

Správné místo pro vaše data



NAŠE CENTRA V PRAZE I V BRNĚ

 **master**
data in motion

DDoS útoky a jak se jim bránit

WUG Praha 6.4.2016

Martin Žídek, CTO Master Internet

Úvod

Cíl přednášky – „Seznámit se s dostupnými typy ochrany proti DDoS útokům“

Jak je definován DDoS

- Distributed
- Denial of Service

Neexistuje univerzální ochrana

Agenda

Zdroje, cíle a důvody útoků ?

Typy útoků

Typy ochran a jejich nasazení

Ochrana pomocí Radware Defense Pro

Cíle útoků

2015-2016

radware
GLOBAL APPLICATION
& NETWORK SECURITY
REPORT

Vysoké riziko - ISP, Hosting Services, Governments, Education

Střední riziko - Financial, Health, Retail, Mobile

Nízké riziko - Energy & Utility, Individuals

Cílem může být každý – s útoky je nutné předem počítat.

602 Gbps! This May Have Been the Largest DDoS Attack in History

Friday, January 08, 2016 Swati Khandelwal

 285  8.5K  8608  1216  127  17.4K



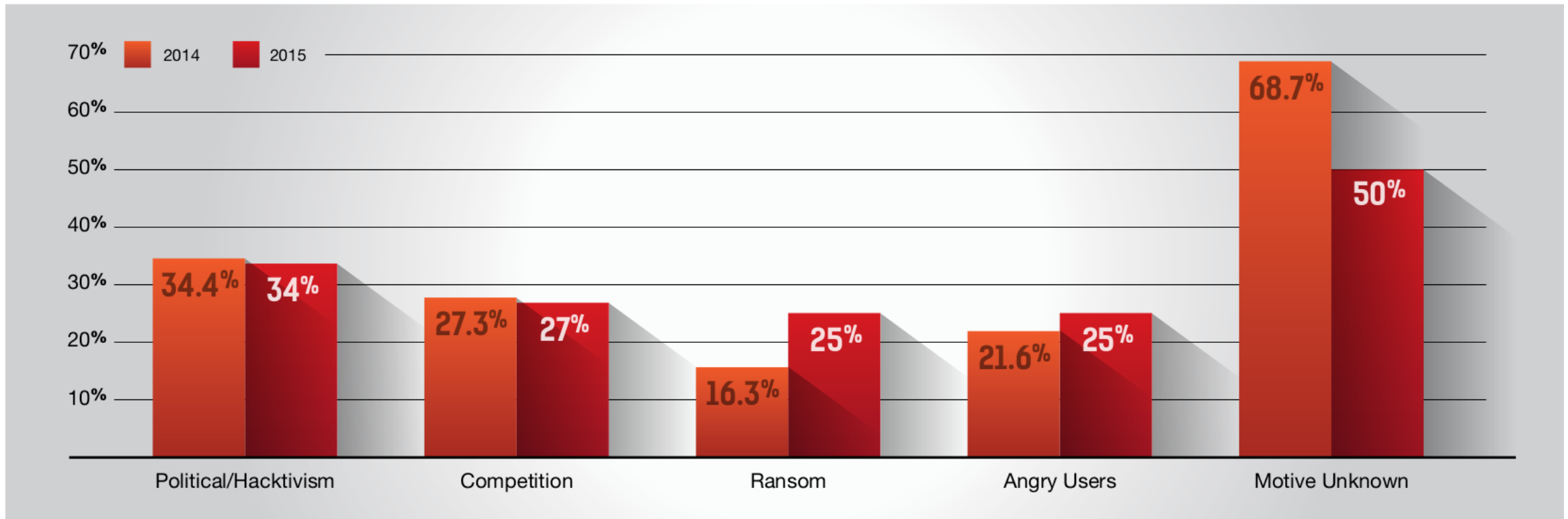
Cyber attacks are getting evil and worst nightmare for companies day-by-day, and the *Distributed Denial of Service (DDoS)* attack is one of the favorite weapon for hackers to temporarily suspend services of a host connected to the Internet.

Until now, nearly every big website had been a victim of this attack, and the most recent one was conducted against the **BBC**'s websites and Republican presidential candidate **Donald Trump**'s main campaign website over this past holiday weekend.

2x více než maximum
v IX nix.cz

Důvody útoků

Which of the following motives are behind any cyber-attacks your organization experienced?



Zdroje útoků

Vyhackované počítače / botnety

Špatně zabezpečené UDP služby (DNS/NTP...)

Staré verze CMS– Drupal, WordPress, Joomla

SOHO routery

DDoS-as-a-Service - „Gwapo’s Professional DDOS”

IoT (“Botnets of Things”)

Časem budou využívány určitě i vyhackované mobily

Typy útoků

UDP Amplification Attacks – UDP (DNS, NTP, CharGen, SNMP,..)

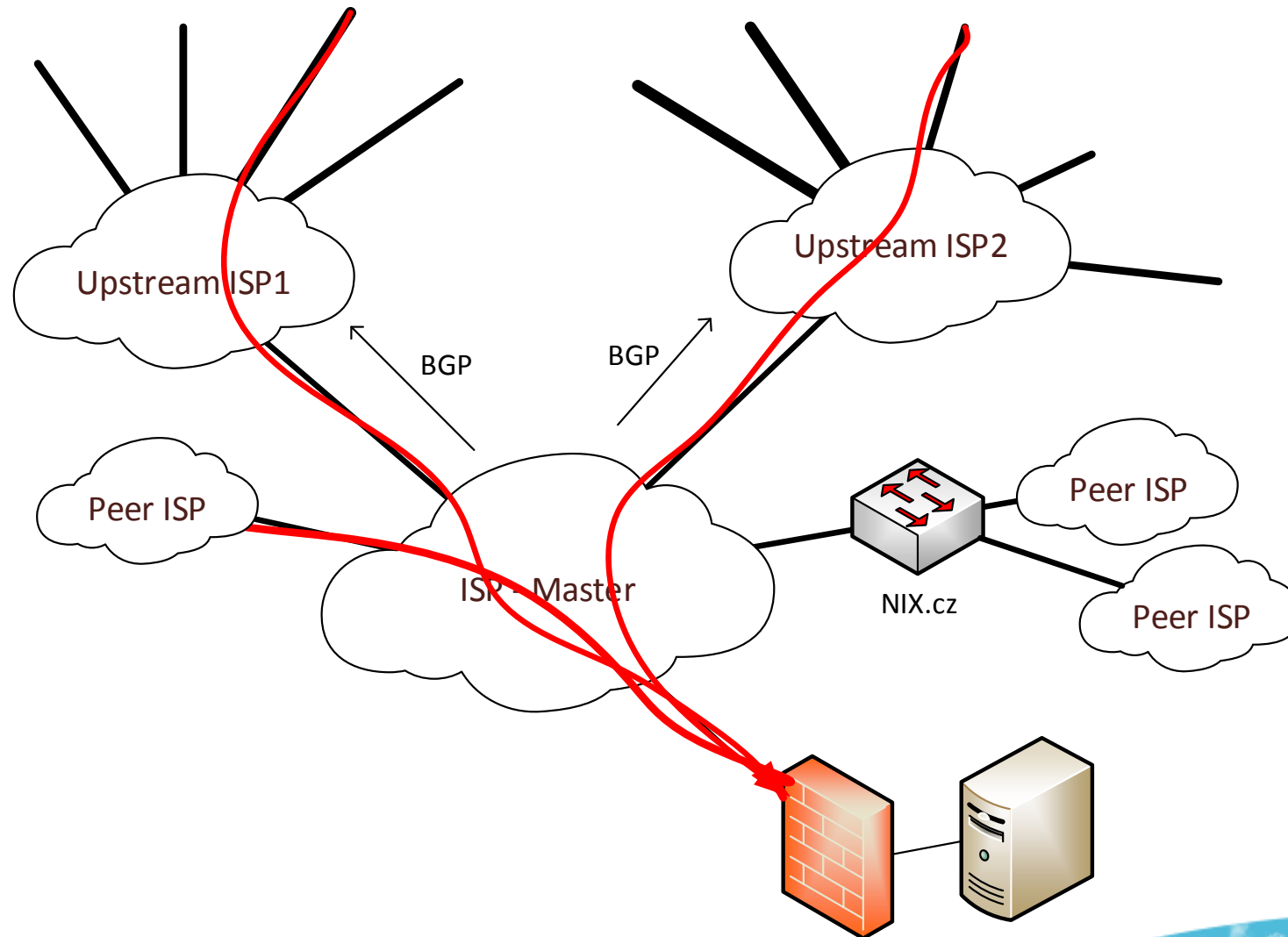
Stateless Protocols Attacks – UDP, ICMP Flood – spoofed source

Stateful Protocols Attacks - SYN Flood, HTTP based, SSL, SIP, ...

