www.widzew.net

Wdrożenie systemu ochrony przed atakami DDoS – **WANGUARD**

Piotr Okupski – STK TV-SAT 364

PLNOG 13 - 2014

Telewizja Kablowa

TV-SAT 364

- Obsługujemy ponad 7 tys. Klientów
- Usługi :TV, Internet, Telefon
- Sprzęt: Juniper, Cisco , D-Link
- Ponad 20 lat na rynku

Piotr Okupski

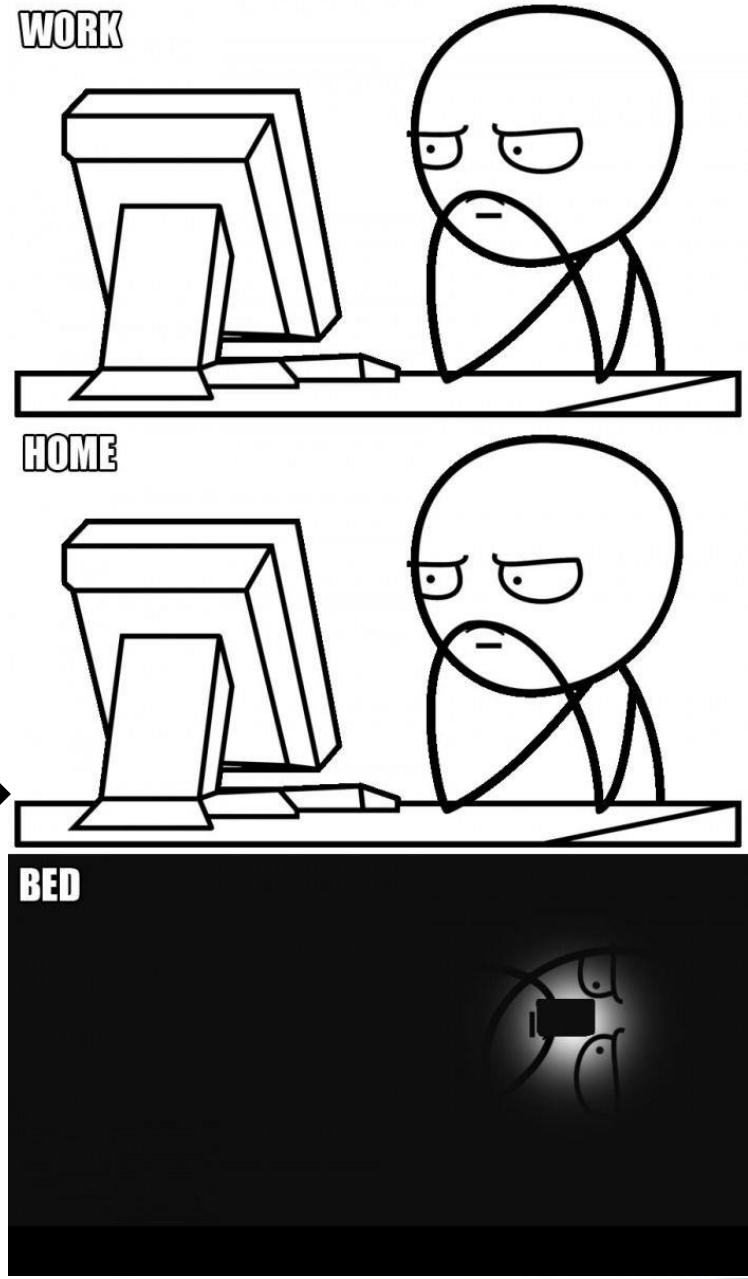
- Dyrektor Techniczny
- Administracja sieci i serwerów
- Rozwój i planowanie

Agenda

- Opis przypadku
- Tryby działania **WANGUARD**
- Wymagania techniczne i sprzęt dostępny na rynku
- Tuning serwera i systemu
- Konfiguracja **WANGUARD i Juniper MX**
- Szybkość działania systemu
- Dodatkowa ochrona routera - **Juniper** Routing Engine
- Przyszłość mechanizmów obrony przed atakami

Opis przypadku – Atak!

1. Atak DDOS na naszą sieć:
   - Głównie UDP Flood (NTP,DNS)
   - 3-4 dziennie po 3-5 minut przez 2 tygodnie
2. Przygotowania do obrony sieci
3. Wdrożenie systemu
4. Testy BGP i Blackholing
5. Tuning systemu



Przykładowe Ataki

Anomaly #90

Feb 16 15:23:47 - 15:27:07 (3m 20s)

Anomaly	Value	Affected	Traffic	Severity
Incoming TOTAL pkts/s > 20.0k	Highest: 82.6k Last: 195.9k	External Zone (91.193.160)	82.6k pkts/s 873.7 Mbits/s	

Details

Sensor	Response	IP Zone	Threshold	Totals	Actions
WAN	BGP Blackhole (Blackhole-Wanguard, Raport)	WAN-Classes (91.193.160.0)	20.0k	8.9 Mpkts 93.4 Gbits	

82.6k pkt/s

873.7 Mbit/s

Anomaly #129

Jun 25 18:28:47 - 18:28:57 (10s)

Anomaly	Value	Affected	Traffic	Severity
Incoming TOTAL pkts/s > 20.0k	Highest: 126.7k Last: 9.4M	External Zone (176.105.1)	126.7k pkts/s 454.8 Mbits/s	

Details

Sensor	Response	IP Zone	Threshold	Totals	Actions
WAN	BGP Blackhole (Blackhole-Wanguard, Raport)	WAN-Classes (176.105.128.0)	20.0k	1.2 Mpkts 4.5 Gbits	

126.7k pkt/s

454.8 Mbit/s

Anomaly #109

Mar 31 20:25:27 - 20:25:32 (5s)

