
Správné místo
pro vaše data
master
data in motion
NAŠE CENTRA V PRAZE I V BRNĚ

DDoS útoky
a jak se jim bránit

LinuxDays 2016

Martin Žídek

Úvod

Cíl přednášky – „Seznámit se s dostupnými typy DDoS útoků a ochranami“

Jak je definován DDoS

- Distributed
- Denial of Service

Neexistuje univerzální ochrana

Agenda

Zdroje, cíle a důvody útoků ?

Typy útoků

Typy ochran a jejich nasazení

Cíle útoků

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.

The Hacker News™
Security in a serious way

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

Friday, January 08, 2016 Swati Khandelwal

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

master
data in motion

The Hacker News™
Security in a serious way

World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

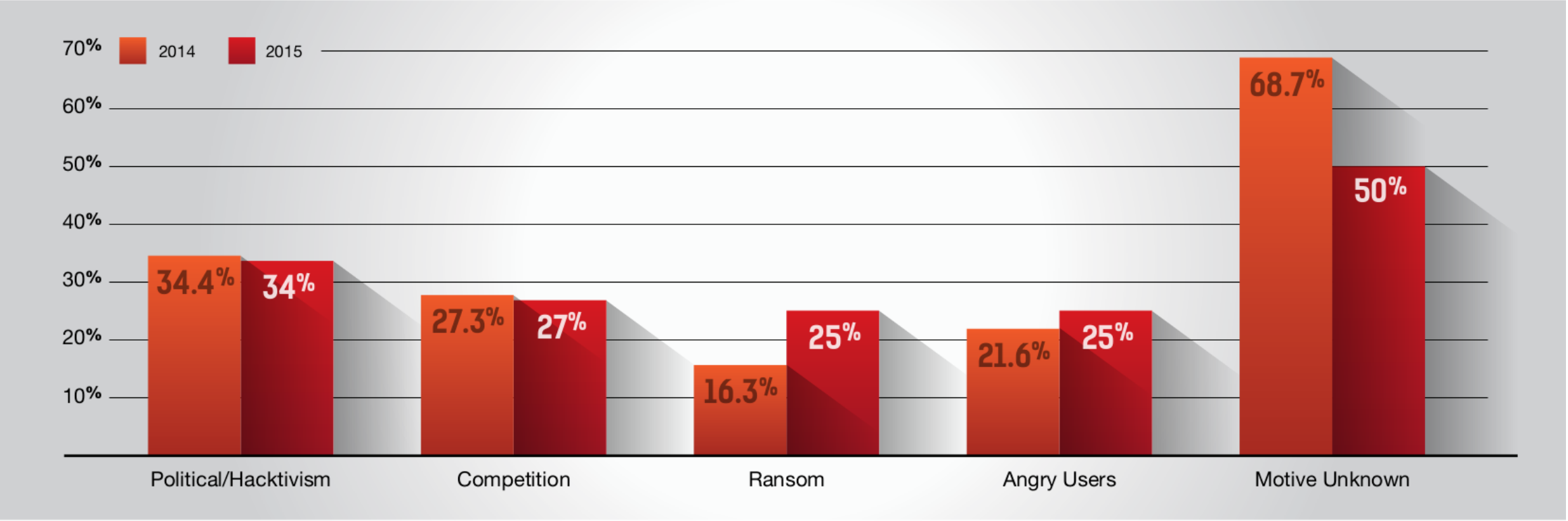
Tuesday, September 27, 2016 Swati Khandelwal

Do you know — Your Smart Devices may have inadvertently participated in a record-breaking largest cyber attack that Internet has just witnessed.

If you own a smart device like Internet-connected televisions, cars, refrigerators or thermostats, you might already be part of a botnet of millions of infected devices that was used to launch the biggest DDoS attack known to date, with peaks of **over 1 Tbps** of traffic.

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“, vDOS

IoT (“Botnets of Things”)