Application and Slow Pace Attacks - Slowloris, Brute Force, SQL injections, XSS, PHP code injection ...

Nárůst multi vector a burst útoků

Jak útok vypadá



Jak funguje routing

Router se rozhoduje jen podle cílové IP adresy

V routovací tabulce je preferován vždy specifitější prefix

UDP Amplification Attacks

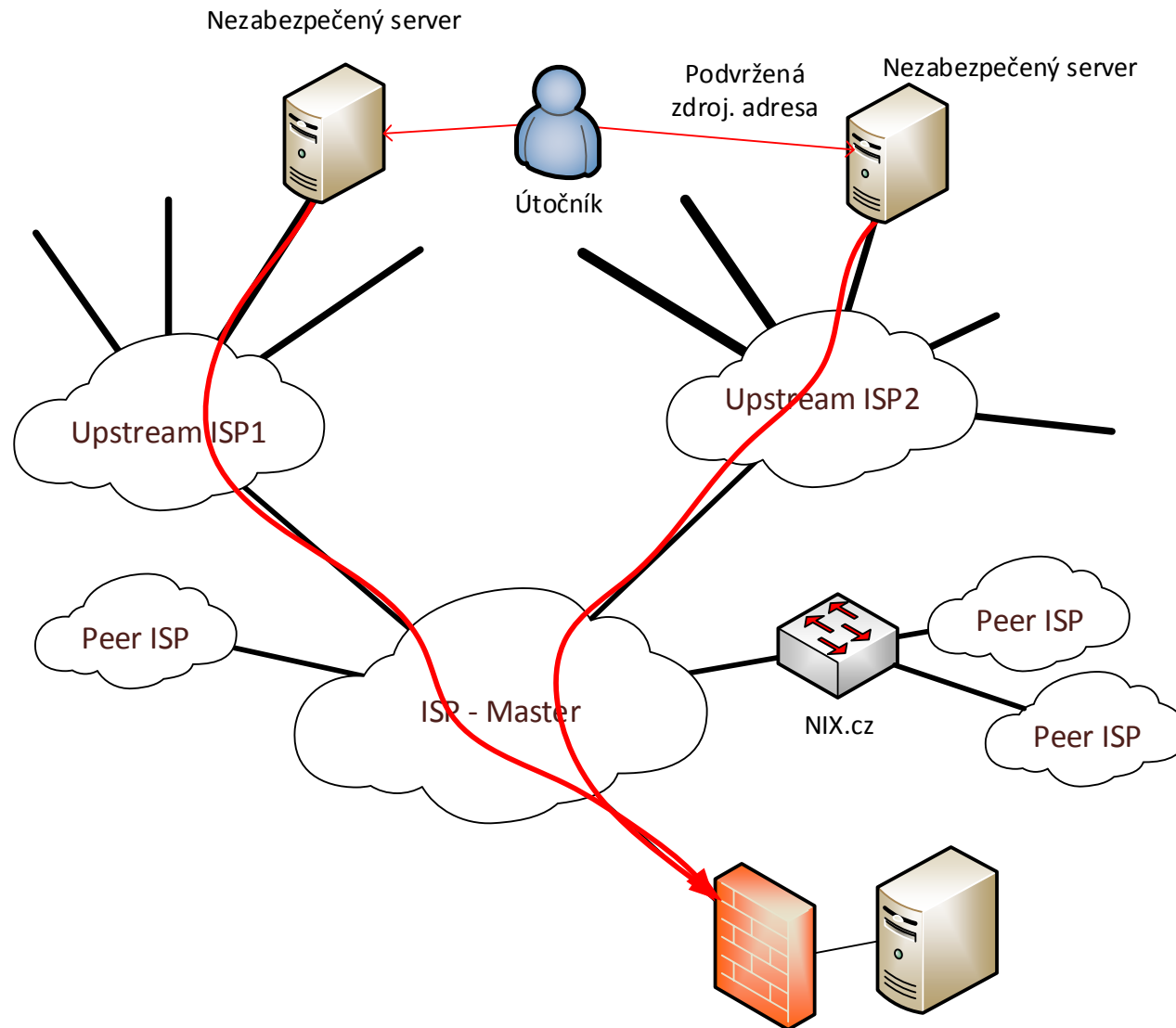
Spoofed source - UDP (DNS, NTP, CharGen, SNMP,..)

Protokol	Zesílení	Příkaz
DNS	28 - 54	
NTP	556.9	
SNMPv2	6.3	GetBulk request
SSDP	30.8	SEARCH request
NetBIOS	3.8	

Problém filtrace zdrojových IP u ISP (BCP-38)

Cíl – saturace linek

UDP Amplification Attacks



UDP Amplification Attacks

Rychlý scan – snadné a levné pro útočníka

Zabezpečení

- <http://openresolverproject.org/>
- <http://openntpproject.org/>
- Poměrně snadná filtrace pro ne UDP služby

Stateless Protocols Attacks

TCP Fragmentation Flood

UDP Flood

UDP Fragmentation Flood

ICMP Flood

IGMP Flood

Zdroje botnety – CMS, malware

Cíl – saturace linek

Stateful Protocols Attacks

SYN Flood

TCP ACK + FIN Flood

TCP RST Flood

TCP SYN + ACK Flood

HTTP/HTTPS Flood

SIP

Menší objem – cíl zaplnění stavových tabulek

Application and Slow Pace Attacks

Slowloris

Brute Force

SQL injections, XSS ...

Řeší se na straně aplikace nebo klasická IDS/IPS, WAF

Nejmenší objem dat.

Kde pracují ochrany

Podle typu útoku - saturace linek

- Nedošlo k saturaci – možno řešit lokálně scrubbing
- Došlo k saturaci – je nutno řešit přes saturovanou linkou

Typy ochran – v síti ISP, upstream ISP

Filtrace – podle granularity

- BGP RTBH (Realtime blackhole) dest / source
- ACL Filtry
- Limited scope – Fenix, RTBH v transitu
- BGP FlowSpec

