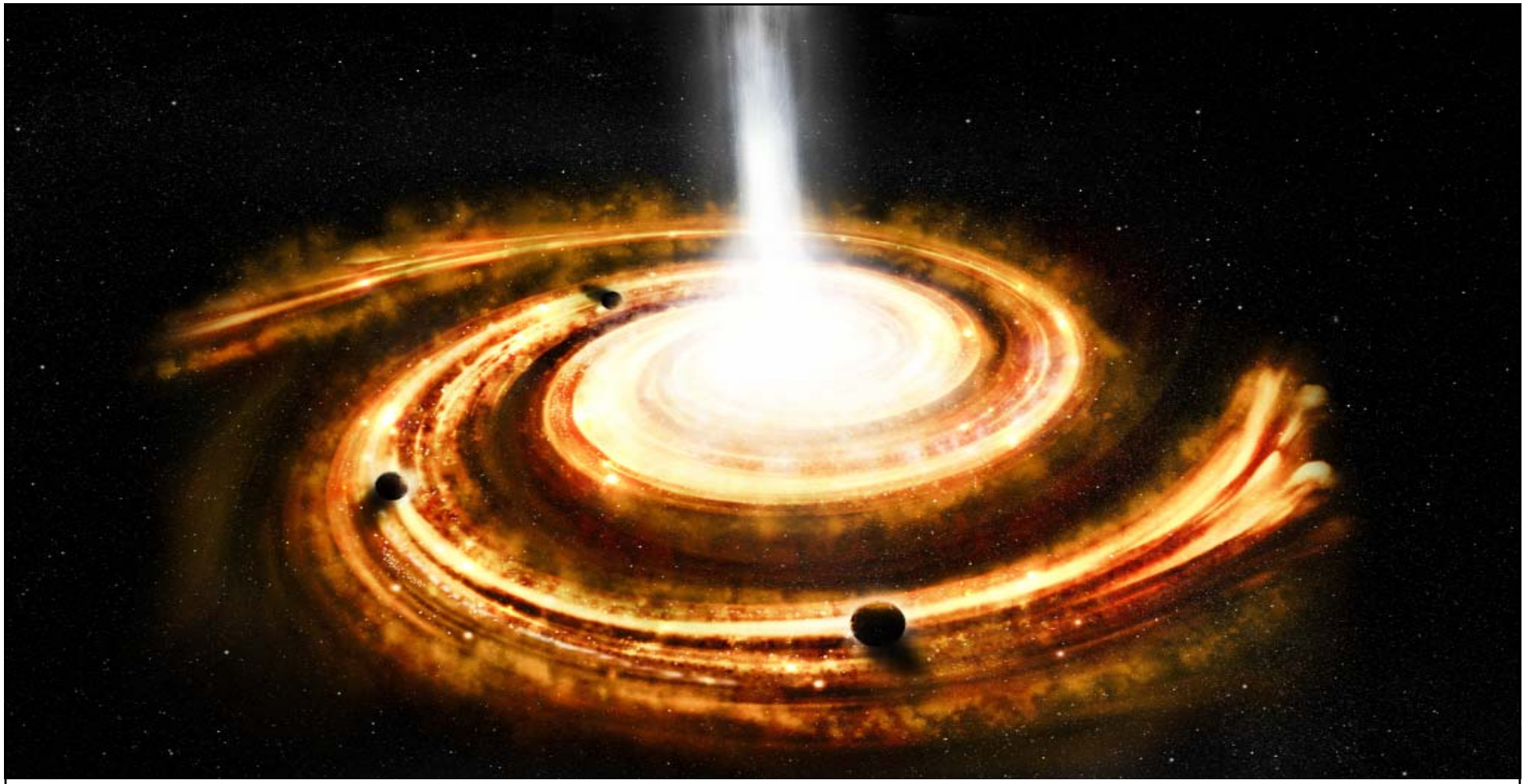


Projekt

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
„Mnie to nie dotyczy”

http://networkers.pl/bgp-blackholing

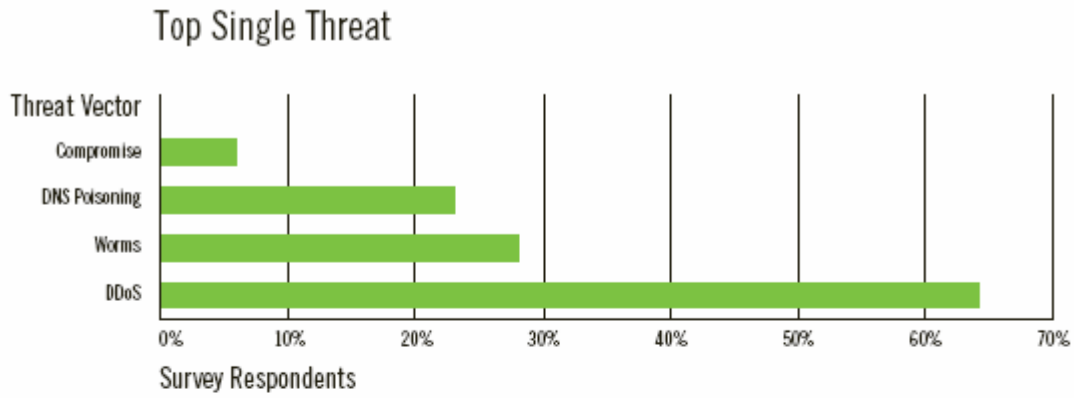


Figure 2: Top Single Threats

Figure 3 illustrates the largest threats perceived by network security operators today.

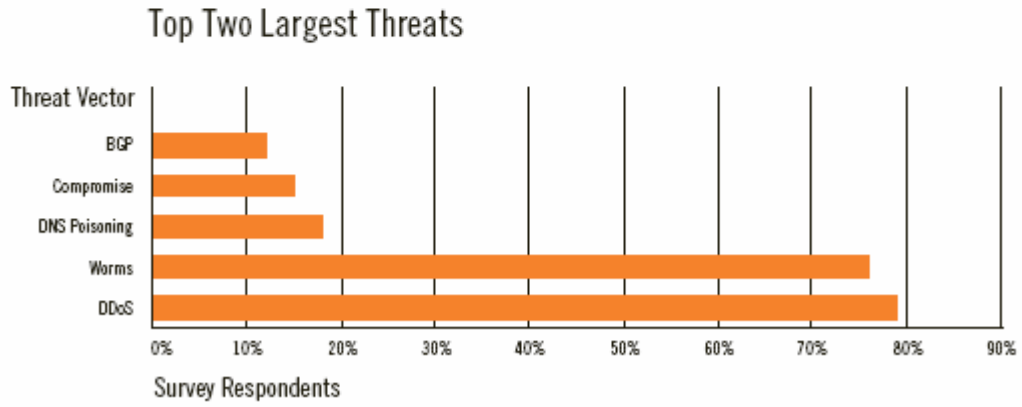


Figure 3: Top Two Largest Threats

http://www.arbor.net/downloads/Arbor_Worldwide_ISP_Security_Report.pdf

Typowy DDoS

„Mnie to nie dotyczy”

http://networkers.pl/bgp-blackholing

DDoS on Blue Security Blog Knocks Typepad, LiveJournal Offline **Performance**

The spam-fighting service Blue Security has been under siege by spammers and digital attackers in recent days. On Tuesday it wound up sharing its pain with a large chunk of the blogosphere. When Blue Security's web site was hit by a distributed denial of service attack attack (DDoS), the company temporarily repointed www.bluesecurity.com to a blog on Six Apart's TypePad service. The DDoS traffic appears to have followed www.bluesecurity.com to its new home, overwhelming Six Apart's network and knocking its TypePad and LiveJournal services offline for nearly eight hours.

LiveJournal hosts more than 1.8 million active blogs, according to its stats page, while TypePad is home to thousands more, including many prominent blogs. In a status advisory, Six Apart said a "sophisticated" DDoS struck at 4 p.m. Pacific time and continued to affect its services until past 11:30 p.m. "This has affected all of Six Apart's sites, causing intermittent and limited availability for TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com."

The DNS change for www.bluesecurity.com to an IP address on Six Apart's network (204.9.178.12) was first noted on the North American Network Operators Group mailing list Tuesday night. Internal links on bluesecurity.blogs.com indicate that the blog was configured to operate under the www.bluesecurity.com URL. Further confirmation came from other blogs, including The SunBelt Blog, which linked to a post published early Wednesday on bluesecurity.blogs.com and cited it as appearing on www.bluesecurity.com.