Časem budou využívány určitě i vyhackované mobily

Typy útoků

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

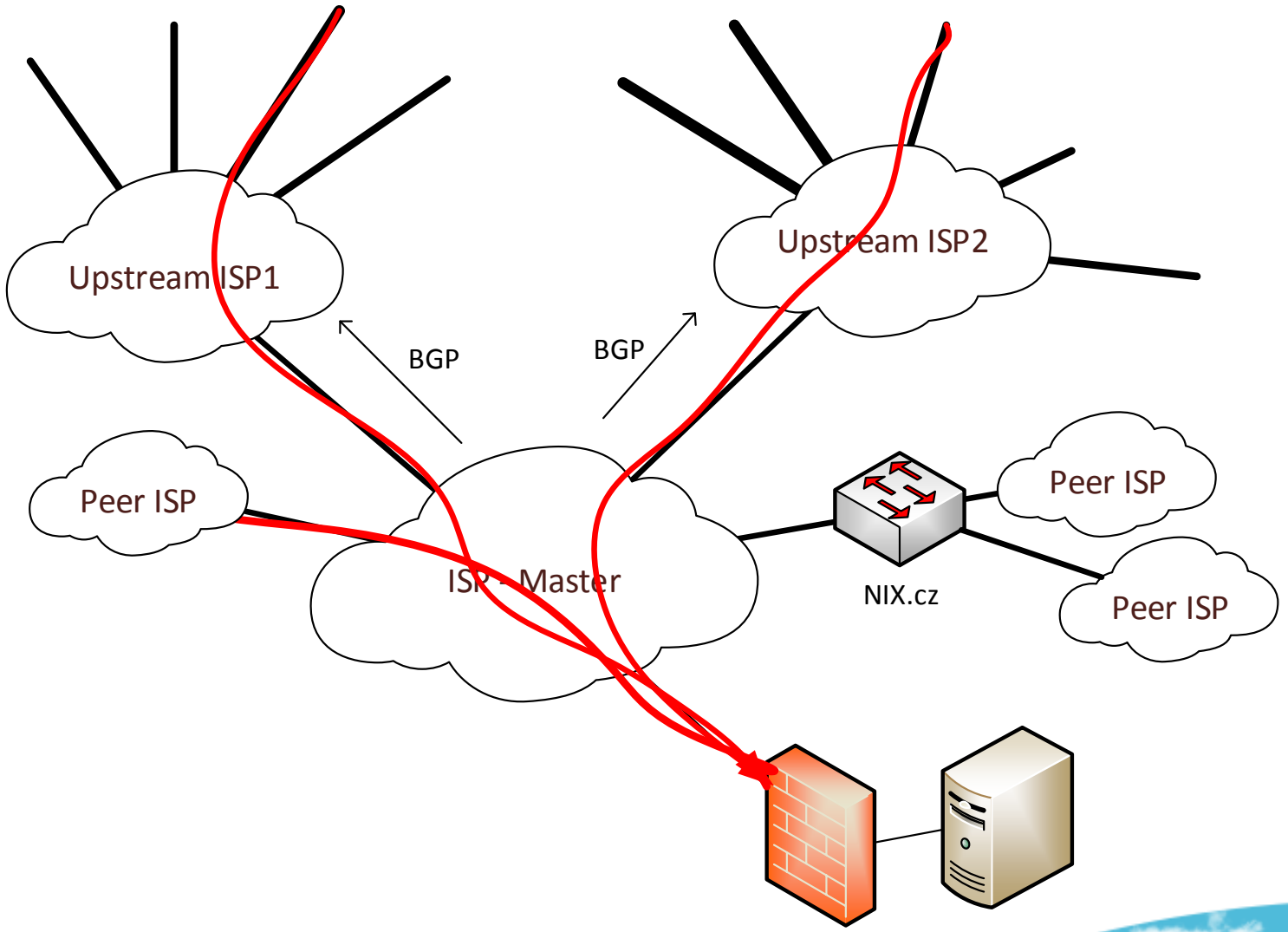
Stateless Protocols Attacks – UDP, ICMP Flood – spoofed source