Scrubbing – podle umístění

- on demand – central, distributed – Arbor
- in line – Radware
- mixed

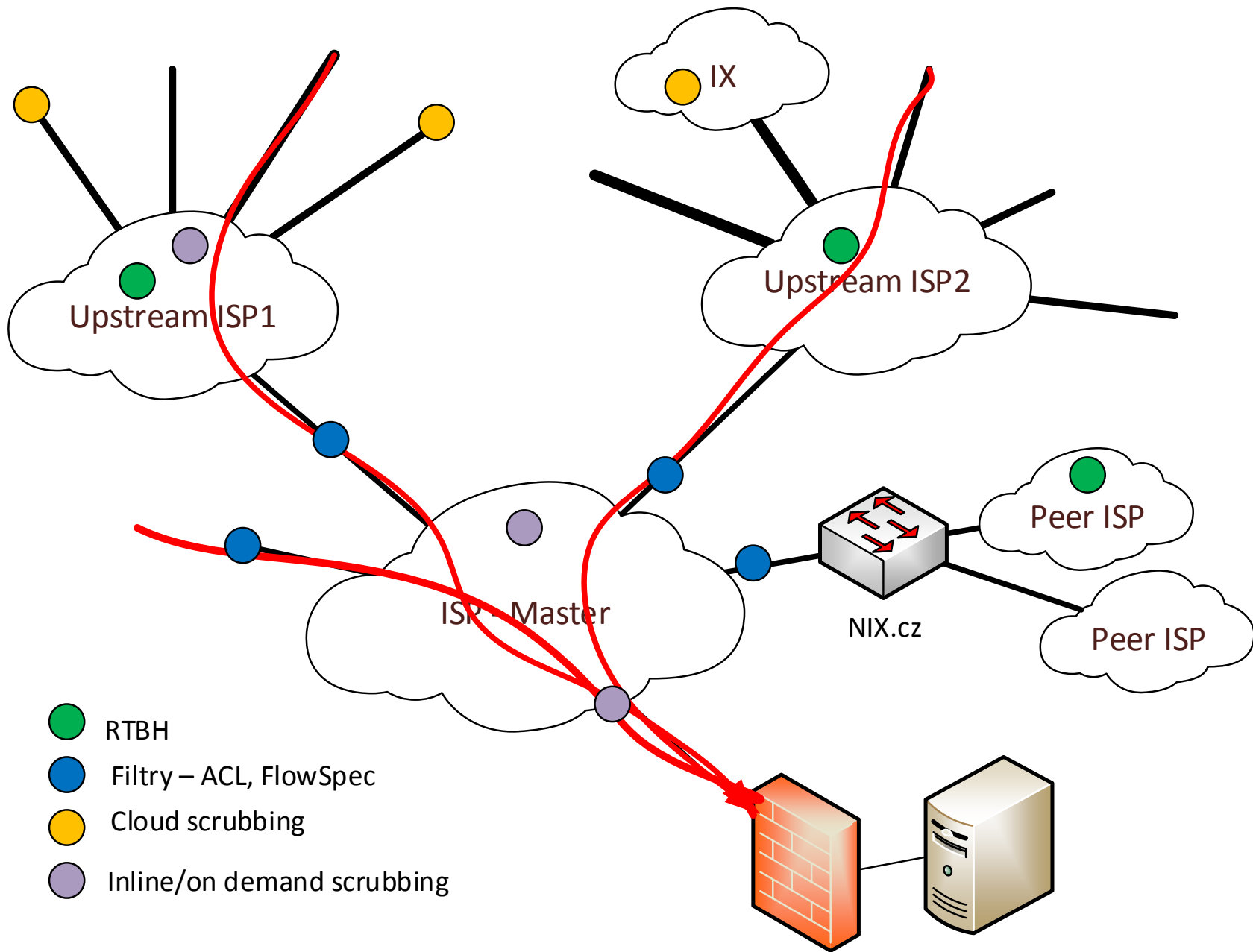
Typy ochran – Cloud

Založené na DNS – Cloudflare, Prolexic (Akamai), Impreva
Incapsula, Radware DefensePipe

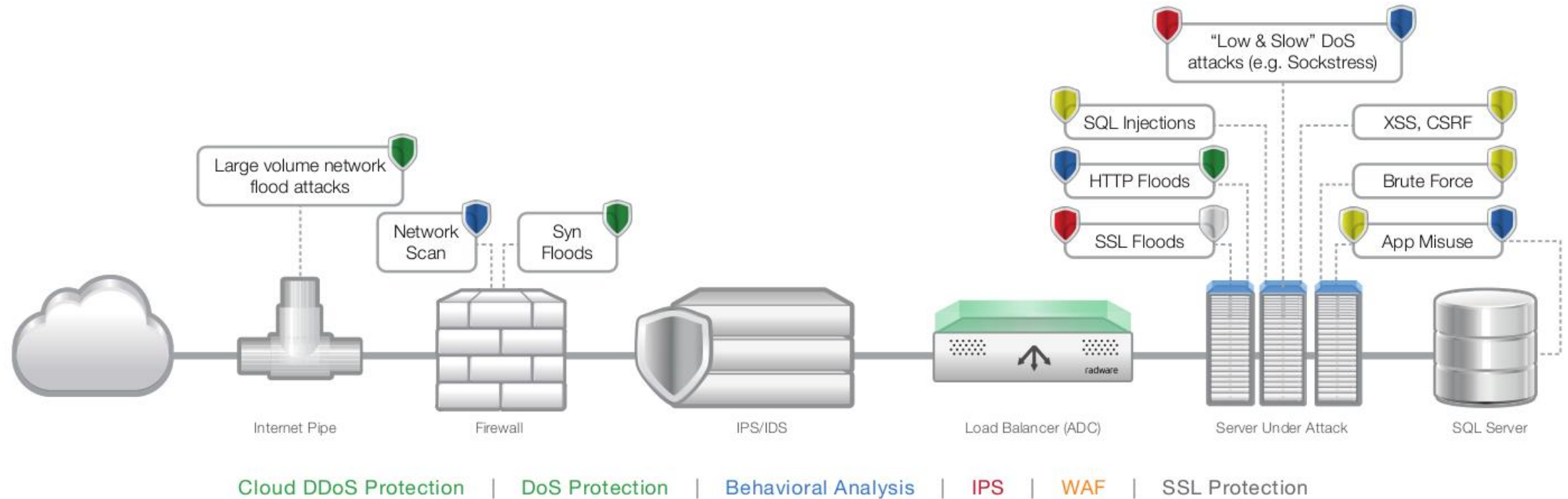
Založené na BGP - Radware DefensePipe

Typy ochran – Hybridní

Radware DefensePro + DefensePipe



Řetězec přípojení



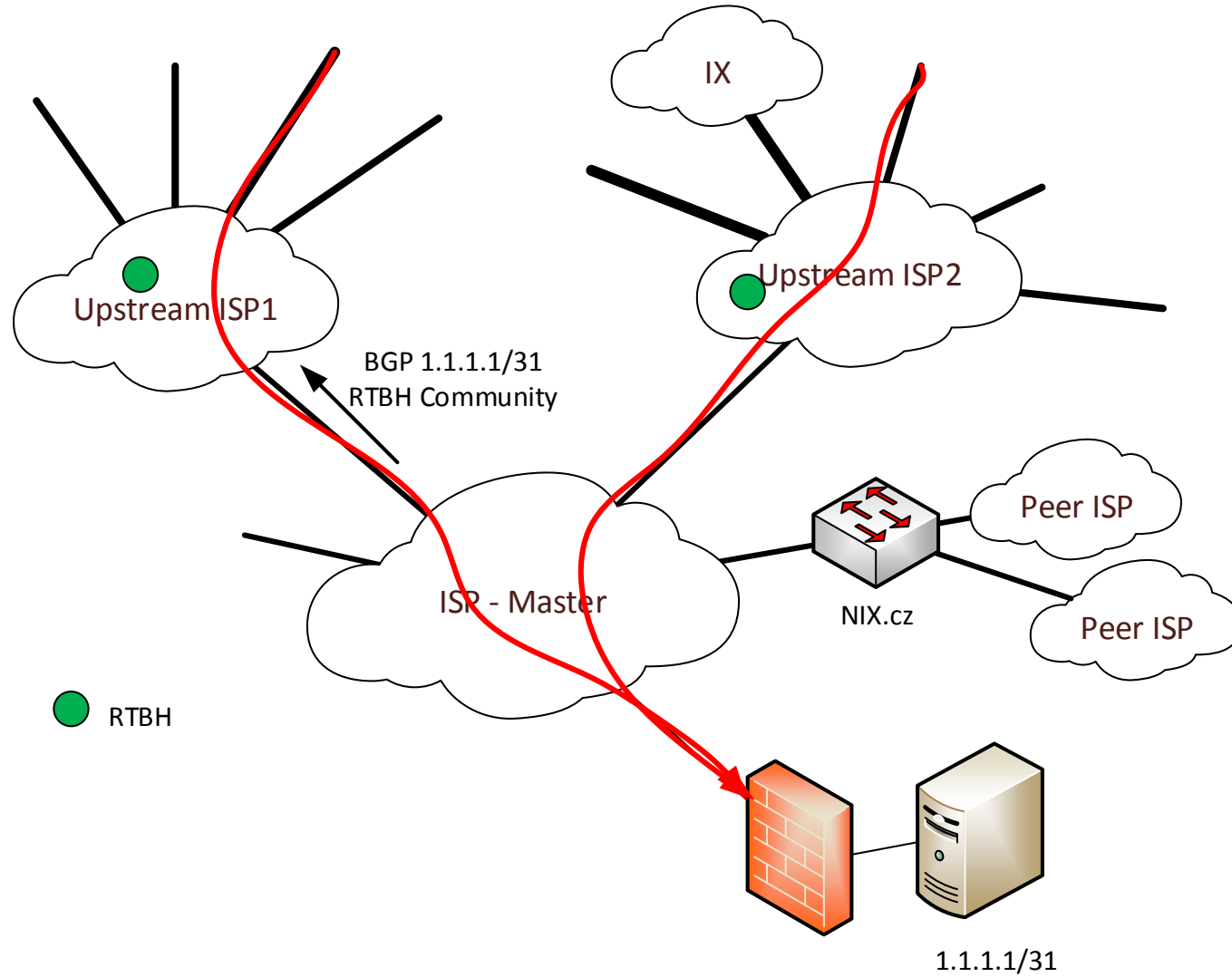
Filtrace

- BGP RTBH (Realtime blackhole) dest / source – collateral damage
- Limited scope RTBH – Fenix, RTBH v transitu
- ACL Filtry
- BGP FlowSpec

