naszymi route-serwerami**
zwykle dwie na każdy AS (członka projektu)
- **Sesje rozgłaszają prefiksy:**
typowe bogon oznaczone community **64999:666**
prefiksy członków oznaczone community **64999:999**
- **Prefiksy należy zaakceptować a następnie:**
za pomocą route-mapy skierować ruch do tych prefiksów do Null0 lub jego odpowiednika
można wykorzystać iBGP żeby rozgłosić prefiksy głębiej do swojej sieci, jeśli składa się z większej ilości routerów

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Definiujemy trasę na Null0:

```
ip route 192.0.2.1 255.255.255.255 Null0
```

- Definiujemy community-list pasującą do **64999:666** i osobną, pasującą do **64999:999**:

```
ip community-list 10 permit 64999:666
```

```
ip community-list 20 permit 64999:999
```

- Definiujemy prefix-listę, która odrzuci wszystkie prefiksy (potrzebne, jeśli nie chcesz rozgłaszać swoich prefiksów do route-serwerów projektu):

```
ip prefix-list 10 deny any
```

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- **Definiujemy route-mapę, która prefiksy oznaczone pasującymi community skieruje do Null0:**

```
route-map BGP-BH-PL permit 10
  match community 10
  set ip next-hop address 192.0.2.1
! jeśli chcesz odrzucać również prefiksy rozgłaszane
! przez innych członków projektu:
route-map BGP-BH-PL permit 20
  match community 20
  set ip next-hop address 192.0.2.1
```

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- Konfigurujemy sesje z route-serwerami projektu BGP Blackholing PL:

```
router bgp <Twój_numer_AS>
  neighbor <IP_rs_1> remote-as 64999
  neighbor <IP_rs_1> description BGP BH 01
  neighbor <IP_rs_1> ebgp-multihop 255
  neighbor <IP_rs_1> route-map BGP-BH-PL in
  neighbor <IP_rs_1> prefix-list 10 out
  neighbor <IP_rs_1> password <tutaj_otrzymane_hasło>
```

<http://networkers.pl/bgp-blackholing/configs.html>

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

<http://networkers.pl/bgp-blackholing>

- **Każdy prefiks otrzymany od danego sąsiada, sprawdzany jest przez route-mapę BGP-BH-PL:**

```
route-map BGP-BH-PL permit 10
  match community 10
  set ip next-hop 192.0.2.1
```

jeżeli prefiks oznaczony będzie pasującym community (w tym przypadku **64999:666**), zostaje umieszczony w tablicy routingu z adresem next-hop ustawionym na 192.0.2.1

trasa do 192.0.2.1 skierowana jest na interfejs Null0

efektywnie, cały ruch pod rozgłoszony prefiks zostaje odrzucony

BGP blackholing

Jak mogę się przyłączyć?

<http://networkers.pl/bgp-blackholing>

- **Napisz maila na adres bgp@networkers.pl**
- **Podaj:**
 - typ swojego routera (np. Cisco 7206 albo Juniper M10i)**
 - rodzaj i ilość styków z operatorami (adresacja IP!)**
 - z jakich IP chcesz zestawiać sesje z route-serwerami**
 - czy posiadasz i jeśli tak to jaki publiczny ASN?**
 - czy chcesz korzystać z możliwości wstrzykiwania prefiksów ze swojego ASa? jeśli tak, jakie to prefiksy?**
 - czy możemy podać informacje o Twoim uczestnictwie na stronie projektu? (tylko AS i nazwa firmy/ew. imię i nazwisko osoby prywatnej)**
 - działający telefon kontaktowy**
- **Postaramy się jak najszybciej skontaktować, podając potrzebne do zestawienia sesji informacje**

BGP blackholing

Jak mogę się przyłączyć? Przykładowy e-mail

<http://networkers.pl/bgp-blackholing>

Cześć !

Chciałbym przyłączyć się do projektu BGP BH PL.

Posiadam dwa routery Cisco 3825.

Sesje będę zestawiał z IP 10.10.10.254 i 10.10.10.250.

Nie posiadam swojego numeru AS.

Chciałbym mieć możliwość wstrzykiwania prefiksów: 10.11.11.0/24

Mój numer telefonu to 0202122

BGP blackholing

Jak mogę się przyłączyć? Przykładowa odpowiedź.

<http://networkers.pl/bgp-blackholing>

Witamy!