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



UDP Amplification Attacks

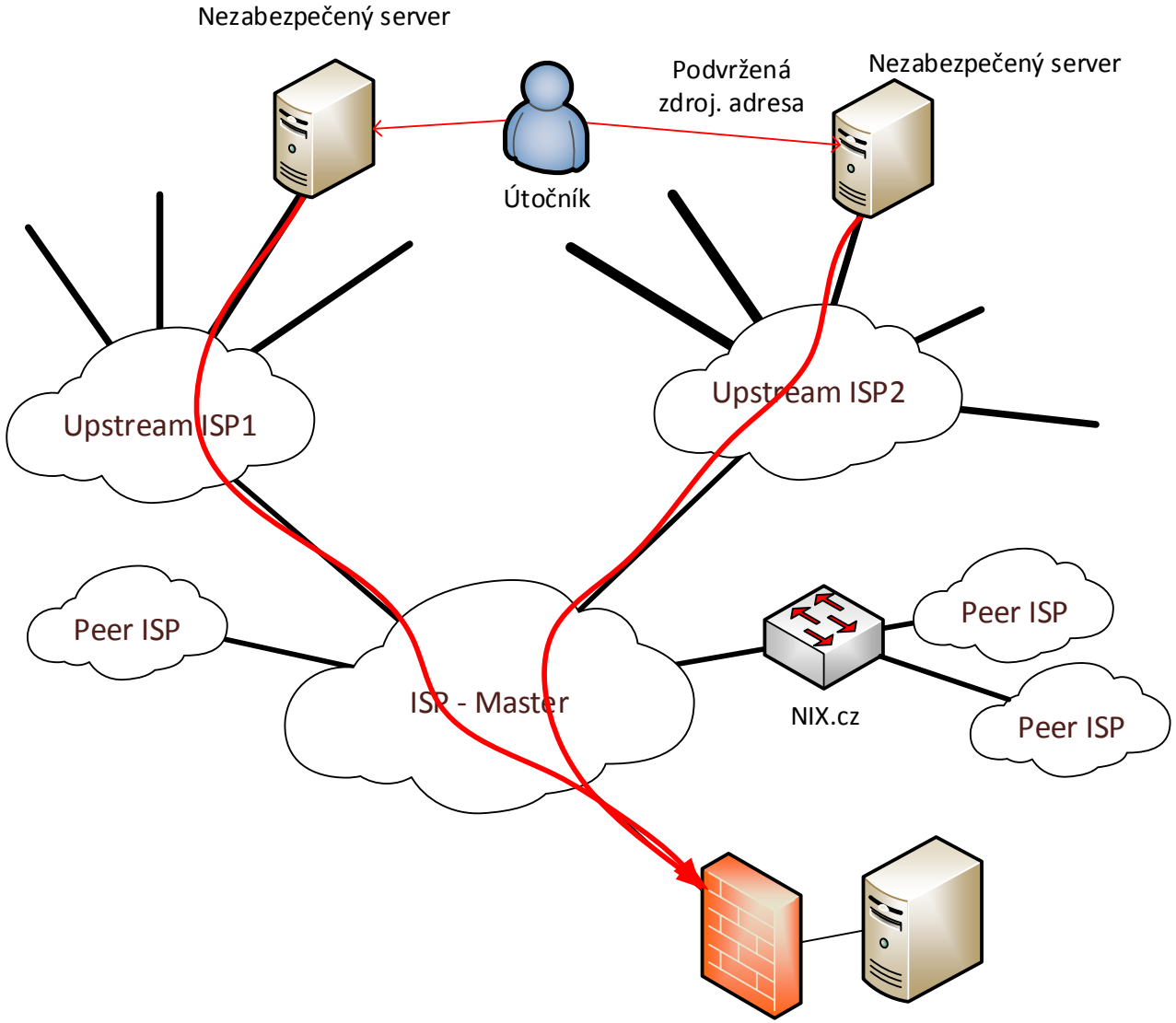
Spoofed source - UDP (DNS, NTP, CharGen, SNMP,..)

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 zdrojů zesílení – 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 RTBH– Fenix, RTBH v transitu
- BGP FlowSpec