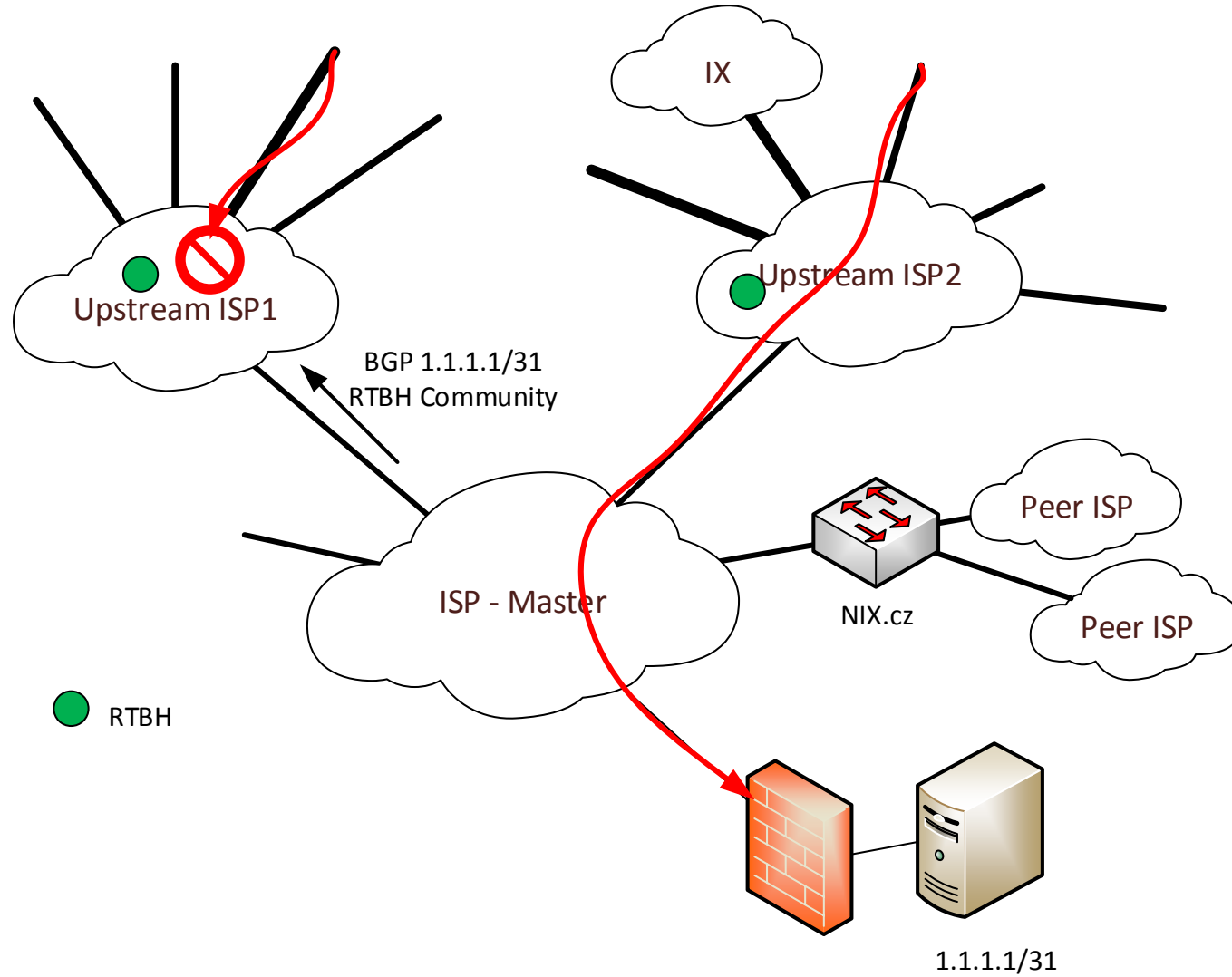
Filtrace – BGP RTBH

- Výhoda – možnost nastavení zákazníkem
- Nevýhoda – někdy není podporováno ISP, blackhole – splněn cíl útočníka
- Limited scope RTBH – Fenix, RTBH v transitu

Filtrace – BGP RTBH



Filtrace – BGP RTBH



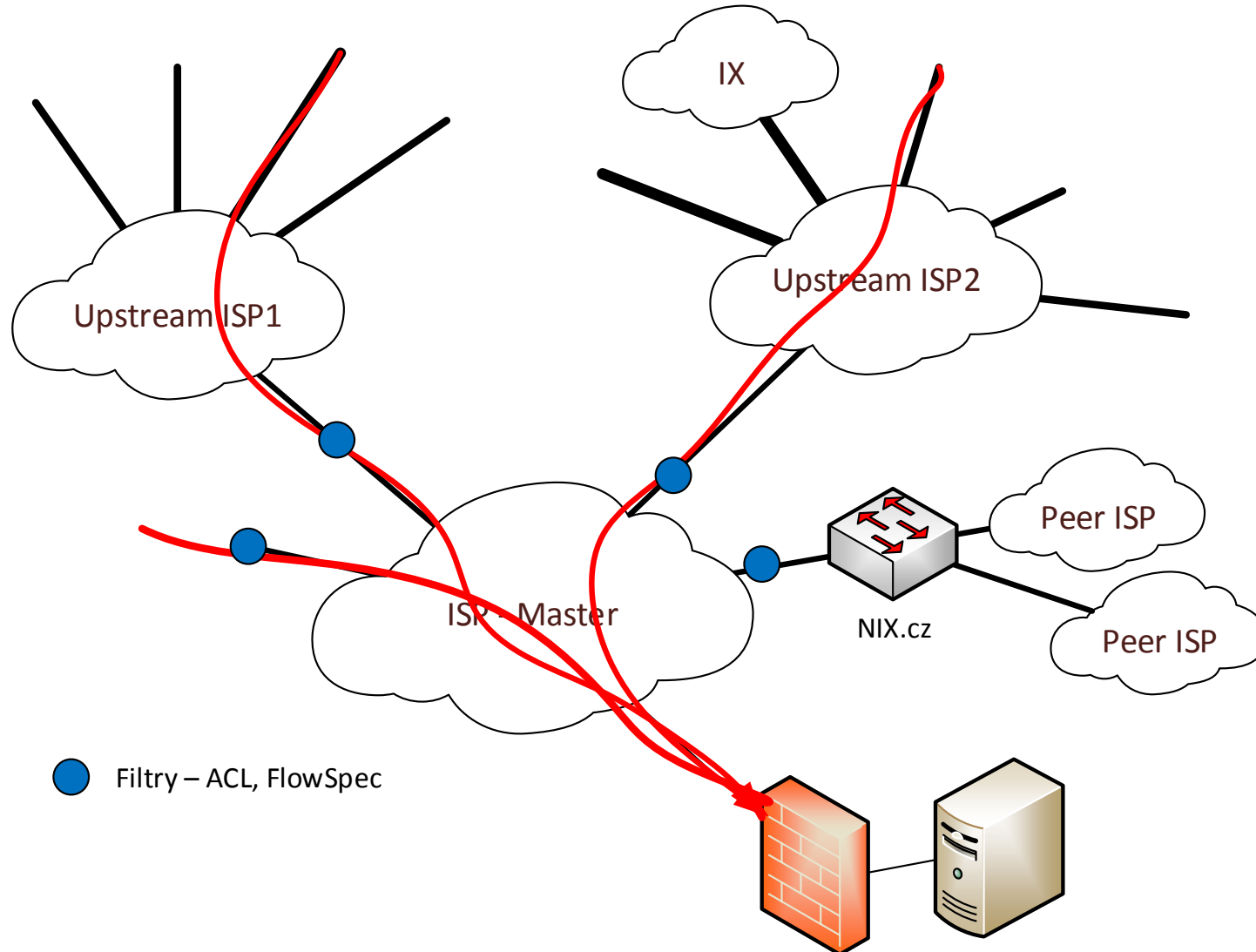
Filtrace - ACL

Nestavové

```
deny udp 192.168.190.100 0.0.0.1 host 192.168.190.200 eq 53
```

Nevýhoda – ruční konfigurace přes NOC

Filtrace - ACL



Filtrace – BGP Flowspec

Signalizace filtrů pomocí BGP / RFC5575

Akce

- Traffic rate
- Redirect
- Mark

Výhoda - Automatické generování, pokud podporuje ISP

Nevýhody - malá podpora u poskytovatelů, omezené množství

Scrubbing - Cloud

Přesměrování DNS chráněné domény na DNS servery providera.