Anomaly	Value	Affected	Traffic	Severity
Incoming TOTAL pkts/s > 20.0k	Highest: 159.6k Last: 352.5k	External Zone (91.193.160.)	159.6k pkts/s 594.1 Mbits/s	

Details

Sensor	Response	IP Zone	Threshold	Totals	Actions
WAN	BGP Blackhole (Blackhole-Wanguard, Raport)	WAN-Classes (91.193.160.0)	20.0k	1.2 Mpkts 4.4 Gbits	

159.6k pkt/s

594.1 Mbit/s

Wanguard (Subskrypcje Roczne)

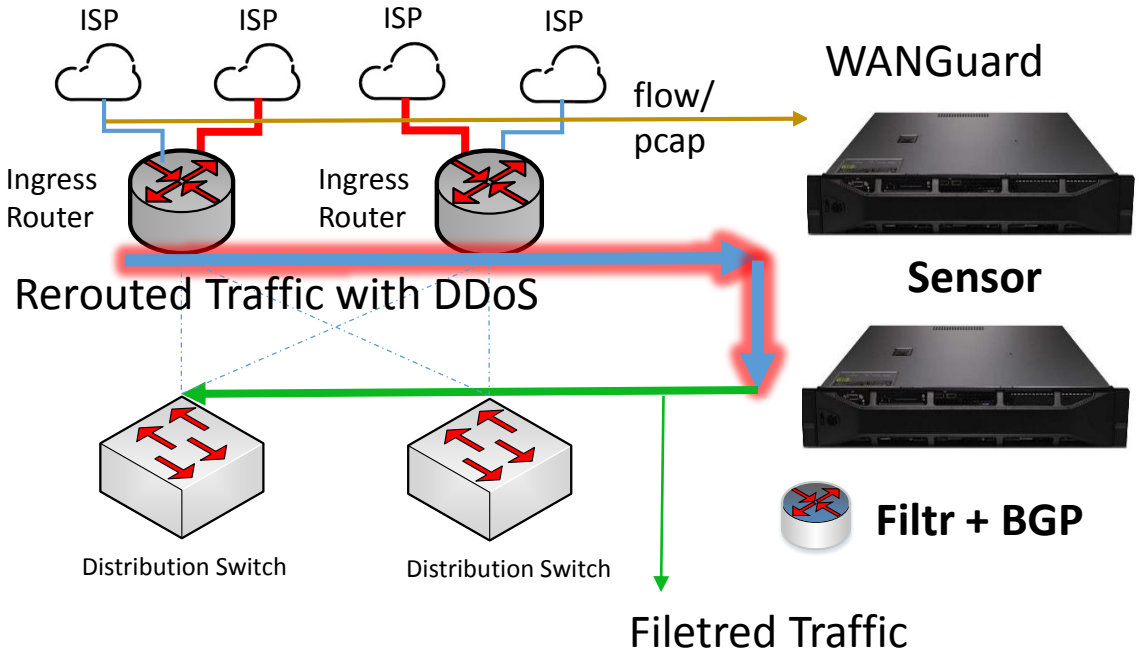
TV SAT 3G4

WANSight	WANGuard Sensor	WANGuard Filter
• Sensor flow/pcap • Wykresy, statystyki • Monitoring ruchu • **Nie obsługuje detekcji sygnatur ataku**	• Sensor flow/pcap • Wykresy, statystyki • Monitoring ruchu • **Detekcja sygnatur ataków**	• **Filtrowanie ruchu z sygnaturami ataku**
1140 PLN (345 $)	1962 PLN (595 $)	3281 PLN (995 $)

Kod rabatowy – 10% zniżki – `PLNOG2014`

Wanguard i tryby działania

Sensor i Filtr z routingiem BGP

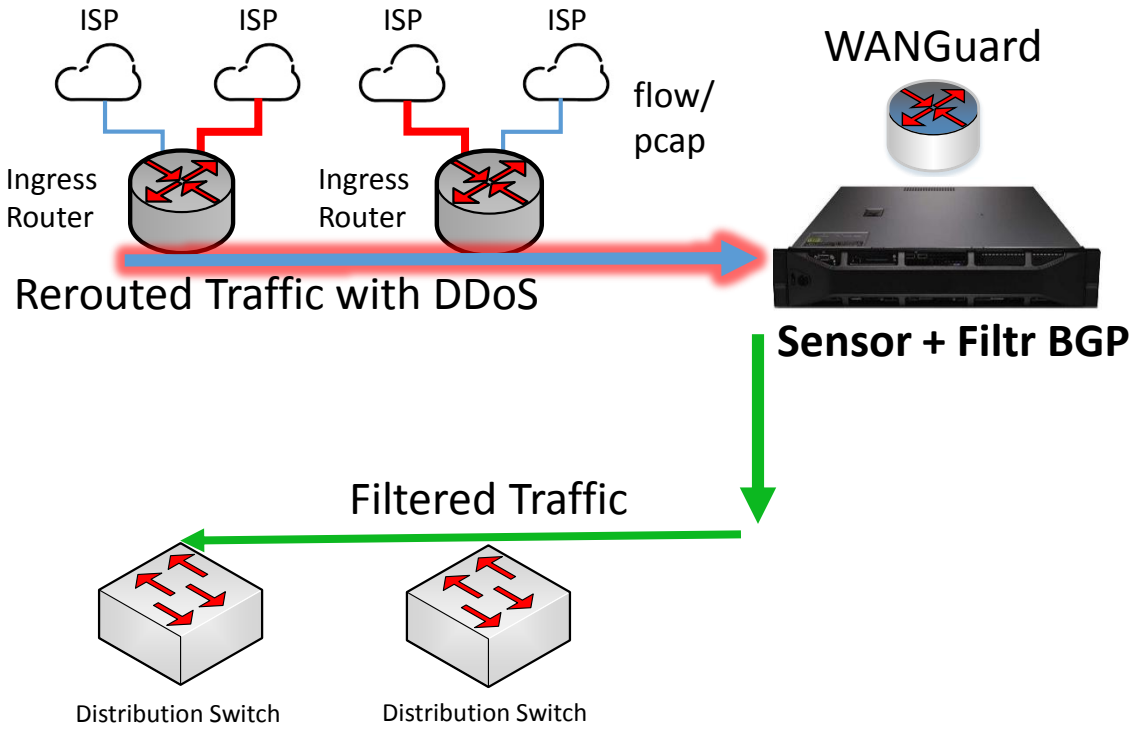


Opis działania:

- Wanguard po wykryciu podejrzanego ruchu wysyła update BGP do routera brzegowego, aby przełączyć ruch na filtr.
- Serwer filtrujący blokuje podejrzany ruch i przepuszcza tylko ruch właściwy bez sygnatur ataku.

Wanguard i tryby działania

Sensor i Filtr na tym samym serwerze jako router BGP

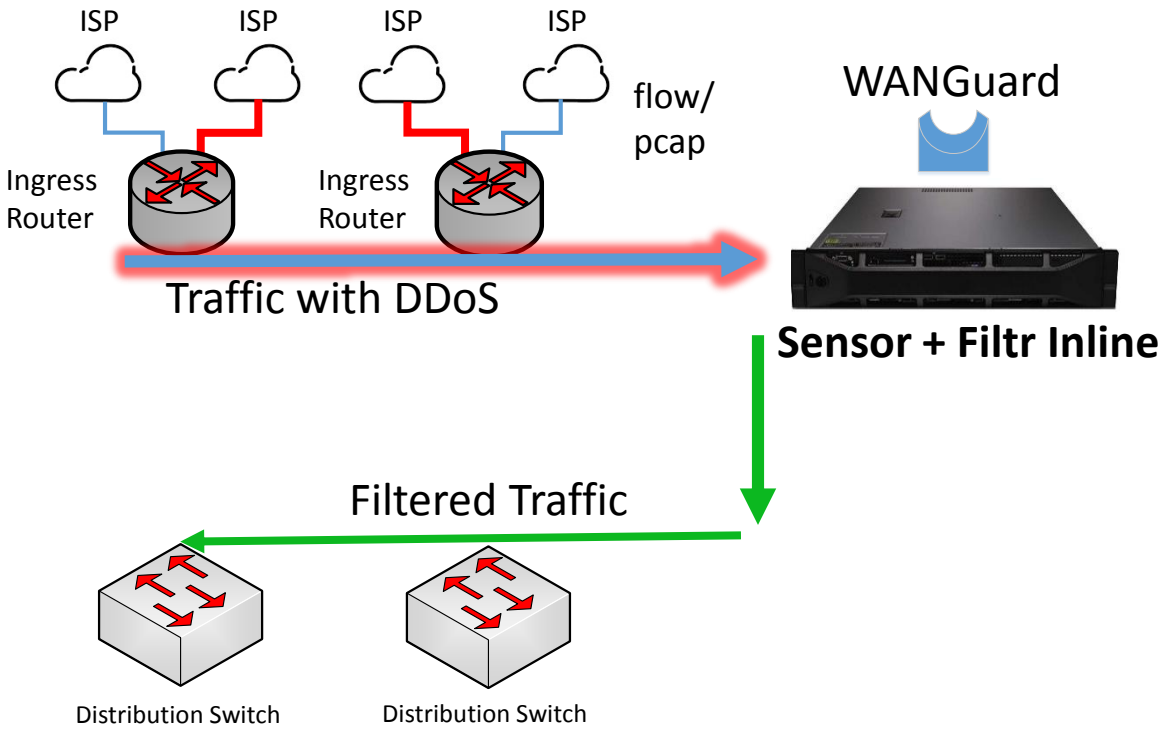


Opis działania:

- Sensor, Filtr i router BGP jest zainstalowany na tym samym serwerze w celu automatycznej filtracji ruchu przepływającego.