Earlier this week users of Blue Security's anti-spam service, known as Blue Frog, began receiving emails claiming Blue Security's mailing list had been compromised. The company denied the charge, saying spammers were using exisiting lists to intimidate its users. The dispute received coverage on Slashdot, C/Net, The Register, Wired News, MSNBC and the Associated Press.

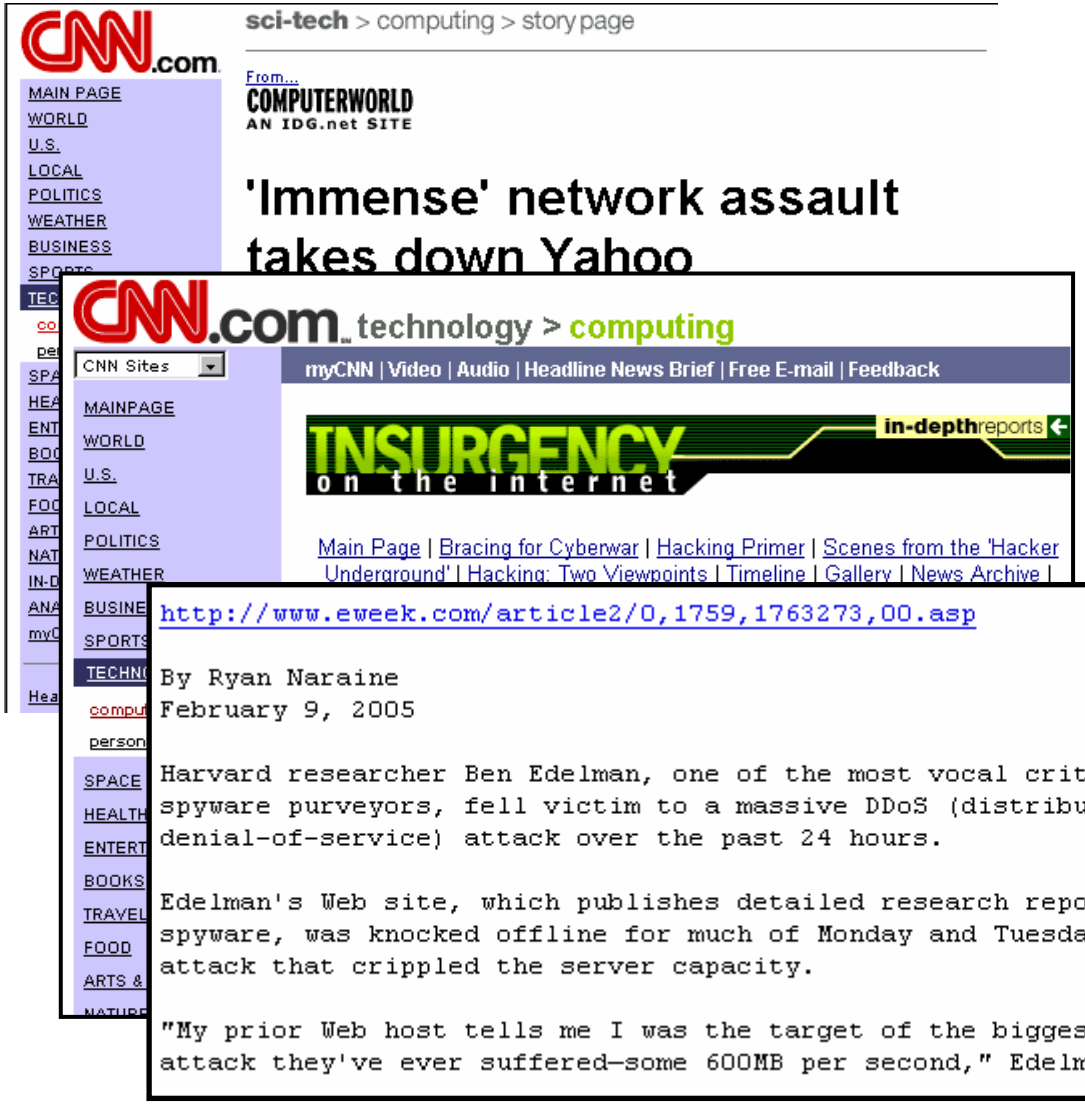
Posted by Rich Miller at May 3, 2006 02:44 PM | Subscribe

http://news.netcraft.com/archives/2006/05/03/ddos_on_blue_security_blog_knocks_typepad_livejournal_offline.html
http://www.bluesecurity.com/announcements/pm_attack_timeline.asp

Typowy DDoS

„Mnie to nie dotyczy”

http://networkers.pl/bgp-blackholing



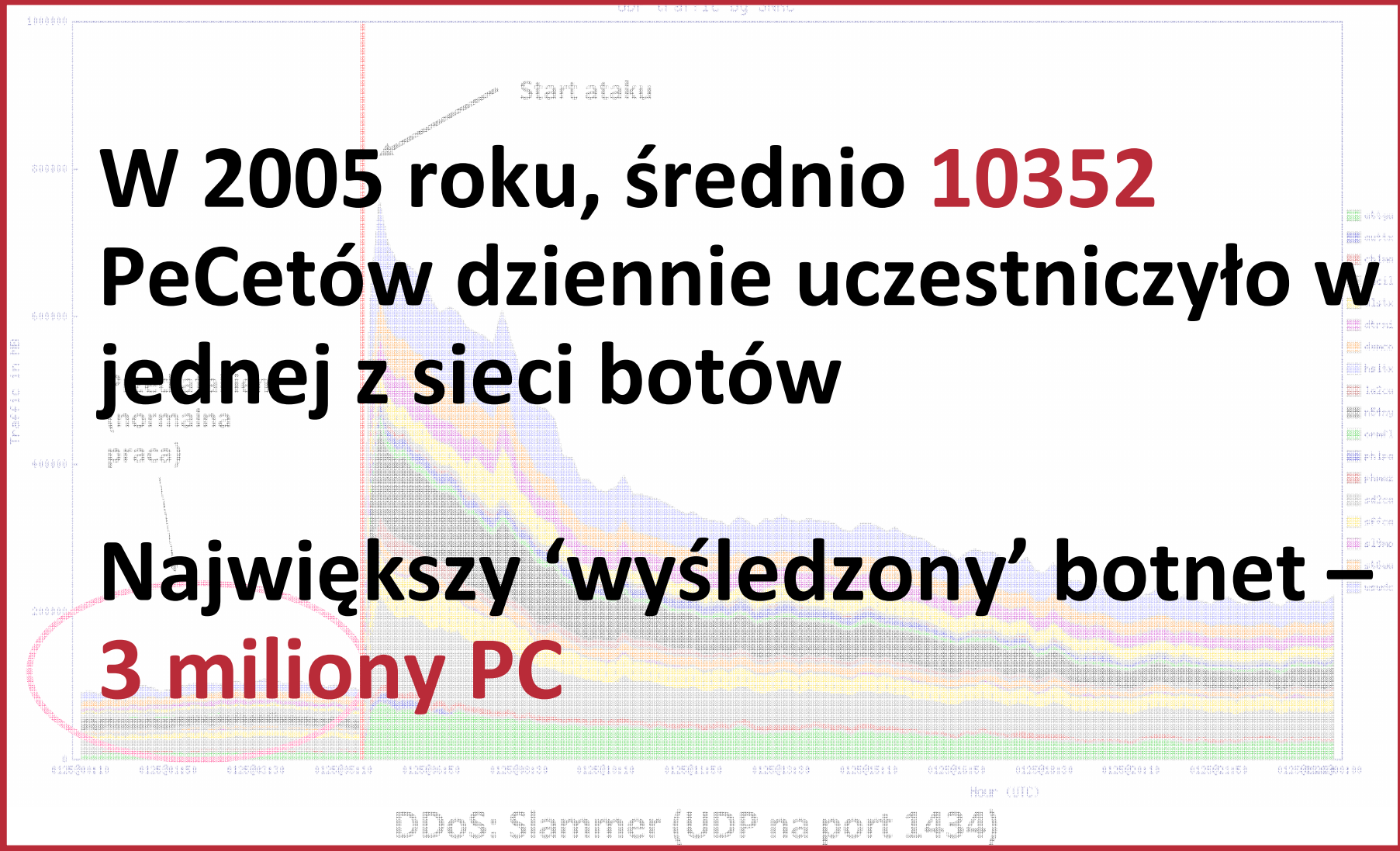
Typowy DDoS

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 – na żywo



W 2005 roku, średnio 10352 PeCetów dziennie uczestniczyło w jednej z sieci botów

Największy ‘wyśledzony’ botnet – 3 miliony PC

Jeśli jeszcze się nie boicie, po prostu **nie rozumiecie** powagi sytuacji.