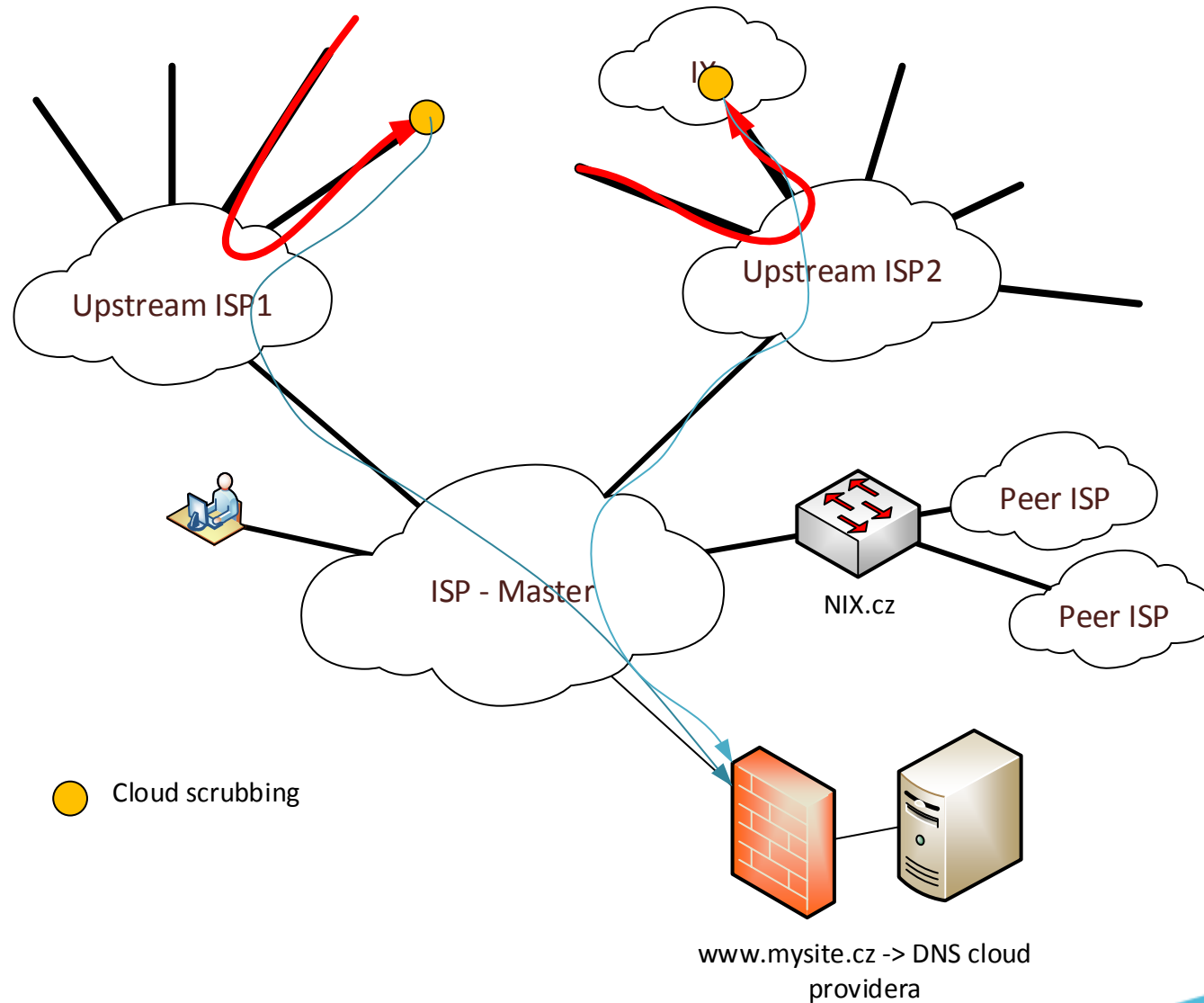
Princip CDN.

V každém regionu jiná IP – IP scrubbing centra

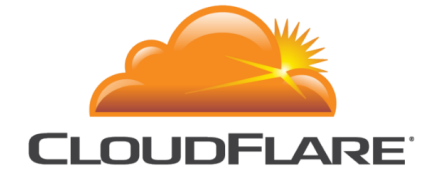
Rozmělnění útoku

Nevýhody - zjištění skutečné IP zdroje, složitý monitoring

Scrubbing - Cloud



Scrubbing - Cloud



Scrubbing - Cloud

Propagace v BGP specifictějšího prefixu od providera

Rychlost reakce

GRE/IPsec tunel k cílovému serveru

Scrubbing – Out of path

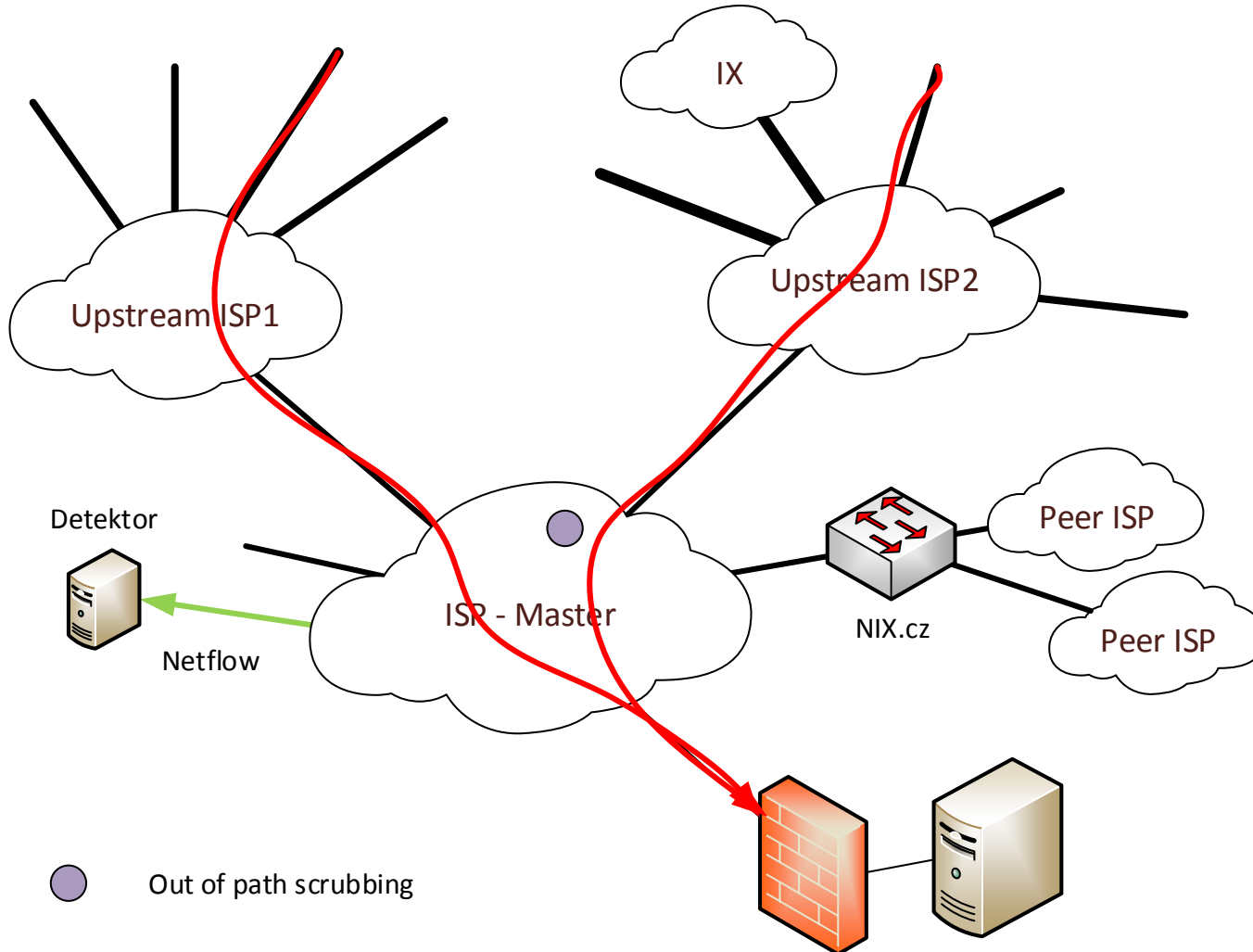
Přesměrování provozu do scrubbing centra, distribuovaný scrubbing