Wanguard i tryby działania

Sensor filtrujący jako bridge L2

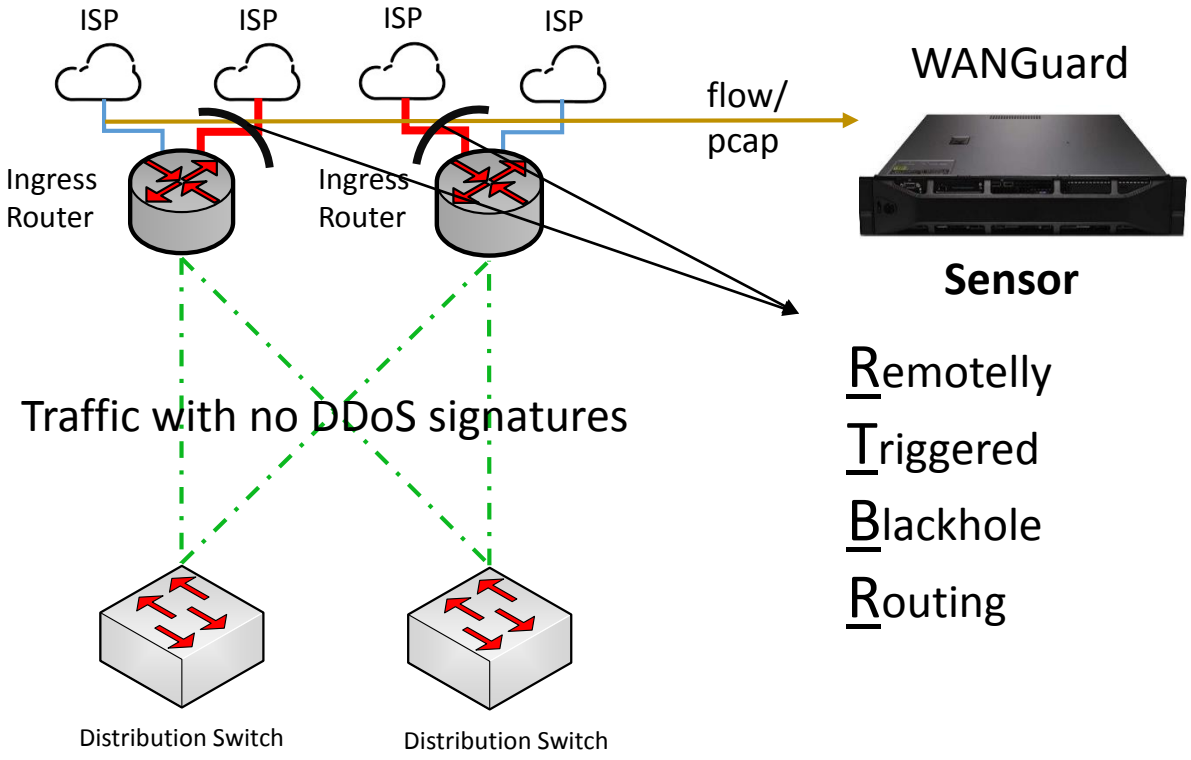


Opis działania:

- Sensor i Filtr jest bridgem przez, który przebiega cały ruch i filtruje ruch przepływający (INLINE).

Wanguard i tryby działania

Serwer w roli sensora w trybie sniffera pasywnego



Opis działania:

- Serwer otrzymuje kopie ruchu z RSPAN/Mirror portu/vlanu. Wychwytuje ataki oraz inne zagrożenia i może przesyłać te informacje w formie prefiksów IP do serwera BGP w celu blackholingu.

Opis działania **Systemu RTBH**

ATTACK

WANGUARD SERVER
(Sniffer & Quagga[BGP])

BGP Prefix 1.1.1.1/32
[42830:666]

SNIFFED TRAFFIC

ATMAN

BGP Prefix 1.1.1.1/32
[3257:2666]

Internet

TV-SAT 364

BGP Prefix 1.1.1.1/32
[24724:666,3257:2666]

BGP Prefix 1.1.1.1/32
[24724:666]

GTT

Wymagania techniczne Wanguard

Rozwiązania	Do 1 Gb/s	Do 10 Gb/s
Typ wdrożenia:	In-line lub out-of-line	Zalecane out-of-line
CPU:	2.5 GHz dual-core Xeon	2.8 GHz quad-core Xeon
RAM:	2 GB	8 GB
Karty Sieciowe:	2 x Gigabit Ethernet	1 x 10 GbE card (Intel 82599/x520/x540) 1 x Gigabit Ethernet lub Karty: Napatech / Emulex
System operacyjny:	RHEL / CentOS 5, RHEL / CentOS 6, OpenSUSE 12, Debian 6 / 7, Ubuntu Server 12	RHEL / CentOS 5, RHEL / CentOS 6, OpenSUSE 12, Debian 6 / 7, Ubuntu Server 12
HDD:	10 GB (wliczając system) + dane dla wykresów i statystyk	10 GB (wliczając system) + dane dla wykresów i statystyk

Karty sieciowe 1-100 Gb/s

Firma	Karta	Symbol	Cena*	Opcje sterowników (np. 0 % CPU)
Emulex (Endance) (1-10 GbE)	2 port 1GbE	DAG 7.5G2	800 -1200 $	• Producenta • PF_RING
	2 port 10 GbE	DAG 9.2X2	14000 $	
Intel (1-10)	2 port 10GbE	x520/x540	400-600 $	Alt.PF_RING – 250€/MAC
Mellanox	2 port 10GbE	MCX312A-XCBT	400$	
	2 port 40 GbE	MCX314A-BCBT	850$	
Myricom (10GbE)	1 port 10GbE	10G-PCIE2-8C-T	600 $	Sniffer10Gv2/v3 – 260$/530$**
	2 port 10GbE	…-8C2-2S	1100 $	
Napatech (1-100 GbE)	4-port 1GbE	NT4E2-4-PTP	5274 $*	• Producenta • PF_RING
	2-port 10GbE	NT20E2-PTP	13,562 $*	
	1-port 40GbE	NT40E2-1	13,562 $*	
	1 port 100GbE	NT100E3-1-PTP	33,908 $*	

*Ceny *MSRP (sugerowana cena producenta)* stan w 08.2014

** Wsparcie przez Wanguard 5.5 (dostępna nowa wersja w ciągu 2-3 miesięcy)

Optymalizacja systemu – BIOS

Opcja			Wartość
General	Operating Mode/PWR Profile		Maximum Performance
Procesor		C-States	Disabled
		Turbo mode	Enabled/Disabled (zależy od modelu)
		C1E	Disabled
		HT	Disabled
		Intel VT-x/i/c/d	Disabled
Memory		Memory Pre-Failure Notification	Disabled
Memory Speed			Maximum Performance
Memory Channel mode			Independent
Node Interleaving			Disabled/NUMA
Thermal Mode			Performance
Power Profile			Maximum Performance

Gotowe dokumentacje opisujące tuning systemów w celu uzyskania niskich opóźnień np.: DELL/HP/IBM [http://goo.gl/cxIvL1]

Optymalizacja systemu – Linux cz. 1

1. Wyłączamy **IRQ Balancer** i usuwamy z systemu(**1**)
2. Przypisujemy **kolejki RX/TX** kart sieciowych/portów do odpowiednich CPU(**2**)
   (**1** i **2** tylko w przypadku braku PF_RING lub innych driverów)
3. Ustawiamy **CPU Affinity** per proces **WANSniff**
   (ręcznie lub skryptem)
4. Ustawiamy **CPU Scalling Governor** jako ondemand [lub performance]

```
#cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
ondemand
```

Warto pamiętać, że każdy z tych parametrów zależy od wielkości i ilości pakietów.