Skonfigurowaliśmy dwie sesje, po jednej do każdego Twojego routera.

Router A:

Nasz IP : A.B.C.D

Twój IP : 10.10.10.250

Hasło MD5 : tajne_haslo_1

Nasz AS : 64999

Twój AS : 65500

Router B:

Z.X.C.V

10.10.10.254

tajne_haslo_2

64999

65500

BGP blackholing

Więcej informacji o konfiguracjach?

<http://networkers.pl/bgp-blackholing>

- **Inne konfiguracje, porady praktyczne oraz regulamin znajduje się na stronie projektu:**

<http://networkers.pl/bgp-blackholing>

- **Dostępne są również dwie listy: dyskusyjna projektu oraz administracyjna – informacje o nowych podsięciach, incydentach itp.:**

bgp-bh-pl@networkers.pl

bgp-bh-announce@networkers.pl

ZASTOSOWANIA BGP BLACKHOLING



Zastosowania BGP Blackholing

<http://networkers.pl/bgp-blackholing>

- **Profilaktyka**
- **Jak wykryć DoS/DDoS?**
- **Wysyłanie informacji o ataku na własną sieć**
- **Wykorzystanie mechanizmu uRPF w filtrowaniu ruchu**
- **BGP Blackholing wewnątrz Twojej sieci**

Profilaktyka

<http://networkers.pl/bgp-blackholing>

- **Dobra obrona jest jak ogr:**
ma warstwy
- **1. hardening**
- **2. ochrona antyspoofingowa**
- **3. ACL/stateful firewall**
- **4. uwierzytelnianie sesji routingu**
- **5. IDS/IPS**
- **6. mechanizmy QoS**
- **7. mechanizmy specyficzne dla sieci**
- **...inne...**



Jak wykryć DoS/DDoS?

<http://networkers.pl/bgp-blackholing>

- **Rozwiązania oparte o rozproszone sondy IDS/IPS**
zwykle z opóźnieniem
- **Rozwiązania oparte o modyfikacje/pluginy aplikacji atrakcyjnych jako cele**
zwykle mało skalowalne
- **Rozwiązania oparte o NetFlow**
powszechnie przyjęty standard
dostępne rozwiązania GPL/BSD/etc. oraz komercyjne
relatywna łatwość w implementacji
dokładne dane – o miejscu, rodzaju i sile ataku

Jak wykryć DoS/DDoS?

Czyli co NetFlow może zrobić dla Ciebie

<http://networkers.pl/bgp-blackholing>

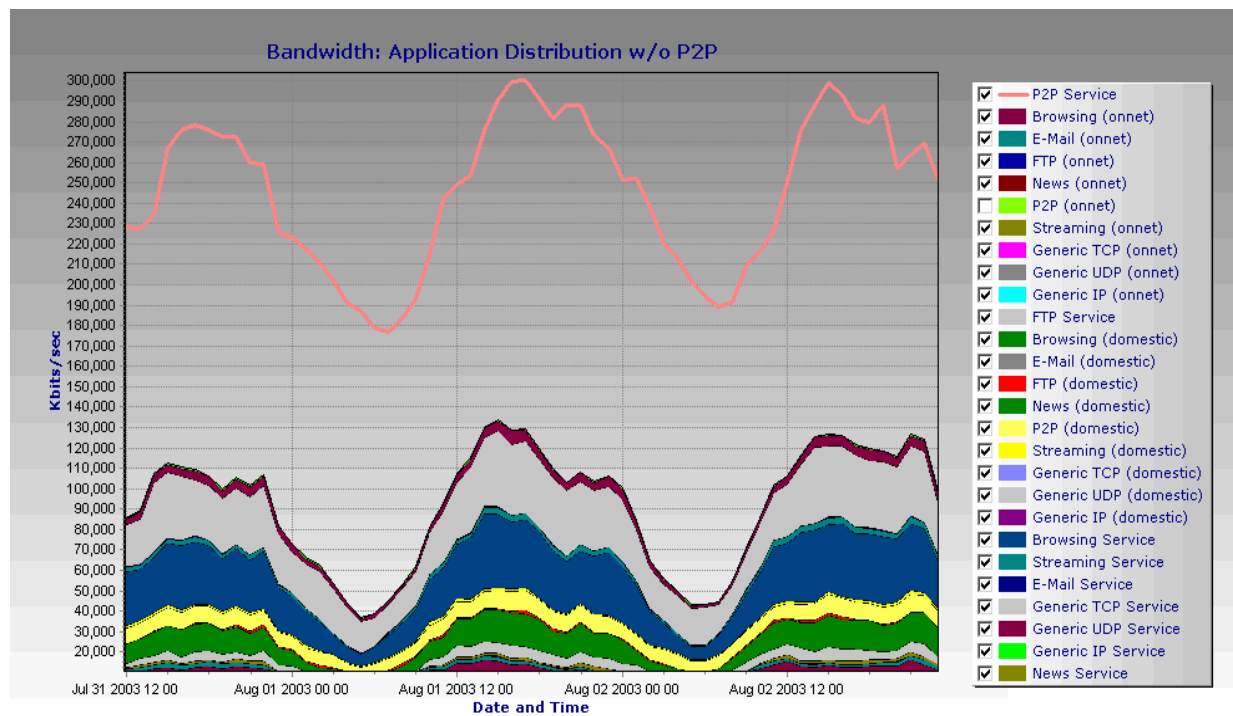
- **NetFlow to mechanizm zbierania informacji o potokach (ang. flow) w sieci**
 - w zależności od wersji, ilość informacji o potoku różni się – wersje 5 i 9 są najpowszechniejsze**
 - w potoku dostajemy źródłowy i docelowy: adres IP, porty TCP/UDP, typ/kod ICMP, numer AS, oraz zwykle również: ilość bajtów, ilość pakietów, czas trwania itp. itd.**
- **Skorzystanie z NetFlow daje doskonałe narzędzie do monitoringu sieci i poznania jej specyfiki**
 - zanim przyjdzie DDoS...**