Pomalá reakce – nutnost zásahu NOC

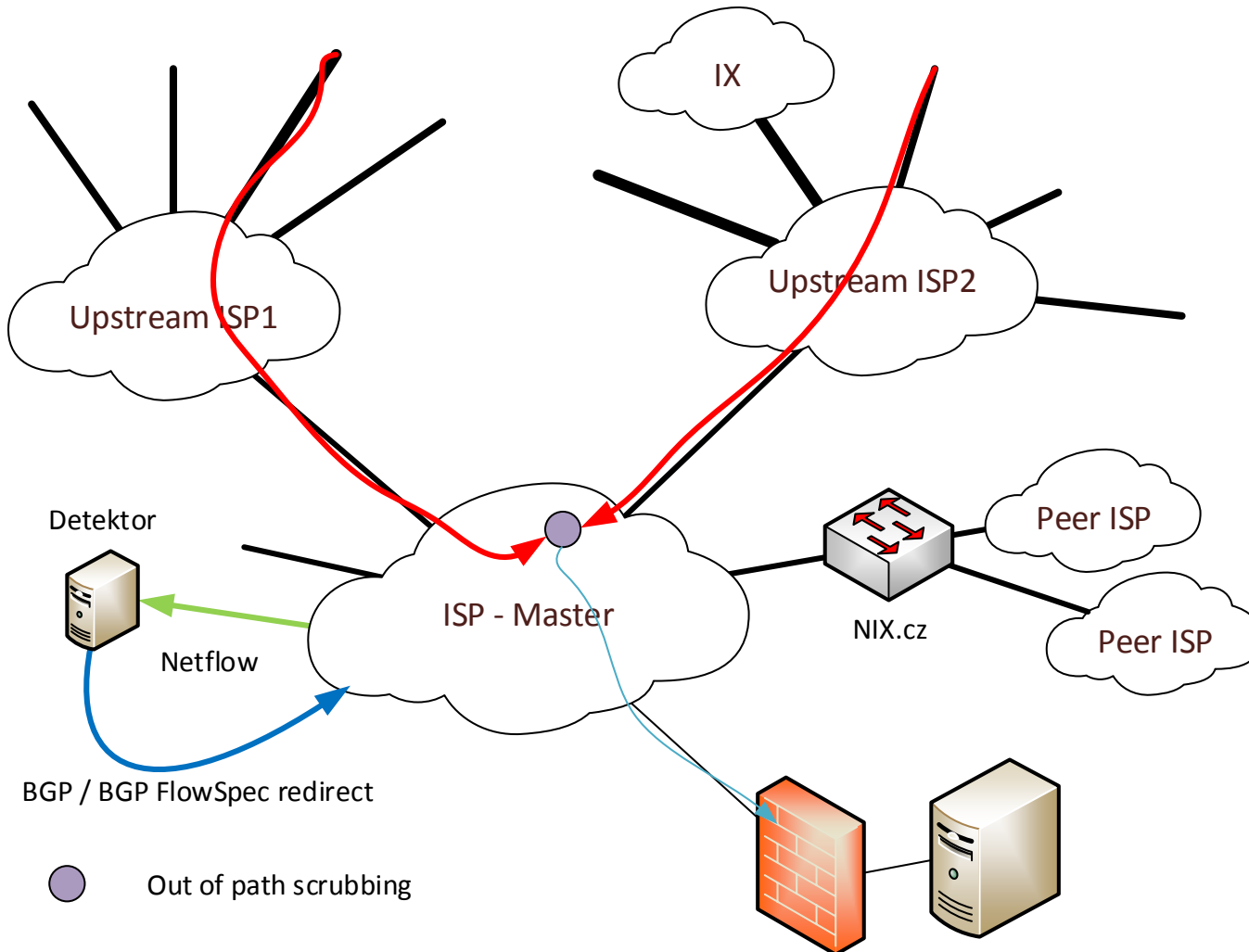
Výhoda – provoz neprochází ochranou

Nevýhoda – pomalost detekce

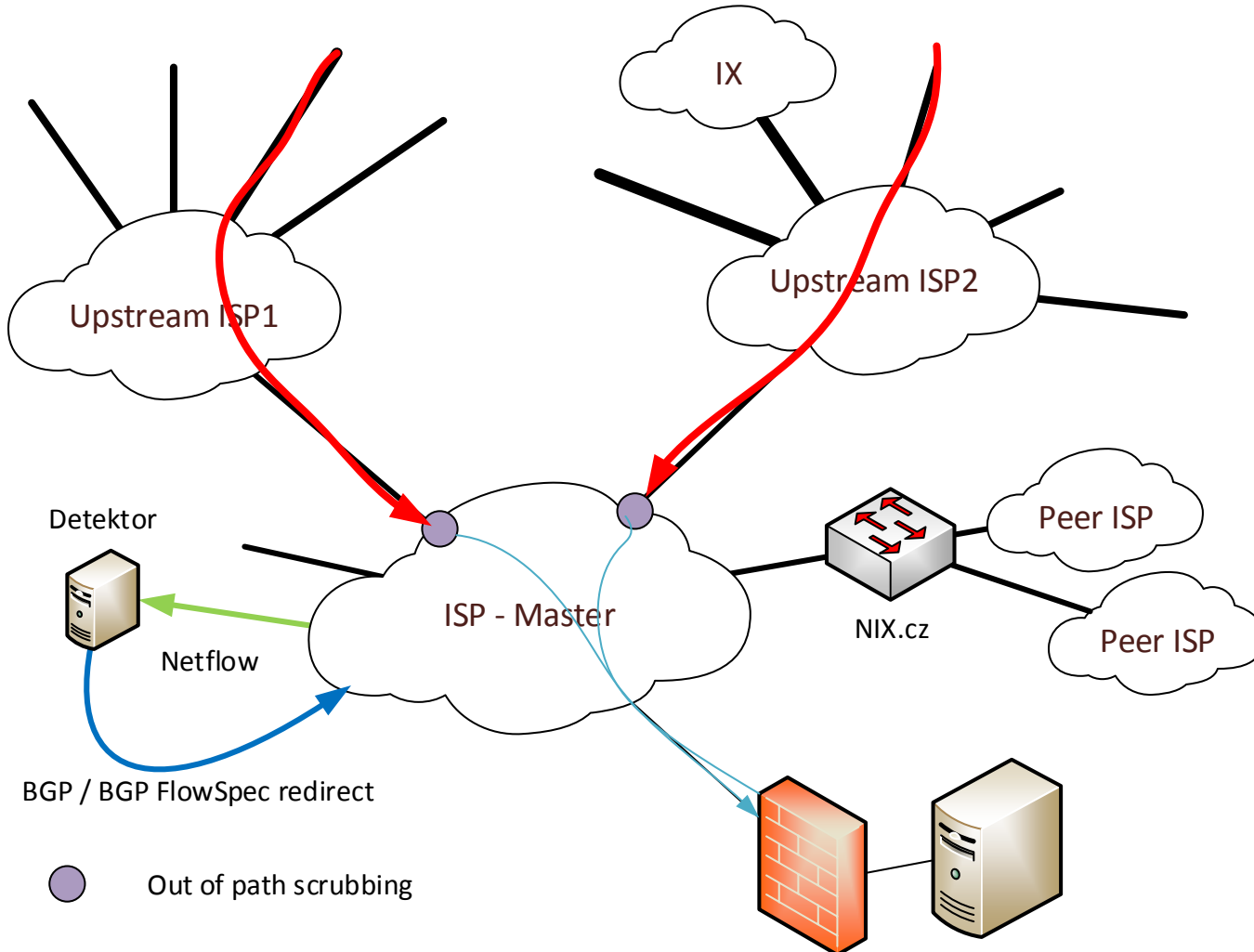
Scrubbing – Out of path



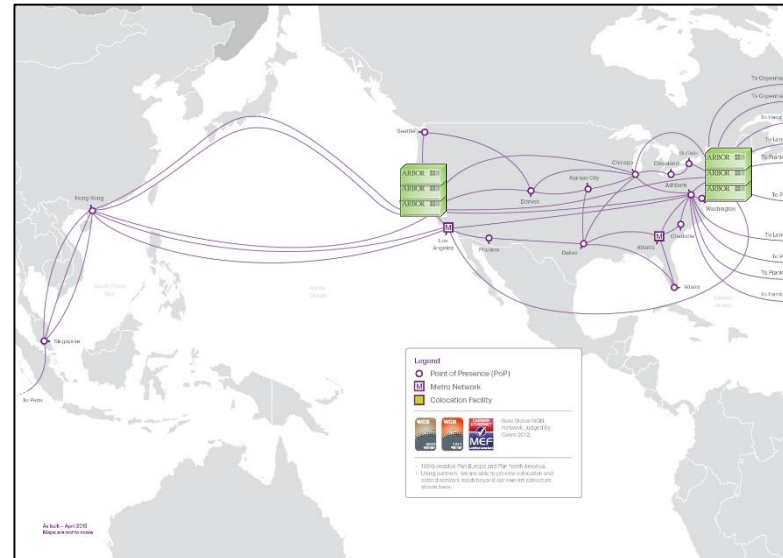
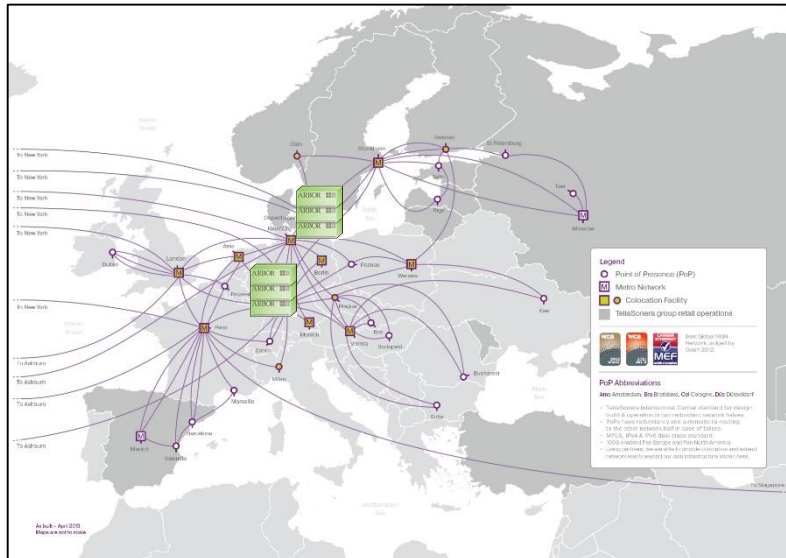
Scrubbing – Out of path