Mike O'Dell, IETF

„Mnie nie zatkacie”

Rzeź routerów...

http://networkers.pl/bgp-blackholing

- Większość routerów nieoperatorskich jest czuła na ilość pakietów/sekundę a nie ich długość (każdy pakiet = konkretny zestaw operacji, realizowanych zwykle w architekturze sterowanej przerwaniami)
- Nawet mając wolny upstream, możemy wygenerować dużo 40 bajtowych pakietów IP

  2Mbit/s = 6400 pakietów/s

  10Mbit/s = 31,250 pakietów/s

  34Mbit/s = 106,250 pakietów/s

  155Mbit/s = 484,375 pakietów/s

  622Mbit/s = 1,943,750 pakietów/s

  2,4Gbit/s = 7,500,000 pakietów/s
- Stacja z pasmem upstream 256kbit/s może wygenerować tylko 800 40-bajtowych pakietów IP/sekundę

  ..ale wystarczy zebrać 8 i zatykamy łącze 2Mbit/s, 600 i zatykamy łącze 155Mbit/s...

*Nie bierzemy pod uwagę narzutu protokołów

„Mnie nie zatkacie”

Kradzież pasma...

http://networkers.pl/bgp-blackholing

- Pasmo jest ograniczone...
- Generujemy 1500 bajtowe pakiety IP

  2Mbit/s = 167 pakietów/s

  10Mbit/s = 834 pakiety/s

  34Mbit/s = 2834 pakiety/s

  155Mbit/s = 12917 pakietów/s

  622Mbit/s = 51814 pakietów/s

  2,4Gbit/s = 200000 pakietów/s
- Stacja z pasmem upstream 256kbit/s może wygenerować tylko 21 1500-bajtowych pakietów/sekundę

  ..ale wystarczy zebrać 8 i zatykamy łącze 2Mbit/s, 600 i zatykamy łącze 155Mbit/s...

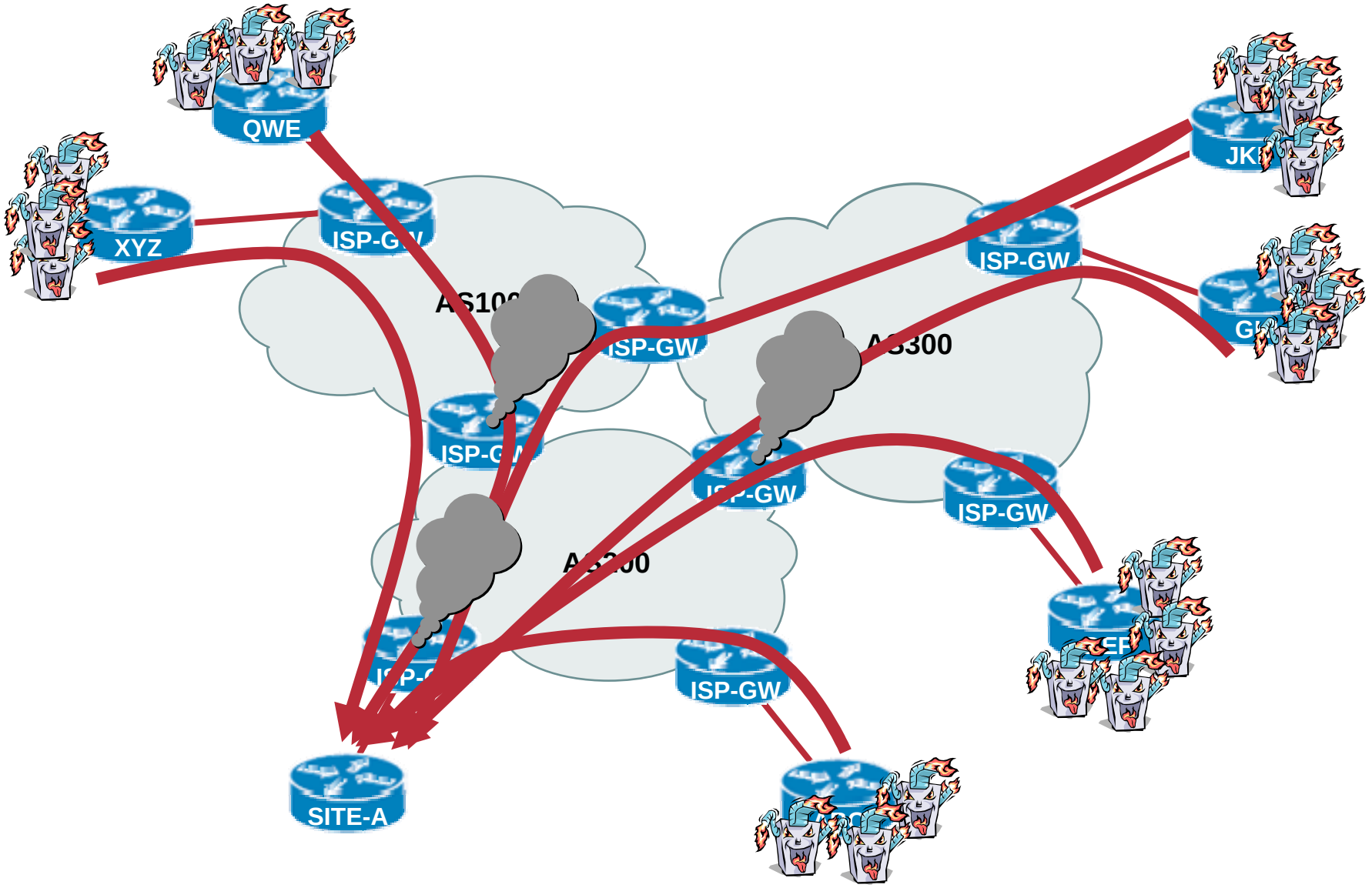
*Pakiet IP = 40 bajtów, najgorszy scenariusz - często stosowany dla DDoS

Nie bierzemy pod uwagę narzutu protokołów

Typowy DDoS

Jak to się dzieje?