Jak wykryć DoS/DDoS?

Czyli co NetFlow może zrobić dla Ciebie

<http://networkers.pl/bgp-blackholing>

- Przykładowe wykresy ruchu z systemu monitoringu NetFlow:



Jak wykryć DoS/DDoS?

Chcę takie dwa!

<http://networkers.pl/bgp-blackholing>

- **Na systemy Linux/BSD:**

cflowd, flow-tools, ng_netflow (FreeBSD), pfflowd (OpenBSD)

fprobe, softflowd, ntop

- **W Cisco IOS:**

włączyć NetFlow na interfejsach

skonfigurować eksport informacji do serwerów

...plus ewentualnie inne opcje (sampling, agregacja itp)

<http://freshmeat.net/search/?q=netflow§ion=projects>

BGP blackholing

Jak wysłać informacje o ataku na własną sieć?

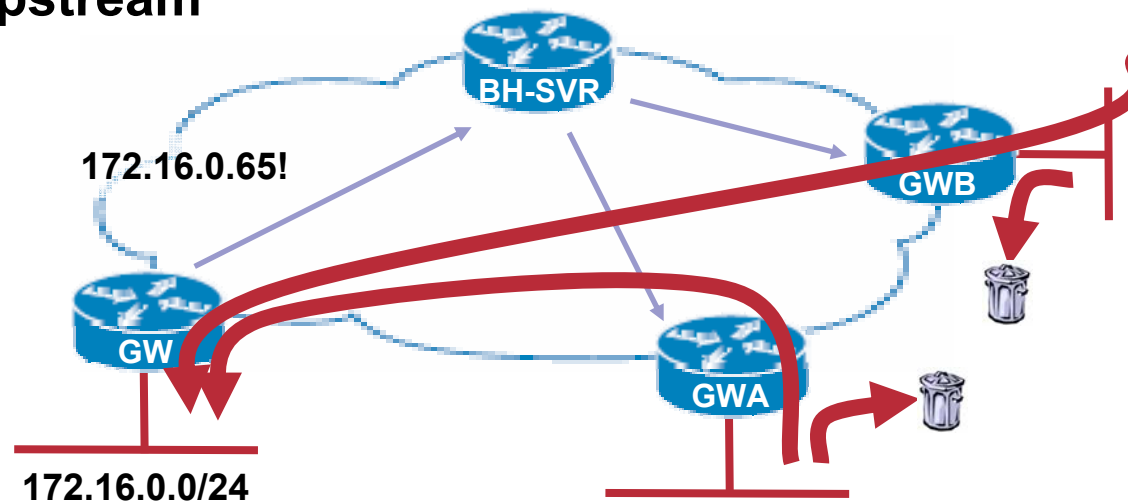
<http://networkers.pl/bgp-blackholing>

- Można rozgłaszać IP i podsieci z **własnego AS'a** jeśli wykryjemy na nie atak do wszystkich uczestników projektu tak, by:

zachować styk z ISP

pomóc walczyć operatorom z DDoSem

zatrzymać zombie w innych sieciach przed generowaniem śmieci upstream



BGP blackholing

Jak wysłać informacje o ataku na własną sieć?