Scrubbing – Out of path



Scrubbing – Out of path



Scrubbing – Inline

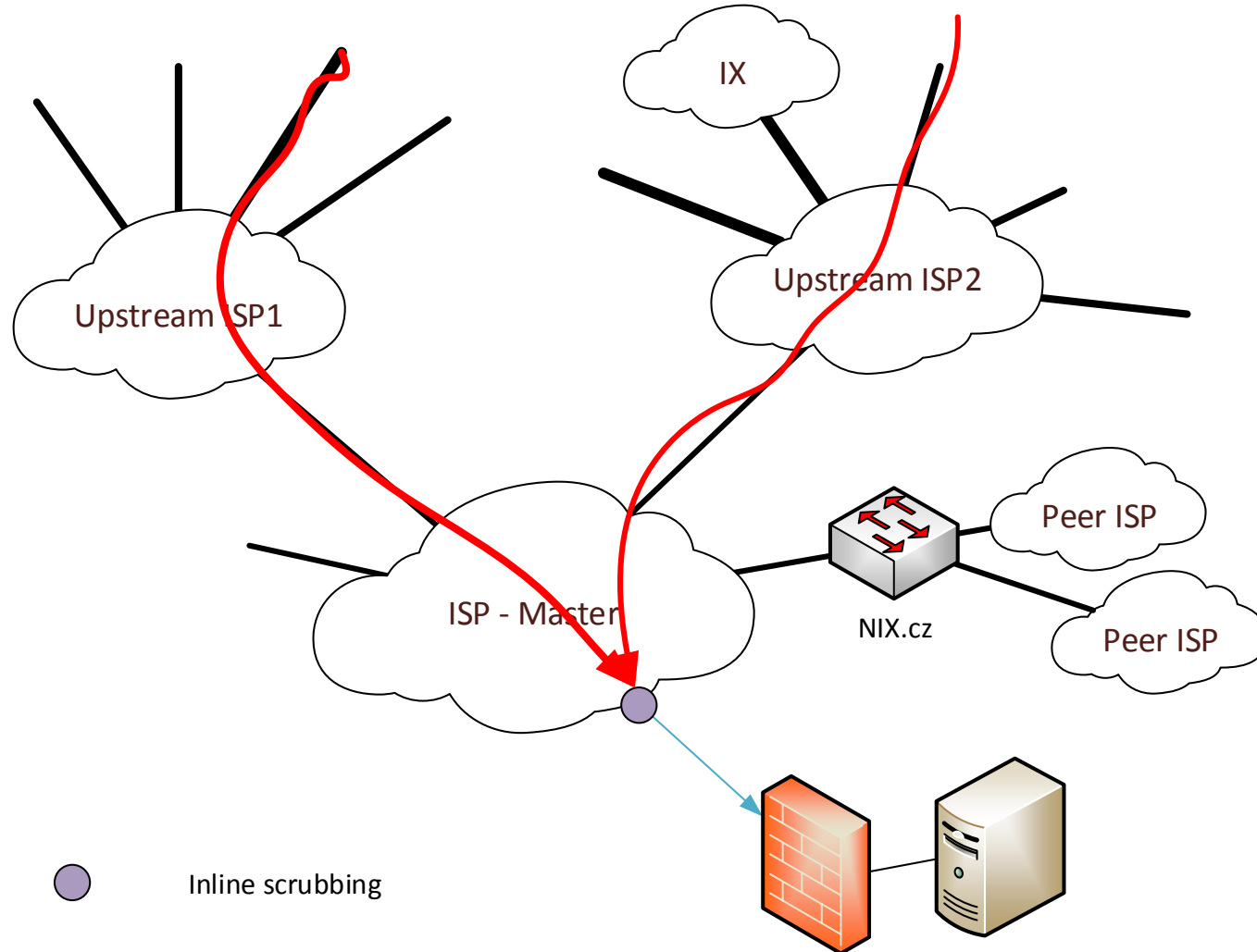
Rychlá reakce

Funkce, které nelze u out of path implementovat

Nevýhoda – data musejí zařízením procházet

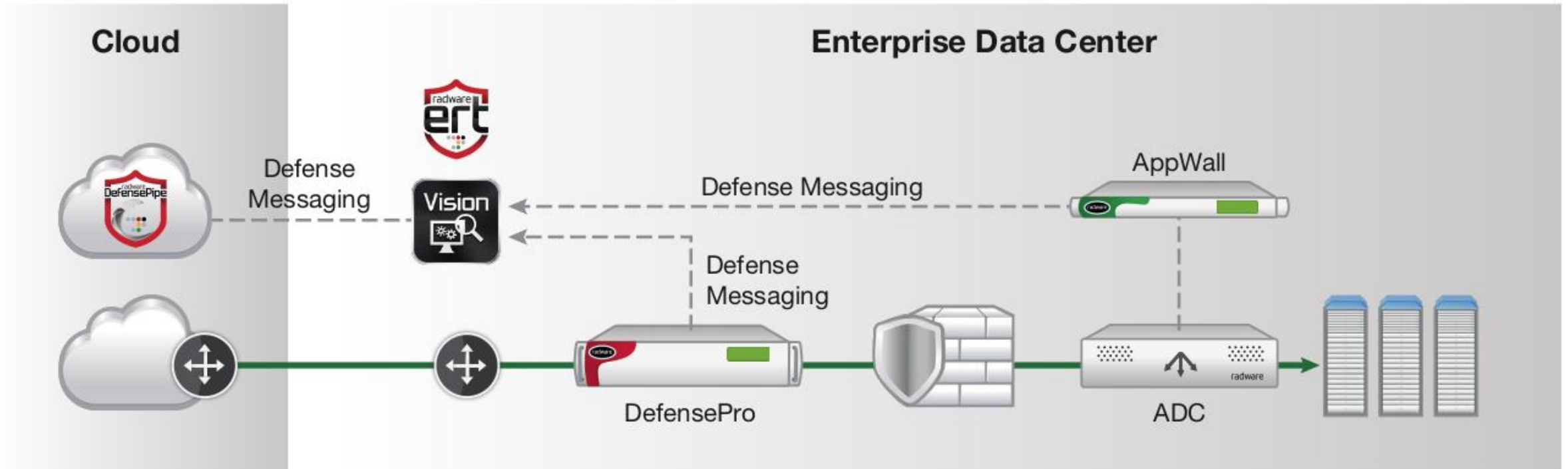


Scrubbing - Inline



Scrubbing - Hybrid

Kombinace scrubbingu



Dostupné v síti MAI

ACL – na vyžádání NOC

BGP RTBL / RTBL v upstreamu / částečné RTBL – auto

Inline scrubbing – Radware DefensePro

Cloud scrubbing – DefensePipe, Telia DDoS Protection (Arbor)

Radware DefensePro

Platforma x420, do 40Gbps /25Mpps

2ks umístění Brno, inline nasazení

Ochrana L3 / L7, integrovaná IPS

Behaviorální analýza BDoS



Radware DefensePro - Moduly

Anomally

BDoS

DoS Shield / Signature Protection

SYN Protection

DNS Protection

Server Cracking

Anti-Scanning

Connection Limit

HTTP Page Flood Protection

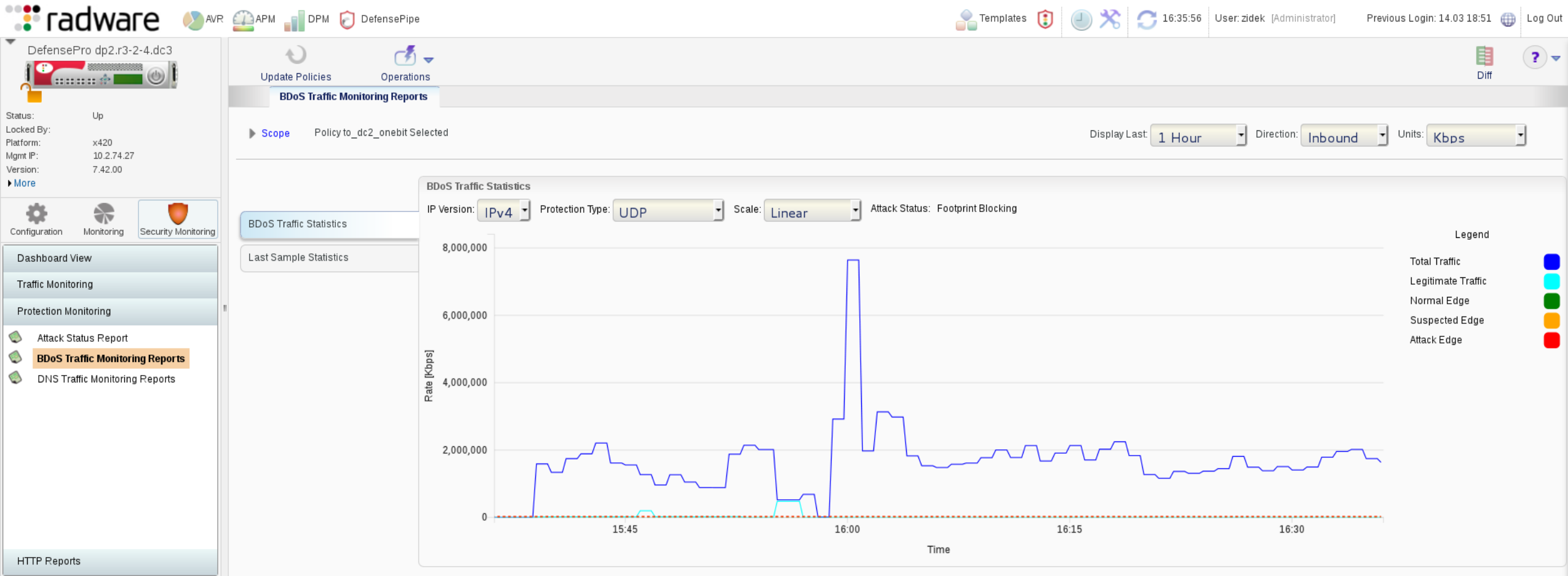
Out of State

PPS Limit

Black White Lists

ACL

Příklad filtrace reálného útoku



Alerts Table Note: The filter on the alert table can be set in its maximized view.

Ack	Severity	Time and Date	Device Name	Device IP	Module	Product Name	User Name	Message
false	Warning	16.03.2016 16:35:43	dp2.r3-2-4.dc3	10.2.74.27	Security Reporting	DefensePro	APSolute_Vision	M_20000: An attack of type "Anoma
false	Minor	16.03.2016 16:35:43	dp2.r3-2-4.dc3	10.2.74.27	Security Reporting	DefensePro	APSolute_Vision	M_20000: An attack of type "HTTP F
false	Warning	16.03.2016 16:31:43	dp2.r3-2-4.dc3	10.2.74.27	Security Reporting	DefensePro	APSolute_Vision	M_20000: An attack of type "Anoma

Radware DefensePro – Ukázka BDoS



```
hping3 -c 100000000 --rand-source -i u1 --udp 77.93.211.244