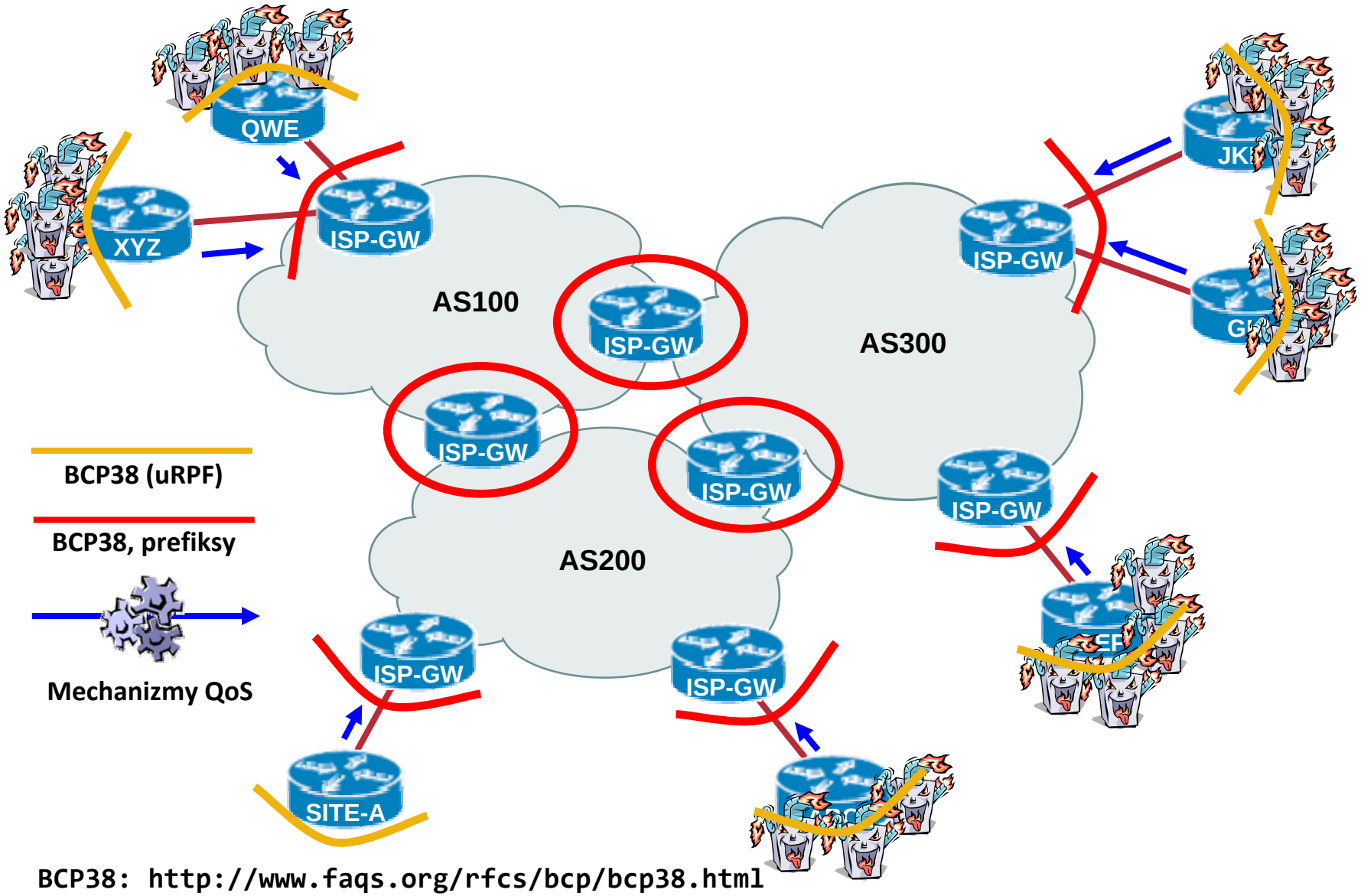
http://networkers.pl/bgp-blackholing



Typowy DDoS

Co ja mogę zrobić dla zwiększenia bezpieczeństwa?

http://networkers.pl/bgp-blackholing



BCP38: http://www.faqs.org/rfcs/bcp/bcp38.html

Czego brakuje do skutecznej 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 oczywiście 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**

JAK DOŁĄCZYĆ DO BGP BLACKHOLING PL

BGP blackholing

BGP refresher

http://networkers.pl/bgp-blackholing

- **BGP rozgłasza osiągalność prefiksów – pul adresów IP**

  Funkcjonalność realizowana dynamicznie

- **Każdy z prefiksów ma pewien zestaw atrybutów – m.in. community**

  Zwykle używane do sygnalizacji co i gdzie rozgłaszać/jak preferować

- **Każdy z prefiksów w trakcie akceptowania przez proces BGP może mieć również zmienione pole next-hop**

  ...routing do interfejsu Null0 powoduje, że pakiety 'znikają' bez potrzeby stosowania ACL

  Czasami routing bezpośrednio do Null0 jest niedostępny lub z innych powodów niewygodny – routujemy zatem do statycznej trasy (192.0.2.1/32 jest dobrym przykładem) która z kolei wskazuje na Null0

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:**

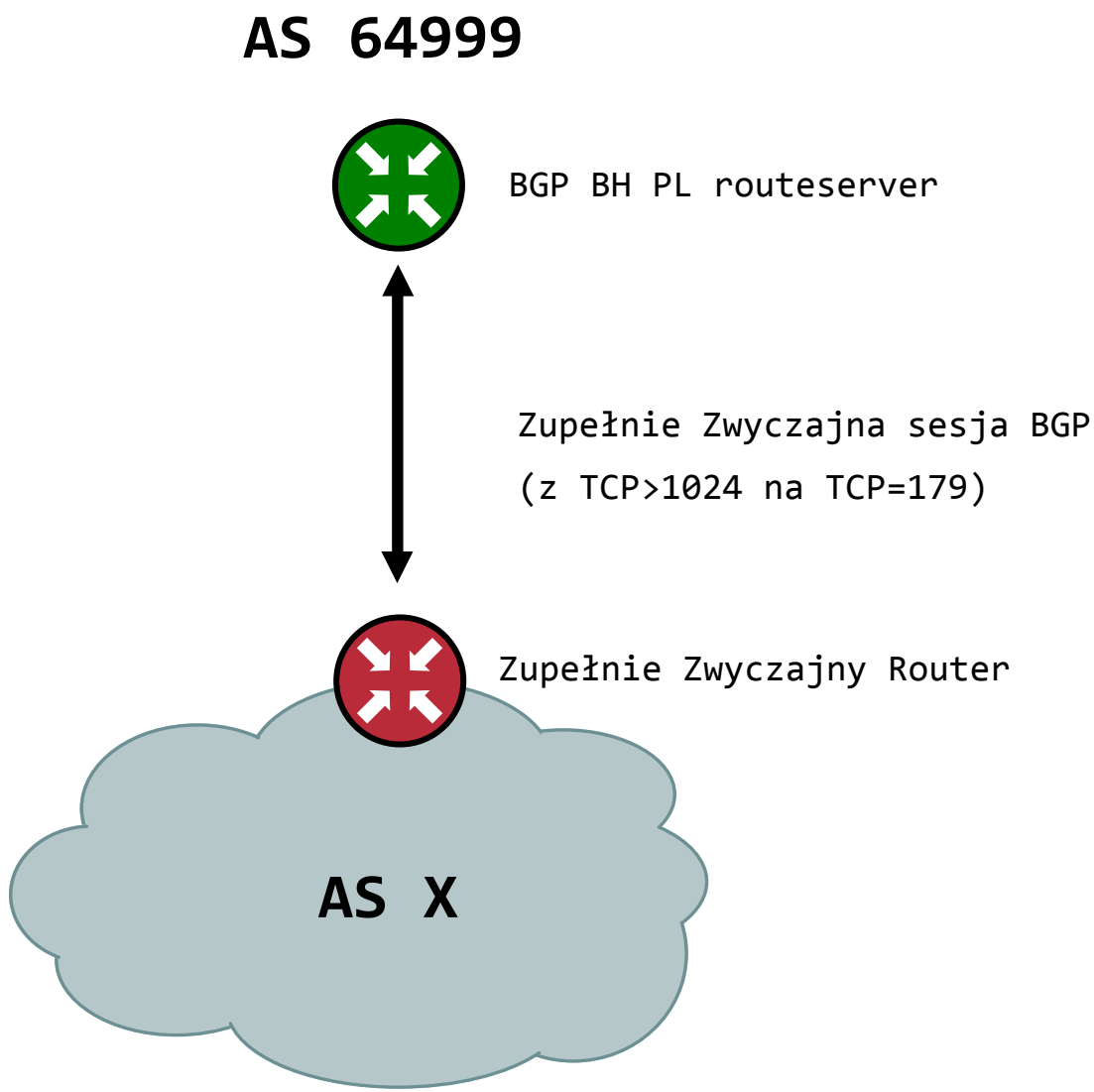
  za pomocą route-mapy skierować ruch do tych prefiksów do Null0 lub jego odpowiednika

  można wykorzystać iBGP żeby rozgłosić prefiksy głębiej do swojej sieci, jeśli składa się z większej ilości routerów

BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

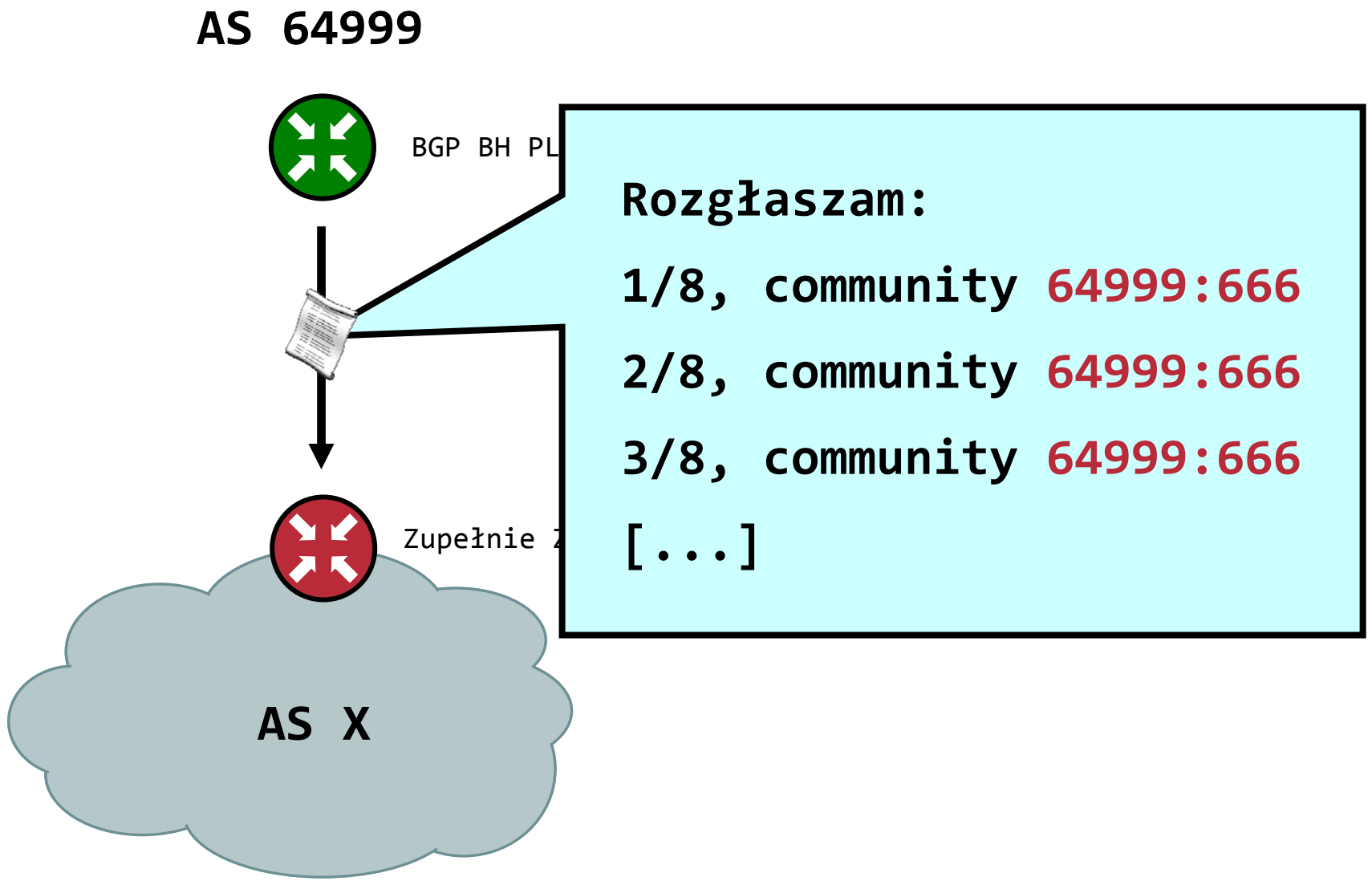
http://networkers.pl/bgp-blackholing



BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

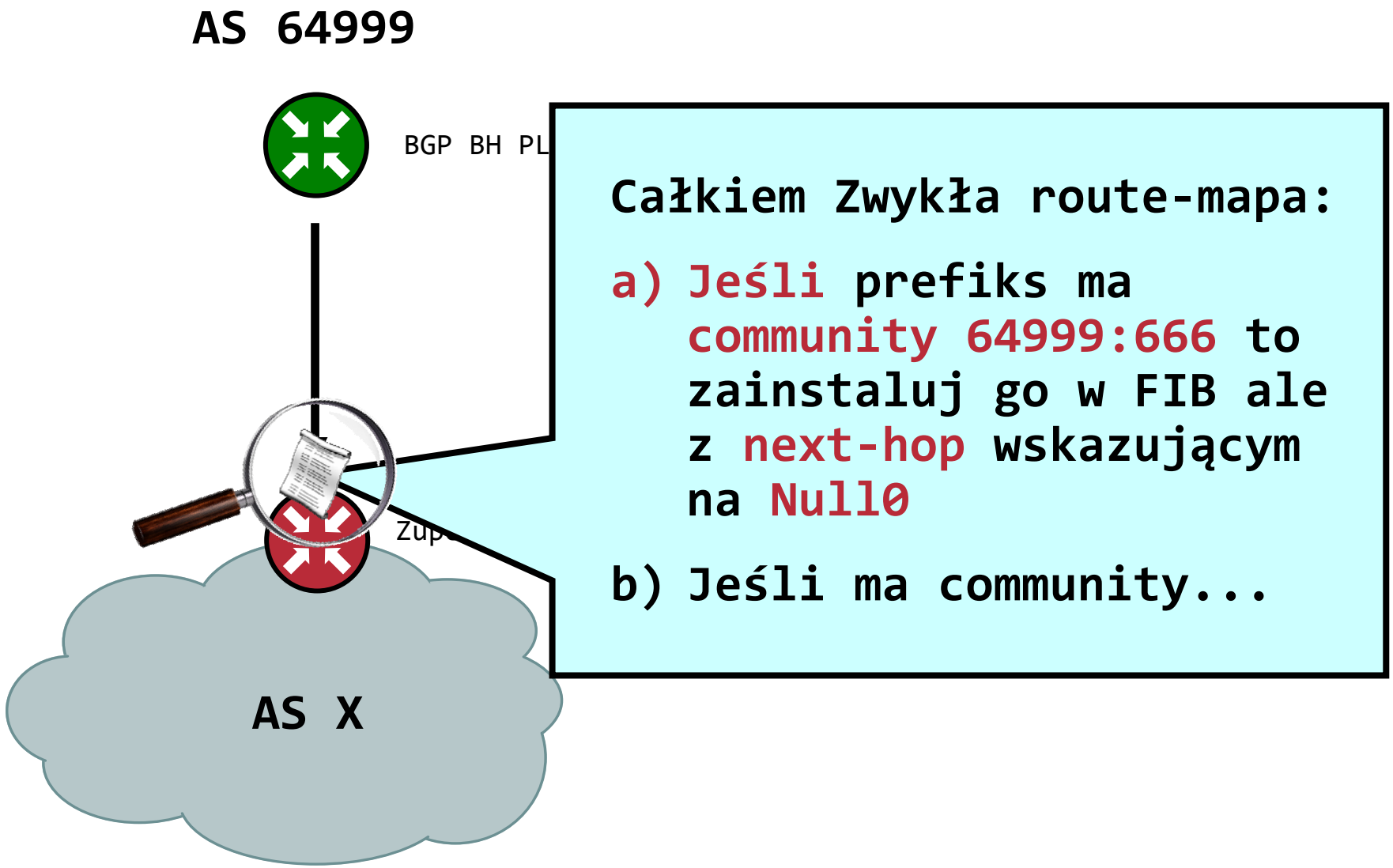
http://networkers.pl/bgp-blackholing



BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

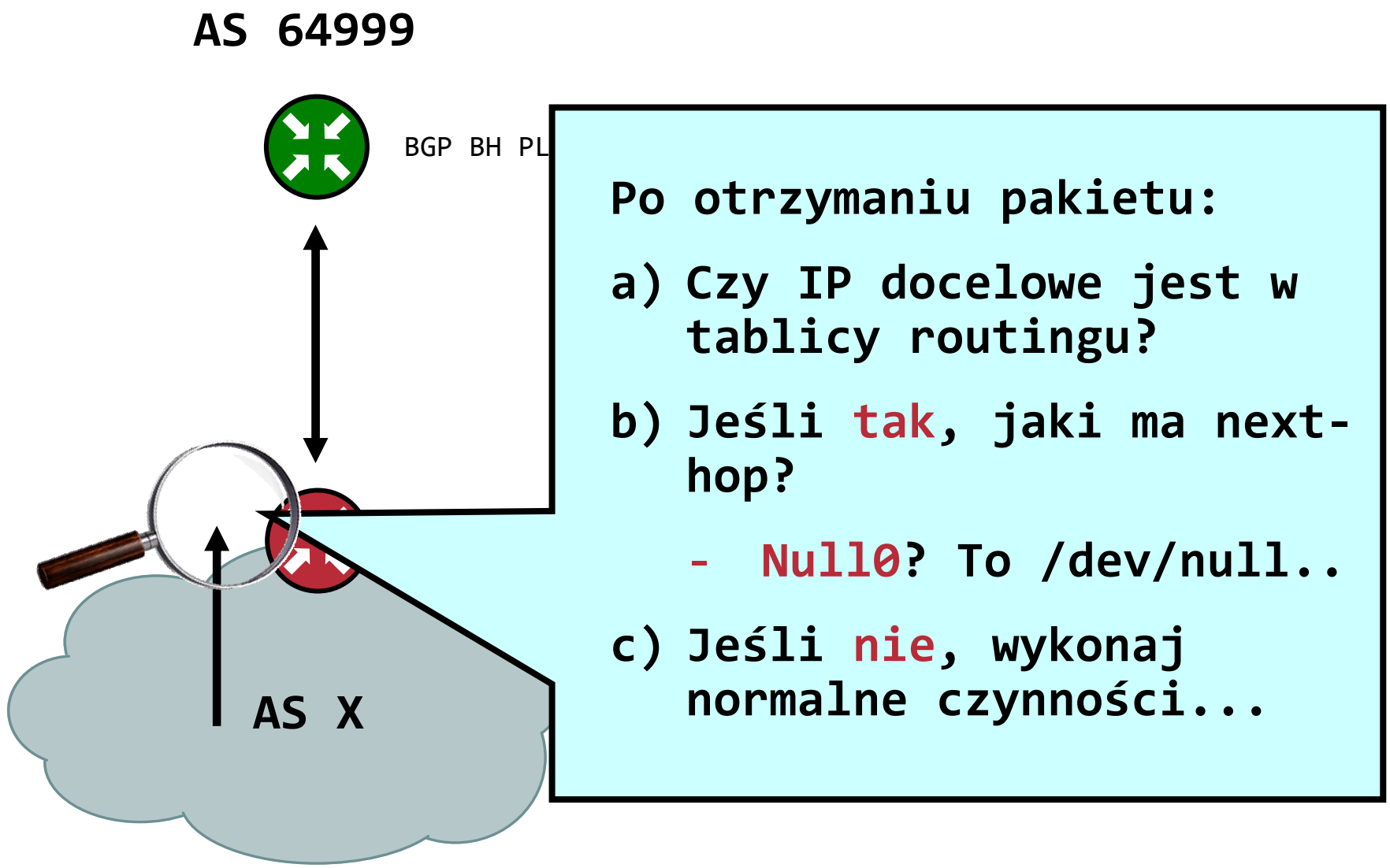
http://networkers.pl/bgp-blackholing



BGP blackholing

Konfiguracja – z lotu ptaka dla wzrokowców

http://networkers.pl/bgp-blackholing



BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

http://networkers.pl/bgp-blackholing

- **Definiujemy trasę wskazującą 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

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

```
route-map BGP-BH-PL permit 10
 match community 10 ! (permit 64999:666)
 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 ! (permit 64999:999)
 set ip next-hop address 192.0.2.1
```

BGP blackholing

Przykład konfiguracji – Quagga/Zebra/Cisco

- **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>
```

Więcej pod: 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? (oczywiście musimy to zweryfikować w RIPE)
  - 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 7200.

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 0(22)202122

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:	Router B:
Nasz IP	A.B.C.D	Z.X.C.V
Twój IP	10.10.10.250	10.10.10.254
Hasło MD5	tajne_hasło_1	tajne_hasło_2
Nasz AS	64999	64999
Twój AS	65500	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 trzy listy:**

  bh-pl-discuss@lists.networkers.pl

  bh-pl-announce@lists.networkers.pl

  bh-pl-submit@lists.networkers.pl

- **Strona z listami na networkers.pl:**

  http://lists.networkers.pl/mailman/listinfo

ZASTOSOWANIA BGP BLACKHOLING

Zastosownania 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 infromacji o potoku różni się – wersje 5 i 9 są najpowszechniejsze

  w potoku dostajemy między innymi źródłowy i docelowy: adres IP, porty TCP/UDP, typ/kod ICMP, numer AS, oraz zwykle również: ilość bajtów, ilość pakietów, czas trwania itp. itd.