Źródło: www.mellanox.com/related-docs/prod_software/Performance_Tuning_Guide_for_Mellanox_Network_Adapters.pdf

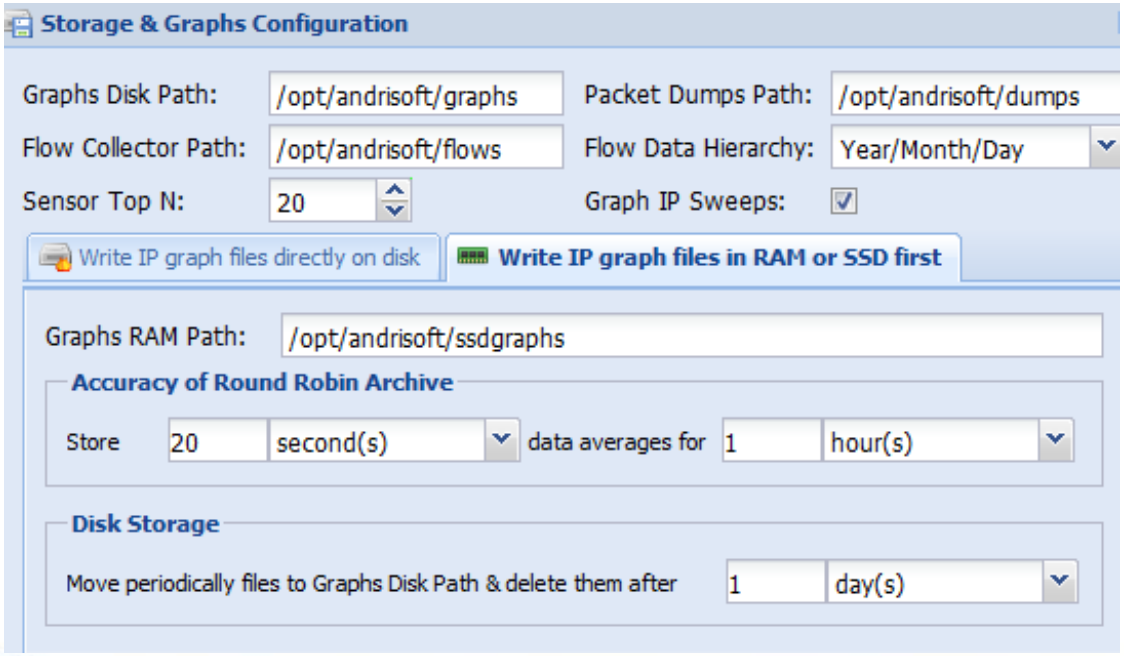
Optymalizacja systemu – Linux cz. 2

5. Ustawiamy **I/O Scheduler** na deadline dla dysków SSD na stałe w grub

```
title Red Hat Enterprise Linux Server (2.6.18-8.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18 ro root=/dev/sda2 elevator=deadline
```

```
# cat /sys/block/sda/queue/scheduler
noop [deadline] cfq
```