```

```
hping3 -c 100000000 --rand-source -i u1 -S -p 80 77.93.211.244
```

Dotazy ?

MasterDC



Zdroje

Approaches for DDoS – an ISP Perspective – <https://www.youtube.com/watch?v=FtaySBwenNg>

Radware 2015-2016 Global Application & Network Security Report - https://www.radware.com/ert-report-2015/?utm_source=security_radware&utm_medium=promo&utm_campaign=2015-ERT-Report

DDoS Attacks: End-to-End Mitigation -

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=89285&tclass=popup

Leveraging BGP FlowSpec to Protect Your Infrastructure -

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=89328&tclass=popup

Arbor annual Worldwide Infrastructure Security Report (WISR) - <https://www.arbornetworks.com/insight-into-the-global-threat-landscape>

Digital attack map - <http://www.digitalattackmap.com/>

Your Bitcoins or Your Site: An Analysis of the DDoS for Bitcoins (DD4BC) DDoS Extortion Campaign -

<https://www.youtube.com/watch?v=ySwYidBv1ro>

Radware On-Premise, Cloud or Hybrid? Approaches to Stop DDoS Attacks -

<http://www.radware.com/PleaseRegister.aspx?returnUrl=6442452954>

DefensePro Security Deployment Strategy Enterprise Data Center Technical Note June 09, 2015 – není dostupné online

UDP-Based Amplification Attacks - <https://www.us-cert.gov/ncas/alerts/TA14-017A>

DDoS Tutorial - https://www.nanog.org/sites/default/files/tzvetanov_ddos.pdf

TeliaSonera DDoS Protection Product Sheet – není dostupné online

TeliaSonera Intelligent DDoS Protection Service Presentation – není dostupné online

Zdroje

Radware Attack Mitigation Solution Technology Overview -

<http://www.radware.com/assets/0/314/6442477977/9901697b-2f2b-4323-a040-3ca4c6d4fed9.pdf>