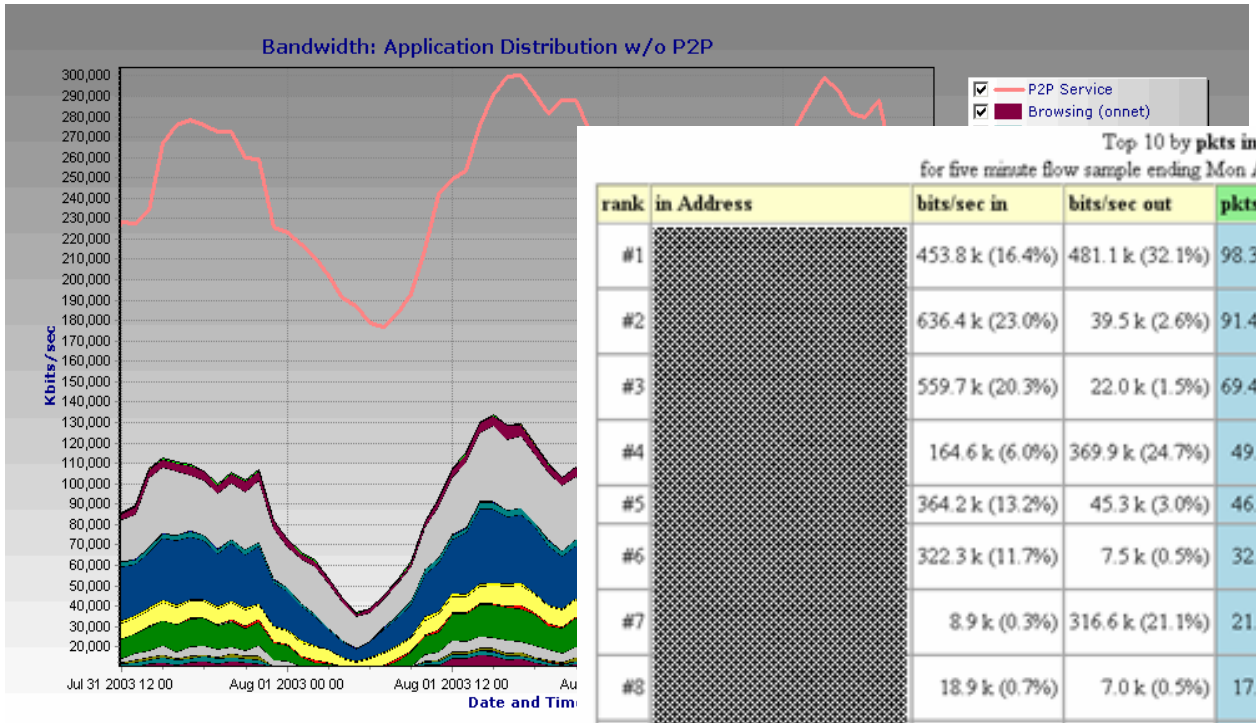
- **Skorzystanie z NetFlow daje doskonałe narzędzie do monitoringu sieci i poznania jej specyfiki**

  zanim DDoS zapuka w Twoje routery...

Jak wykryć DoS/DDoS?
Czyli co NetFlow może zrobić dla Ciebie

http://networkers.pl/bgp-blackholing

- **Przykładowe dane z systemu monitoringu NetFlow:**



Top 10 by **pkts in**
for five minute flow sample ending Mon Apr 17 04:19:07 2006

rank	in Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1		453.8 k (16.4%)	481.1 k (32.1%)	98.3 (18.3%)	100.8 (19.2%)	4.3 (13.4%)	5.2 (14.1%)
#2		636.4 k (23.0%)	39.5 k (2.6%)	91.4 (17.0%)	72.8 (13.8%)	2.9 (9.0%)	3.3 (9.0%)
#3		559.7 k (20.3%)	22.0 k (1.5%)	69.4 (12.9%)	60.5 (11.5%)	756.7 m (2.4%)	840.0 m (2.3%)
#4		164.6 k (6.0%)	369.9 k (24.7%)	49.2 (9.2%)	64.5 (12.2%)	2.3 (7.2%)	3.0 (8.1%)
#5		364.2 k (13.2%)	45.3 k (3.0%)	46.4 (8.6%)	45.6 (8.7%)	2.4 (7.5%)	2.5 (6.7%)
#6		322.3 k (11.7%)	7.5 k (0.5%)	32.2 (6.0%)	20.7 (3.9%)	243.3 m (0.8%)	283.3 m (0.8%)
#7		8.9 k (0.3%)	316.6 k (21.1%)	21.1 (3.9%)	36.1 (6.9%)	1.3 (4.1%)	1.8 (4.9%)
#8		18.9 k (0.7%)	7.0 k (0.5%)	17.1 (3.2%)	17.7 (3.4%)	790.0 m (2.5%)	1.1 (2.9%)
#9		9.9 k (0.4%)	17.6 k (1.2%)	16.6 (3.1%)	18.0 (3.4%)	3.4 (10.4%)	3.8 (10.4%)
#10		118.6 k (4.3%)	4.6 k (0.3%)	14.8 (2.8%)	11.1 (2.1%)	590.0 m (1.8%)	626.7 m (1.7%)

Jak wykryć DoS/DDoS?
Chcę takie dwa!

http://networkers.pl/bgp-blackholing

- **Potrzebujesz co najmniej dwóch komponentów:**

  źródła próbek (router fizycznie routujący pakiety) i kolektora/analizatora (zwykle osobna, wydajna maszyna)

- **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&section=projects

BGP blackholing

Jak wysłać informacje o ataku na własną sieć?

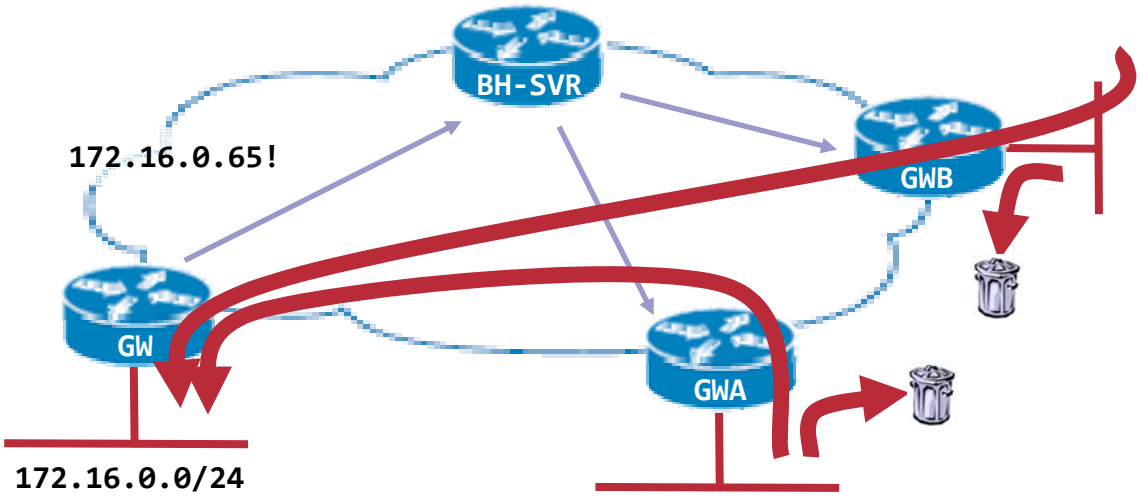
http://networkers.pl/bgp-blackholing

- **Można rozgłaszać prefiksy 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?

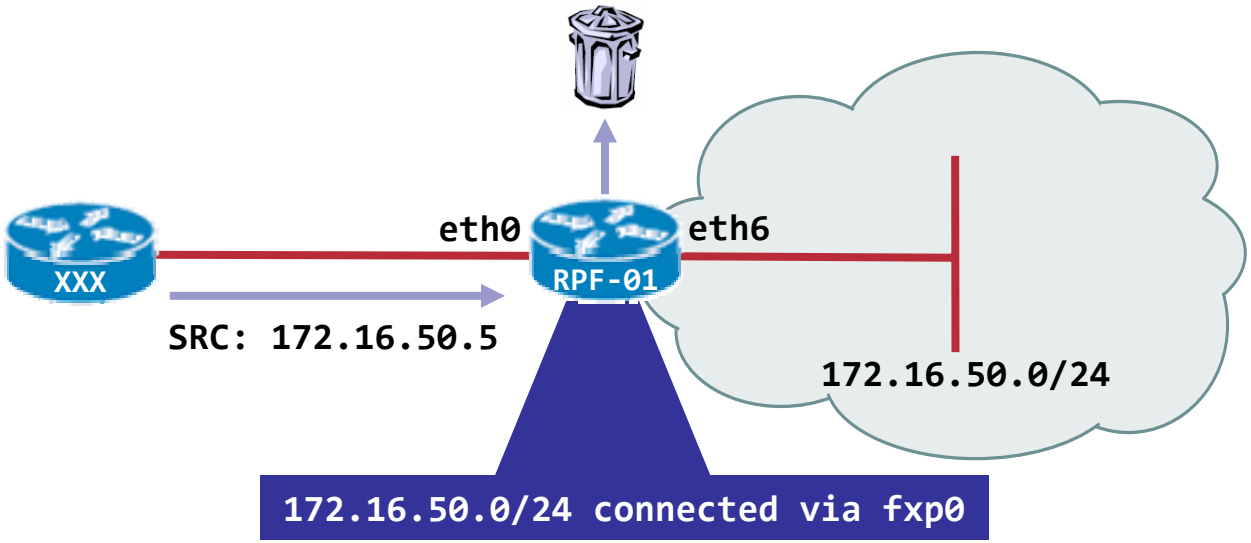
http://networkers.pl/bgp-blackholing