<http://networkers.pl/bgp-blackholing>

```
route-map BH-SEND permit 10
  match tag 666
  set community 64999:999
!
router bgp 100
  redistribute static route-map BH-SEND
  neighbor 10.0.0.8 remote-as 64999
  neighbor 10.0.0.8 send-community
  [...]
! atak na 172.16.10.15?
ip route 172.16.10.15/32 Null0 tag 666

...

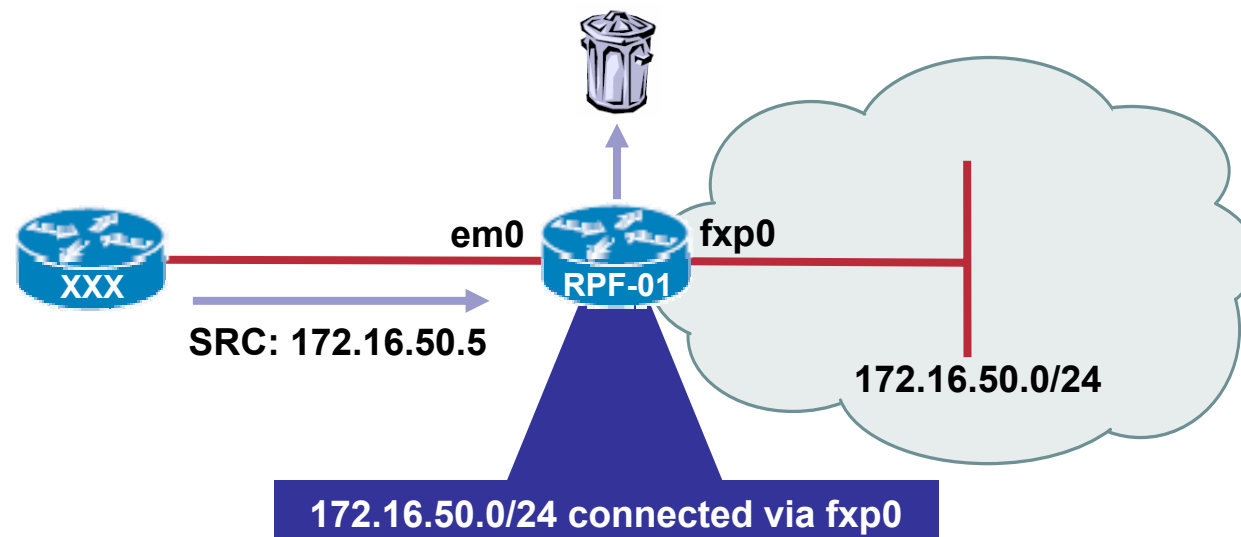
! koniec ataku na 172.16.10.15?
no ip route 172.16.10.15/32 Null0 tag 666
```

BGP blackholing

RPF - Jak to działa?

<http://networkers.pl/bgp-blackholing>

- RPF = Reverse Path Filtering
- Źródłowy adres każdego pakietu jest porównywany z zawartością tablicy routingu
- Adres źródłowy pakietu i interfejs którym dotarł on do routera, musi zgadzać się z tablicą routingu



BGP blackholing

Konfiguracja - RPF

<http://networkers.pl/bgp-blackholing>

- Dzięki mechanizmowi RPF, ruch również **z** odebranych z route-servera prefiksów, kierujemy na interfejs Null0:

FreeBSD, tryb „strict”:

```
deny log ip from any to any not verrevpath in via em0
```

FreeBSD, tryb „loose”:

```
deny log ip from any to any not versrcpath in via em0
```

Cisco, tryb „strict”:

```
ip verify unicast source reachable via rx [allow-default]
```

Cisco, tryb „loose”:

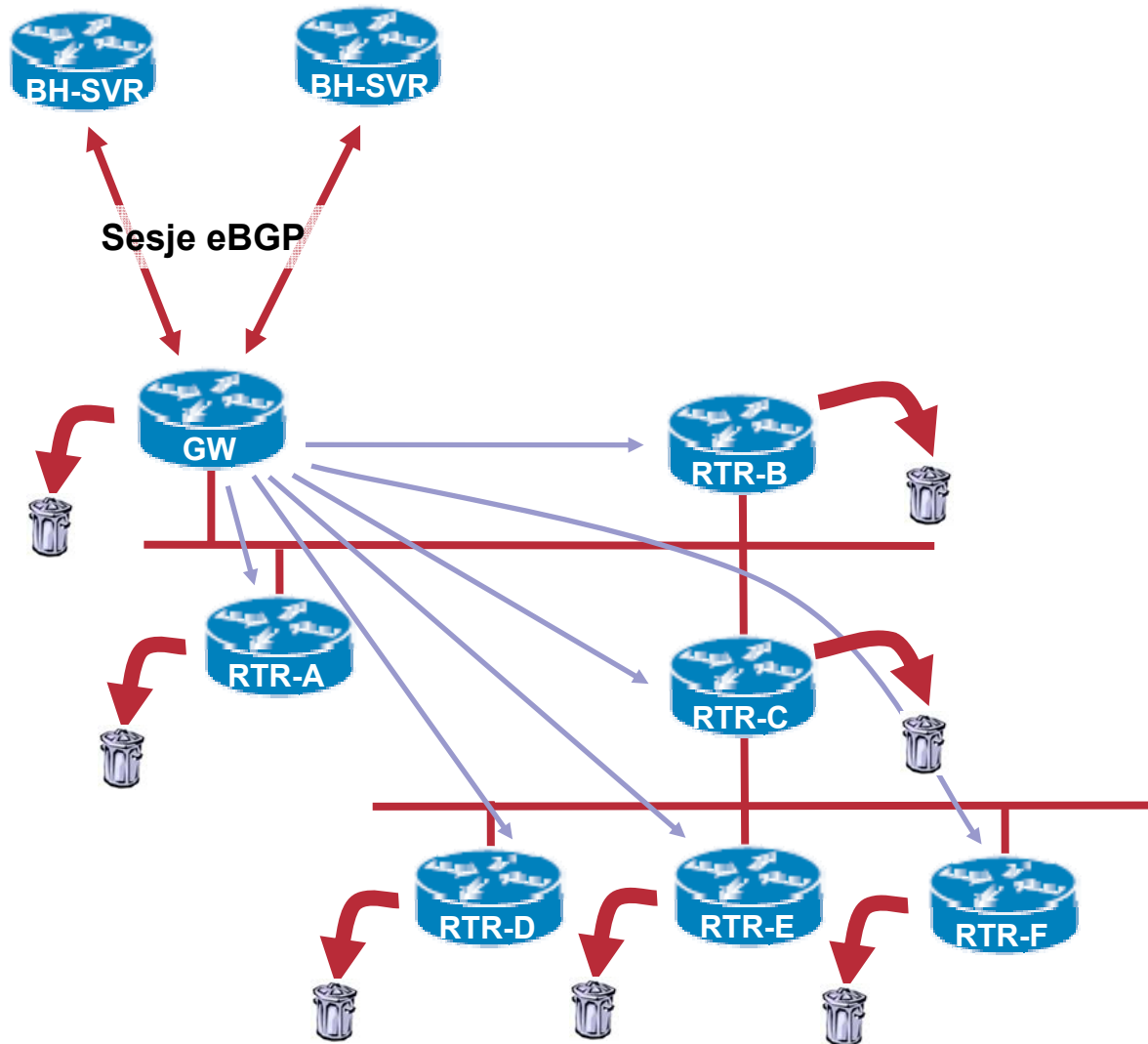
```
ip verify unicast source reachable via any
```


BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- Mimo uruchomienia BGP BH na GW, nadal reszta sieci może być przeciążana przez ataki inicjowane z jej środka
- Rozwiązaniem jest konfiguracja iBGP



BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- **GW – eBGP do BGP BH PL i iBGP do routerów w środku sieci:**

```
router bgp 100
  neighbor 10.0.0.8 remote-as 64999
  neighbor 10.0.0.8 description BGP BH 01
  neighbor 10.0.0.8 route-map BH in
  neighbor 10.0.0.8 ebgp-multihop 255
  neighbor 172.16.0.10 remote-as 100
  neighbor 172.16.0.10 description iBGP-RTR-A
  neighbor 172.16.0.10 send-communities
  [...]
```

BGP blackholing

Jak wykorzystać peering z BGP BH PL w środku sieci?