6. Ustawiamy export wykresów do RAM (tmpfs) lub na SSD

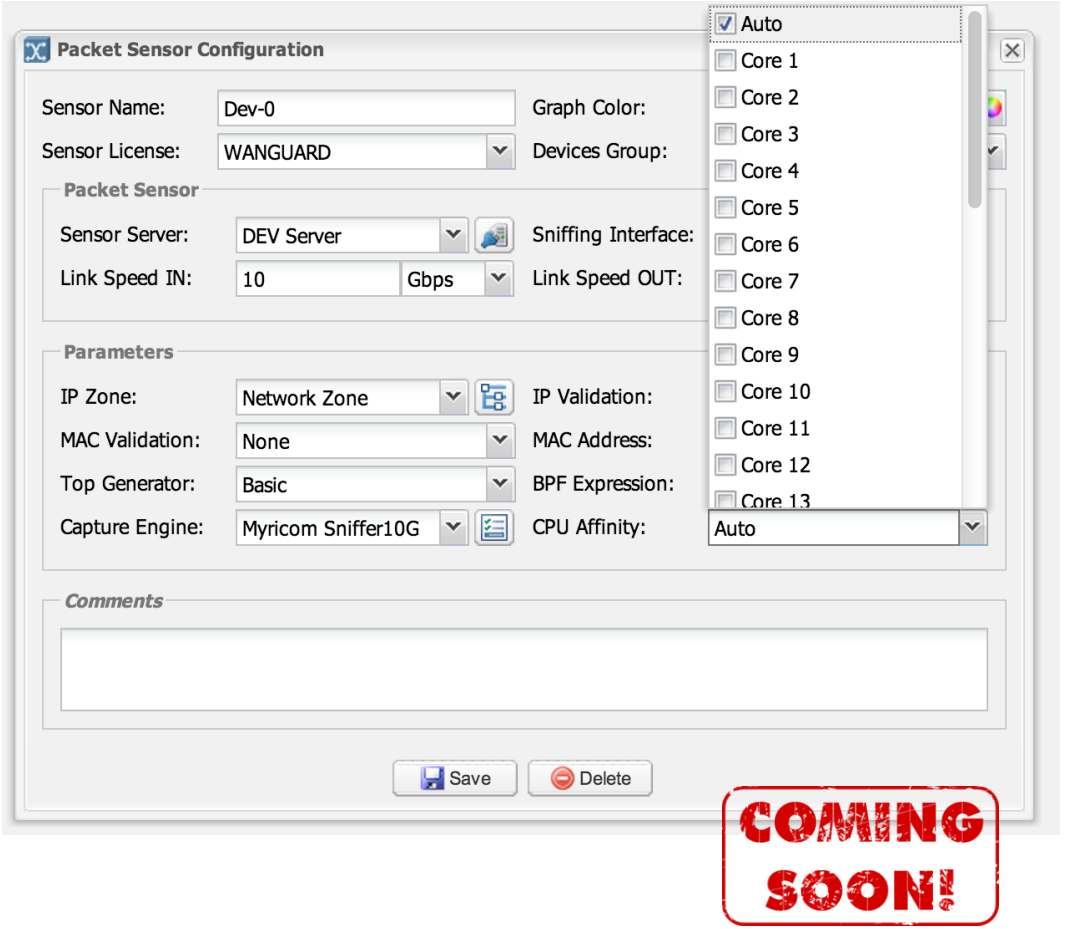


Skrypt przypisujący **WANsniff** per CPU

Wanguard 5.4
(brak przypisania CPU Affinity)

```
#!/bin/bash
CPU_WG=2
WG_SNIFF=`pgrep WANsniff`
for wpid in $ WG_SNIFF
do
 taskset -cp $CPU_WG $wpid
 CPU_WG=$[$CPU_WG +1]
done
```

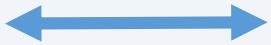
Wanguard 5.5
(wersja dostępna za 2-3 miesiące)

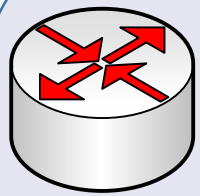


COMING SOON!

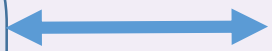
Schemat konfiguracyjny

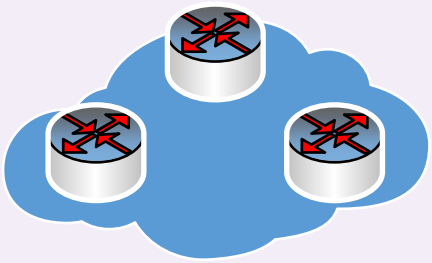
WANGuard Server
Sniffer + Quagga BGP





TV-SAT 364





ISP i Peeringi
(IX-y)

Konfiguracja Quagga – Juniper 1/2
[bgpd.conf] 1

Konfiguracja Quagga – Juniper 2/2
[bgp group IBGP-Wanguard] 2
[policy-statement import-Wanguard]

Juniper Polityka 1/2 3
[protocols bgp group EBGP-ATMAN]

Juniper Polityka 2/2 4
[policy-statement export-myAS-with-blackholing]

Konfiguracja Quagga – Juniper 1/2

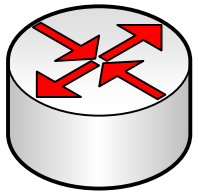
1

Konfiguracja QUAGGA

```
router bgp 42830
bgp router-id 10.0.0.2
neighbor 10.0.0.1 remote-as 42830
neighbor 10.0.0.1 description R1
neighbor 10.0.0.1 next-hop-self
neighbor 10.0.0.1 soft-reconfiguration inbound
neighbor 10.0.0.1 distribute-list nothing-in in
neighbor 10.0.0.1 route-map WANGUARD-Filter-out out
!
access-list nothing-in deny any
route-map WANGUARD-Filter-out permit 10
set community 42830:666
```

WANGuard Server
Sniffer + Quagga BGP
AS **42830**
IP **10.0.0.2**

Juniper



TV-SAT 364
AS **42830**
IP **10.0.0.1**

- Ustawiamy taki sam AS jak na naszym routerze.
- Tworzymy sesje iBGP.
- Dodajemy next-hop-self, aby umożliwić prawidłowy import prefiksów do eBGP.

666 – Blackhole Community

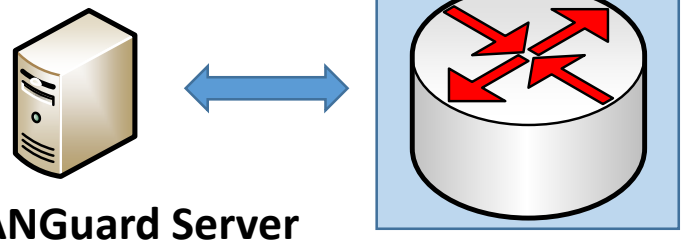
exa COMING SOON!

Konfiguracja Quagga – Juniper 2/2

2

Juniper

```
[protocols bgp group IBGP-Wanguard]
type internal;
description Wanguard-Blackholing;
family inet {
    unicast {
        rib-group only-inet.0;
    }
}
peer-as 42830;
neighbor 10.0.0.2 {
    no-advertise-peer-as;
    import import-Wanguard;
    export no-export;
}
```



WANGuard Server
Sniffer + Quagga BGP
AS **42830**
IP **10.0.0.2**

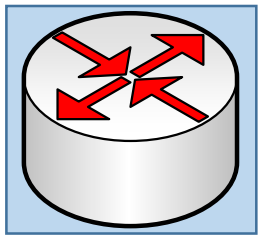
TV-SAT 364
AS **42830**
IP **10.0.0.1**

- Nie eksportujemy nic do Wanguard-a.
- Używamy polityki **import-Wanguard**, aby sterować co będziemy dalej robić z wykrytymi prefiksami podczas ataku.