```
route-map BH-SEND permit 10
 match tag 666 ! trasy oznaczone tym tagiem wysyłamy przez BGP
 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 172.16.10.15 255.255.255.255 Null0 tag 666

...

! koniec ataku na 172.16.10.15?
no ip route 172.16.10.15 255.255.255.255 Null0 tag 666
```

BGP blackholing

RPF - Jak to działa?

- 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

- **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
```

Linux:

```
echo [1|2] > /proc/sys/net/ipv4/conf/(all|ethX)/rp_filter
```

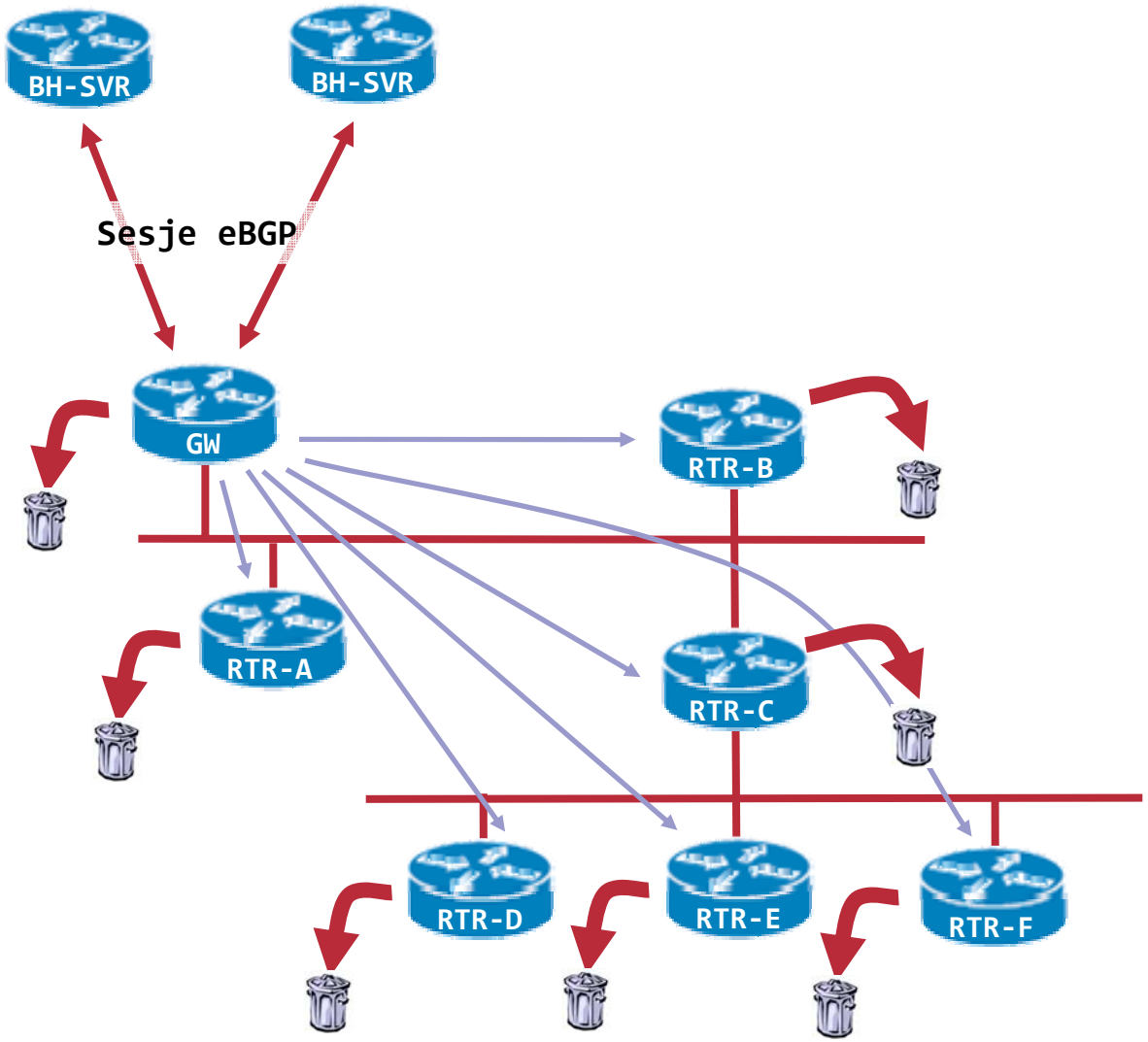
uRPF dla FreeBSD niezależny od filtra pakietów:
http://lukasz.bromirski.net/projekty/patches.html

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
- Dodatkowo, za pomocą dodatkowych skryptów można pokusić się o alarmowanie administratorów w przypadku wykrycia pojedynczego pakietu do przestrzeni z blackholingu!