<http://networkers.pl/bgp-blackholing>

- **RTR-A – iBGP z GW**

```
router bgp 100
  neighbor 172.16.0.1 remote-as 100
  neighbor 172.16.0.1 description iBGP-GW
  neighbor 172.16.0.1 route-map BH in
!
ip route 192.0.2.1/32 Null0
ip community-list 99 permit 64999:666
!
route-map BH permit 10
  match community 99
  set ip next-hop 192.0.2.1
```

BGP blackholing

Czy to w ogóle działa?

<http://networkers.pl/bgp-blackholing>

```
busy-bsd ~$ netstat -nrf inet | grep B
```

1	127.0.0.1	UG1cB	0	31490	1o0
2	127.0.0.1	UG1cB	0	2853	1o0
5	127.0.0.1	UG1cB	0	11921	1o0
7	127.0.0.1	UG1cB	0	4321	1o0
10	127.0.0.1	UG1cB	0	184921	1o0
23	127.0.0.1	UG1cB	0	9392	1o0
169.254	127.0.0.1	UG1cB	0	94812	1o0
172.16/12	127.0.0.1	UG1cB	0	119486	1o0
173.0/8	127.0.0.1	UG1cB	0	11602	1o0
174.0/8	127.0.0.1	UG1cB	0	6731	1o0
175.0/8	127.0.0.1	UG1cB	0	996	1o0
192.168.0/16	127.0.0.1	UG1cB	0	89483	1o0

```
busy-cisco# sh ip traffic | incl RPF
```

```
7 no route, 4386198 unicast RPF, 0 forced drop
```

GDZIE WARTO RZUCIĆ OKIEM



Strona projektu

<http://networkers.pl/bgp-blackholing>

BGP Blackholing PL

opis projektu

BGP blackholing PL team <bgp@networkers.pl>
v1.1 13-08-2005

[OPIS PROJEKTU](#) | [KONFIGURACJE](#) | [REGULAMIN](#) | [FAQ](#) | [MATERIAŁY](#) | [UCZESTNICZY](#)

O co chodzi?

Projekt **BGP Blackholing PL** narodził się jako pomysł na zwiększenie bezpieczeństwa naszej części internetu.

Nazwa projektu pochodzi od idei jego działania. Po angielsku **black hole** to czarna dziura, a sformułowanie **blackholing** opisuje wrzucanie do niej różnego rodzaju rzeczy - w naszym przypadku, chodzi o niepotrzebny lub szkodliwy wręcz ruch sieciowy.

Projekt ma na celu zbudowanie i utrzymywanie infrastruktury, która każdej mniejszej lub większej sieci udostępni automatyczne informacje o:

- ♦ **pulach nieużywanych (nieprzydzielonych) adresów IP**
organizacja IANA zajmuje się przydzielaniem (lub delegacją praw do przydzielania) przestrzeni adresowej dla protokołów IPv4 i IPv6; adresy obecnie [zarezerwowane przez IANA](#) są nieużywane i jako takie, nie powinny pojawiać się w internecie; zadziwiająco jednak często widzimy taki ruch, generowany głównie przez rozmaite konie trojańskie i boty, które nie zważając na takie subtelności jak plan używanej przestrzeni adresowej, losowo generują adresy IP do dalszego rozmnażania
- ♦ **obecnie atakowanych adresach IP członka projektu**
mechanizm ataków DoS/DDoS polega na tym, że wiele hostów, świadomie bądź nie generuje ruch pod wskazany adres IP lub pulę adresów IP, efektywnie odcinając ją od Internetu i przeciążając różnego rodzaju połączenia na drodze od nich do celu ataku; jeśli atakowany adres IP lub pula adresów IP należy do członka projektu, może on kosztem odcięcia celu ataku rozgłosić do innych członków projektu ten adres; pierwsza zaleta tego rozwiązania to fakt, że jeśli członków projektu będzie odpowiednio dużo, możemy ograniczyć wpływ ataku DoS/DDoS na funkcjonowanie styków z Internetem atakowanej sieci; kolejne zalety, to higiena całej infrastruktury - jeśli ISP i inni członkowie projektu również będą odrzucać takie pakiety już u siebie, oszczędzimy wysycania ich połączeń;

Jak mogę się przyłączyć?