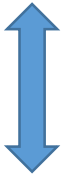
Juniper Polityka 1/2

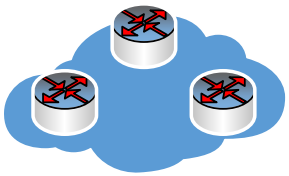
3

Juniper



TV-SAT 364

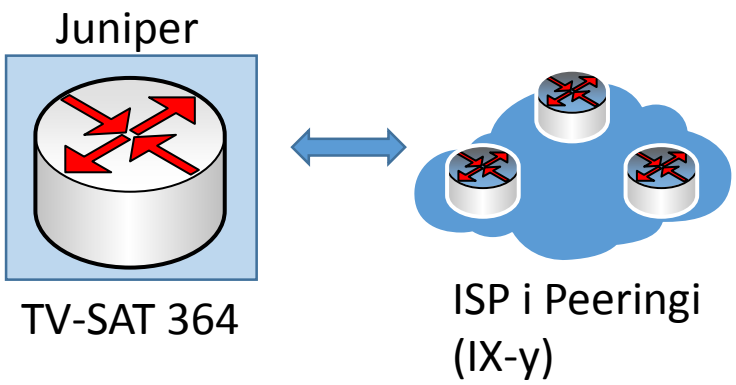




ISP i Peeringi (IX-y)

```
[policy-options policy-statement import-Wanguard]
term local_exceptions {
   from {
      protocol bgp;
      prefix-list local-exclude-from-blackholing;
            }
   then reject; }
term only_32_prefixes {
   from {
      protocol bgp;
      community com-wanguard;
      route-filter 2.2.2.0/22 prefix-length-range /32-/32;
      route-filter 3.3.3.0/20 prefix-length-range /32-/32;
   }
   then {
      community delete com-wanguard;
      community add blackhole-ATM;
      community add blackhole-GTT;
   accept;   }
            }
term last-deny-all {  then reject; }
```

Juniper Polityka 2/2 4



Juniper BGP

[edit protocols bgp group EBGP-ATMAN]
type external;
description ATMAN-World;
import import-atm-glob;
family inet {
  unicast {
    rib-group only-inet.0;
  }
}
export
export-myAS-with-blackholing;
peer-as 24724;
neighbor 193.x.x.x;

Juniper BGP

[edit policy-options policy-statement export-myAS-with-blackholing]
term blackhole {
from {
protocol bgp;
community [**blackhole-ATM blackhole-GTT**];
  }
  then accept;
}
term my-PI-prefixes {
  from {
    prefix-list PI-SPACE;
  }
  then accept;
}
term no-transit {
  then reject;
}
[edit policy-options]
community **blackhole-ATM** members 24724:666;
community **blackhole-GTT** members 3257:2666;
community **com-wanguard** members **42830:666**
community blackhole-providers members
[target:24724:666 target:3257:2666];

Jak szybko działa system ?

WANGUARD CONSOLE

Anomalies Dashboard | BGP Prefixes | Console | Anomalies | Packet Analyzers | All Sensors - Extended Tops

Actions: Clear Active Announcements

Rows Filtering Expression

№	Anomaly#	BGP Connection	IP Address	Mask	From	Until
145	-	BGP-Wanguard	9.9.9.9	32	2014-08-31 15:26:14	2014-08-31 15:27:14

15:26:14

570375	Console	BGP Interface	DEBUG	Sending BGP announcement # 145 requested by "admin"	2014-08-31 15:26:15

15:26:15

[Start update-u Juniper]

Aug 31 **15:26:18**.313185 BGP RECV 10.0.0.52+41386 -> 10.0.0.1+179 15:26:18

[Update do peerów]

Aug 31 15:26:18.315247 bgp_send: sending 59 bytes to 7x.x.x.x (External AS 3257)

Aug 31 15:26:18.315484 BGP SEND 9.9.9.9/32

Aug 31 15:26:18.316102 bgp_send: sending 59 bytes to 1x.x.x.x (External AS 24724)

Aug 31 **15:26:18**.316331 BGP SEND 9.9.9.9/32

[Koniec akcji:15:26:18.316331]

00:00:00.003146 = **3.146 ms – BGP, Całkowity czas** **4 sekundy !**

Dodatkowa ochrona routera Juniper RE (1)

Day One Book: Securing The Routing Engine on M/MX/T Series
– Douglas Hanks Jr. [http://goo.gl/648hrU]

Juniper Routing Engine (lo0)

```
lo0 {
    unit 0 {
        family inet {
            filter {
             input-list [ accept-bgp accept-common-services accept-established discard-all ];
            }
        }
        family inet6 {
            filter {
             input-list [ accept-v6-bgp accept-v6-common-services accept-established-v6 discard-
v6-all ];
            }
        }
    }
}
```

Dodatkowa ochrona routera Juniper RE (2)

Juniper accept-bgp filter

```
show firewall filter accept-bgp {
apply-flags omit;
term accept-bgp {
from {
 source-prefix-list {
                bgp-neighbors;
                bgp-neighbors-logical-systems;
}
destination-prefix-list {
                router-ipv4;
                router-ipv4-logical-systems;
}
                protocol tcp;
                port bgp;
}
then {
                count accept-bgp;
                accept;
}
}
```

Dodatkowa ochrona routera Juniper RE (3)

Juniper prefix listy

show policy-options prefix-list router-ipv4
apply-path “interfaces <*> unit <*> family inet address <*>”;

show policy-options prefix-list bgp-neighbors
apply-path “protocols bgp group <*> neighbor <*>”;

show policy-options prefix-list bgp-neighbors-logical-systems
apply-path “logical-systems <*> protocols bgp group <*> neighbor <*>”;

show policy-options prefix-list router-ipv4-logical-systms
apply-path “logical-systems <*> interfaces <*> unit <*> family inet address <*>”;