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 ! w nowszych Quaggach zbędne
 [...]
```

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 192.0.2.1 255.255.255.255 Null0
ip community-list 99 permit 64999:666
!
route-map BH permit 10
 match community 99
 set ip next-hop 192.0.2.1
```

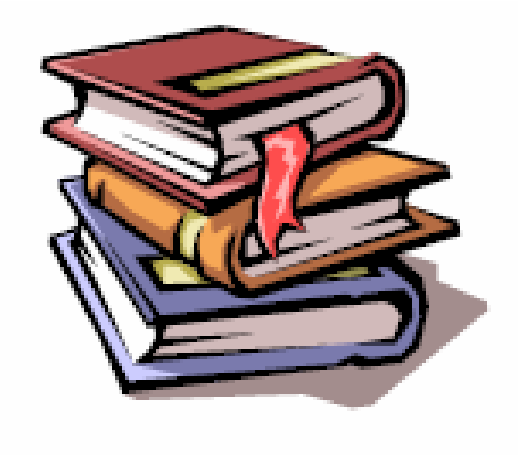
BGP blackholing

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    lo0
2                  127.0.0.1          UG1cB       0     2853    lo0
5                  127.0.0.1          UG1cB       0    11921    lo0
7                  127.0.0.1          UG1cB       0     4321    lo0
10                 127.0.0.1          UG1cB       0   184921    lo0
23                 127.0.0.1          UG1cB       0     9392    lo0
169.254            127.0.0.1          UG1cB       0    94812    lo0
172.16/12          127.0.0.1          UG1cB       0   119486    lo0
173.0/8            127.0.0.1          UG1cB       0    11602    lo0
174.0/8            127.0.0.1          UG1cB       0     6731    lo0
175.0/8            127.0.0.1          UG1cB       0      996    lo0
192.168.0/16       127.0.0.1          UG1cB       0    89483    lo0

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>
v1.2 18-iii-2006

OPIS PROJEKTU | KONFIGURACJE | REGULAMIN | FAQ | MATERIAŁY | UCZESTNICY

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 wrzucania 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

Strona projektu

http://networkers.pl/bgp-blackholing

BGP Blackholing PL statistics

```
Total prefixes served on 2006-05-09 17:55
      70

Prefixes served:
*>      1.0.0.0/8               64999   i
*>      2.0.0.0/8               64999   i
*>      5.0.0.0/8               64999   i
*>      7.0.0.0/8               64999   i
*>      10.0.0.0/8              64999   i
*>      23.0.0.0/8              64999   i
*>      27.0.0.0/8              64999   i
*>      31.0.0.0/8              64999   i
*>      36.0.0.0/8              64999   i
*>      37.0.0.0/8              64999   i
*>      39.0.0.0/8              64999   i
*>      42.0.0.0/8              64999   i
*>      49.0.0.0/8              64999   i
*>      50.0.0.0/8              64999   i
*>      69.13.31.57/32          64999   i
*>      77.0.0.0/8              64999   i
*>      78.0.0.0/8              64999   i
*>      79.0.0.0/8              64999   i
*>      92.0.0.0/8              64999   i
```

Dwa osobne LG:

Dostępne dla wszystkich:

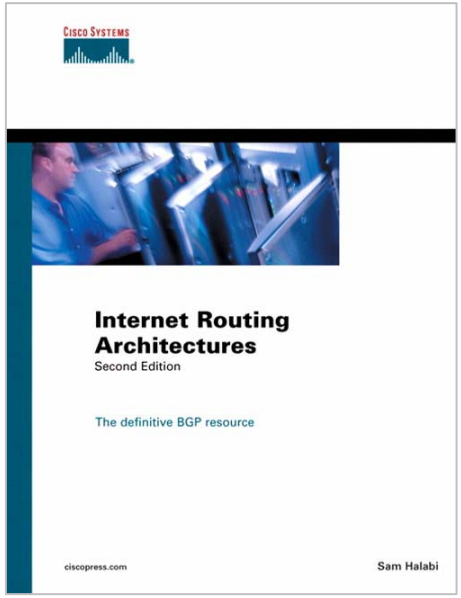
http://networkers.pl/bgp-blackholing/stats.html

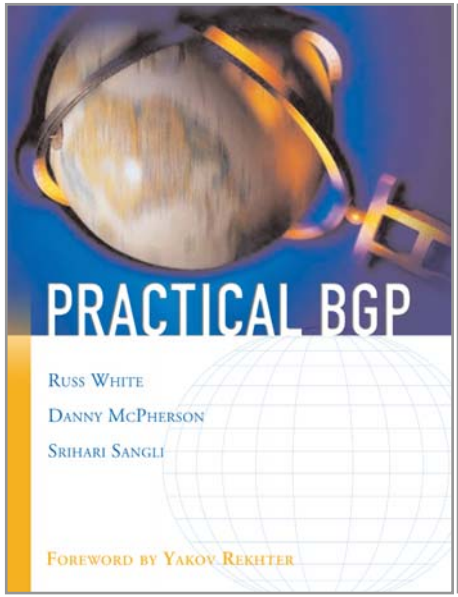
Dostępne dla członków projektu

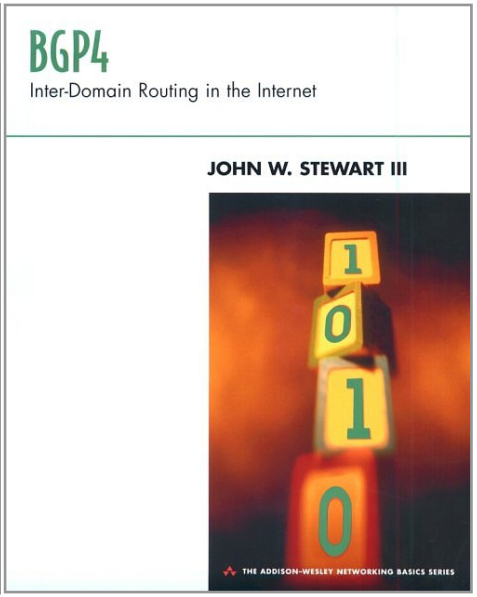
http://networkers.pl/bgp-blackholing/stats-login.html

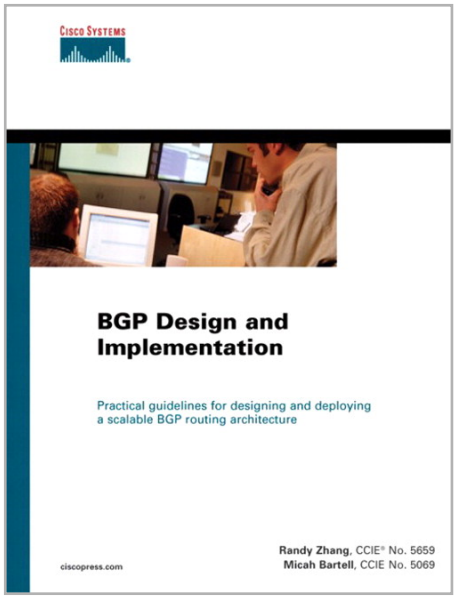
Książki

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


NO
QUESTIONS
VIOLATORS
WILL BE SHOT
SURVIVORS
WILL BE SHOT
AGAIN