Projekt jest **niekomercyjny** i opiera się na współpracy ludzi, którzy chcą budować bezpieczny internet.

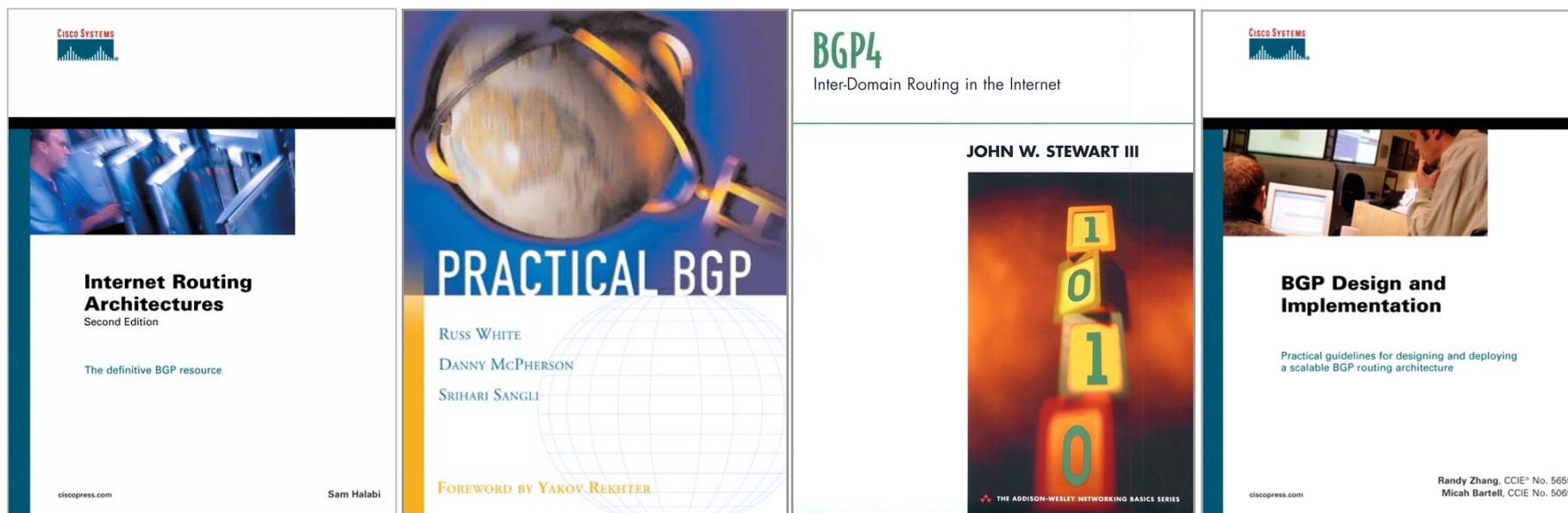
Potrzebujemy pomocy!



Nasza infrastruktura jest obecnie ograniczona do sprzętu i łącz, które mogliśmy zdobyć sami. Jeśli jesteś w stanie jakoś nam pomóc - poświęcając niepotrzebny router lub kolokację naszego routera z dobrej jakości połączeniem internetowym - napisz do nas pod adres bgp@networkers.pl, opisując dokładnie co jesteś w stanie oferować. Sprzęt i łącz nadal pozostaje Twoją własnością - "wypożyczamy" go tylko na czas trwania projektu.

Książki

<http://networkers.pl/bgp-blackholing>



Zasoby WWW

<http://networkers.pl/bgp-blackholing>

- **Strona projektu BGP Blackholing PL:**

<http://networkers.pl/bgp-blackholing>

- **BGP4.AS**

<http://www.bgp4.as>

- **ISP Essentials:**

<ftp://ftp-eng.cisco.com/cons/isp/essentials/>

- **ISP Security Essentials (NANOG):**

<http://www.nanog.org/ispsecurity.html>

- **Prezentacje Philipa Smitha**

<ftp://ftp-eng.cisco.com/pfs/seminars/>

Q&A



PROJEKT BGP BLACKHOLING PL

Łukasz Bromirski
lukasz@bromirski.net

bgp@networkers.pl