Opcja dla IPv6

show policy-options prefix-list router-ipv6

apply-path “interfaces <*> unit <*> family inet address **<*:*>**”;

Dodatkowa ochrona routera Juniper RE (4)

Juniper apply-path w akcji

show configuration policy-options prefix-list router-ipv4 | display inheritance
##
apply-path was expanded to:
x.x.x.x/30;
x.x.x.x/22;
x.x.x.x/30;
x.x.x.x/30;
x.x.x.x/23;

Juniper BGP hold-time (czas rozpięcia sesji BGP)

[edit protocols bgp group EBGP-przykład]
type external;
description Sesja_EBGP_przyklad;
hold-time 90; [Domyślnie 90 sekund, 0 blokuje]
import import-policy;

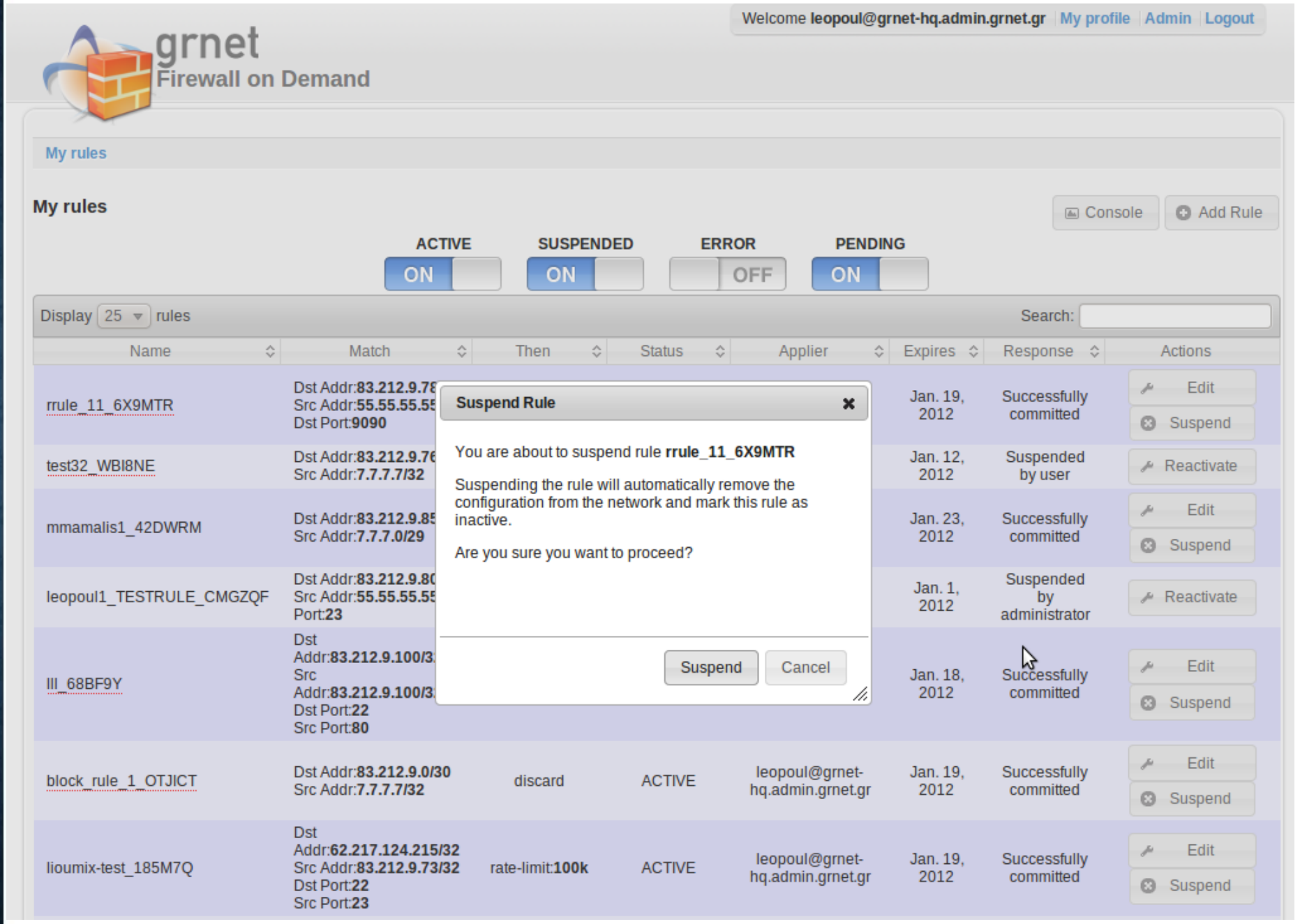
Co nowego na froncie DDoS?

FlowSpec RFC 5575

1. Juniper – wsparcie od JUNOS 7.3
   Od JUNOS 15.x wsparcie dla ISSU/NSR,
   Redirect i IPv6 – w planach
2. eXaBGP – FlowSpec READY!
3. WANGUARD wsparcie FlowSpec – COMING SOON!
   obecnie tylko współpraca z WANFilter i własne skrypty.

4. Firewall on Demand –
http://code.grnet.gr/projects/flowspy/

Firewall On Demand



Punkty Wymiany Ruchu i wsparcie RTBH

Nazwa IX-a	Wsparcie RTBH	Strona WWW
EPIX	TAK √	www.epix.net.pl
KIX	TAK √	tanielacze.pl
PLIX	TAK √	www.plix.pl
THINX	TAK √	www.thinx.pl
TPIX	TAK √	www.tpix.pl

Piotr Okupski

okupski@widzew.net

Specjalne podziękowania dla Adama Wiechnika @ ATMAN