Scrubbing – podle umístění

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

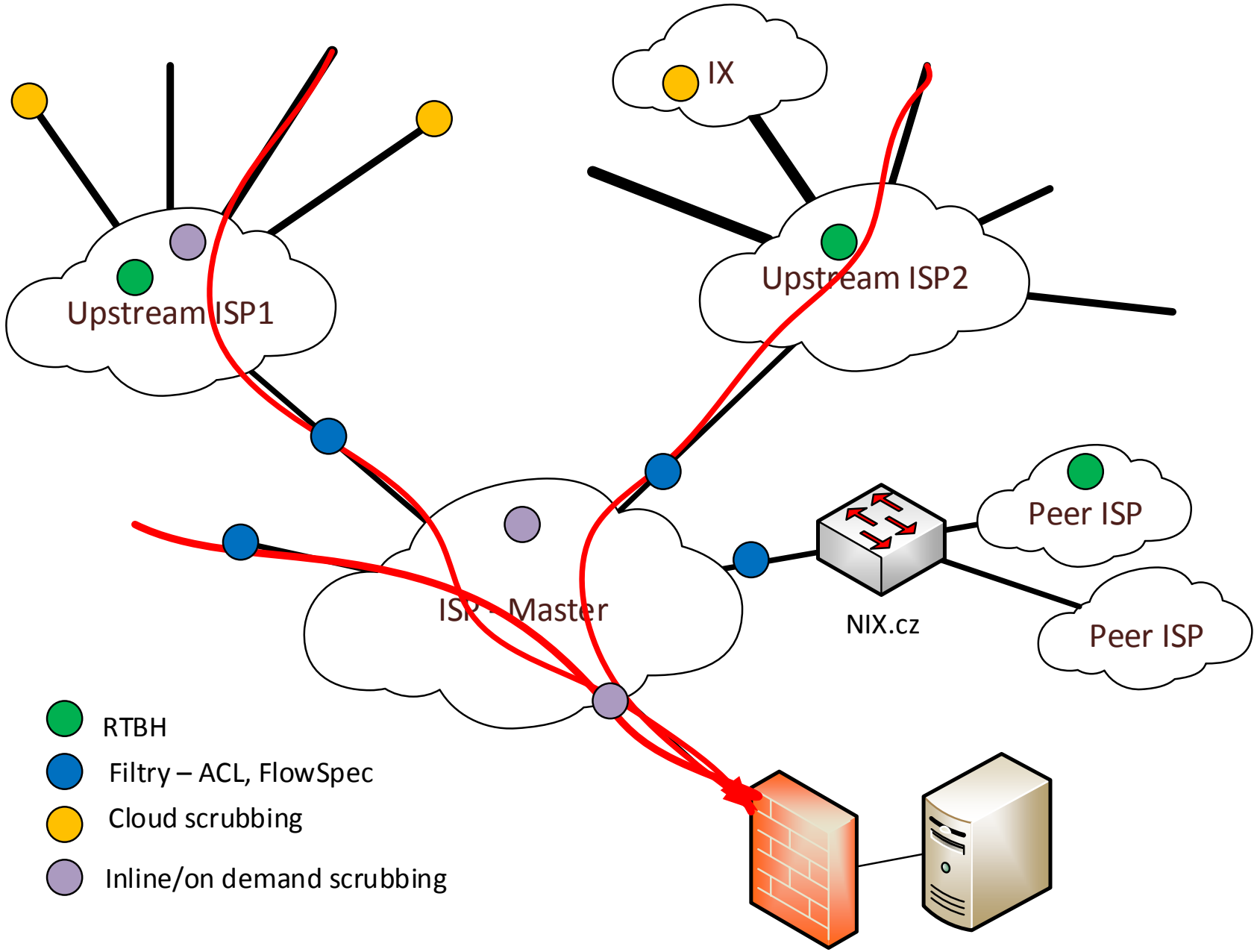
Typy ochran – Scrubbing Cloud

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

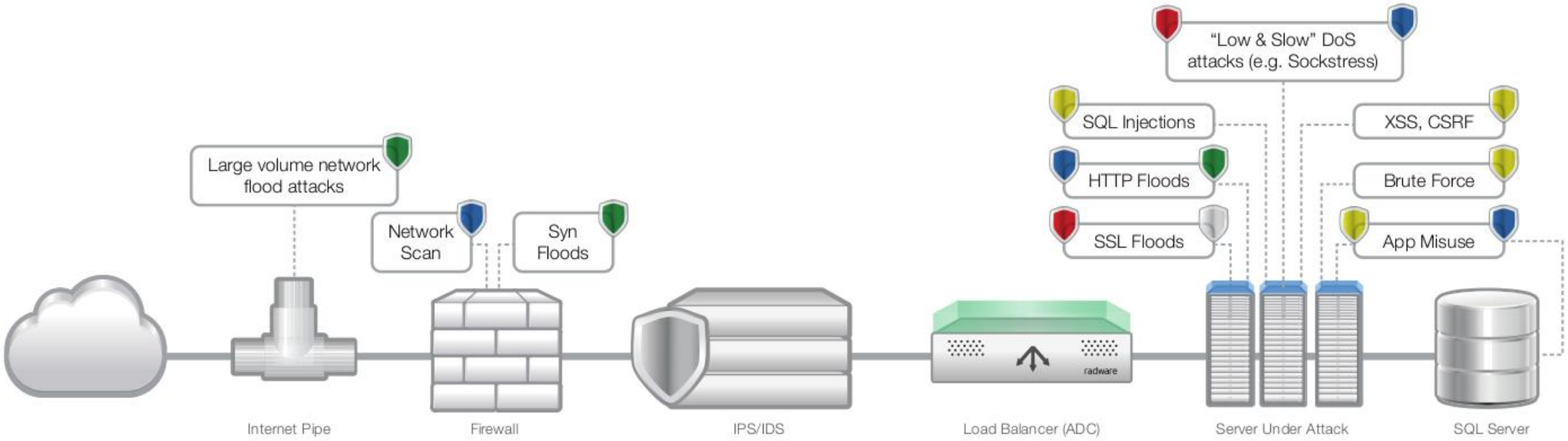
Založené na BGP - Radware DefensePipe

Typy ochran – Hybridní

Radware DefensePro + DefensePipe


IX
Upstream ISP1
Upstream ISP2
Peer ISP
NIX.cz
Peer ISP
RTBH
Filtry – ACL, FlowSpec
Cloud scrubbing
Inline/on demand scrubbing

Řetězec připojení



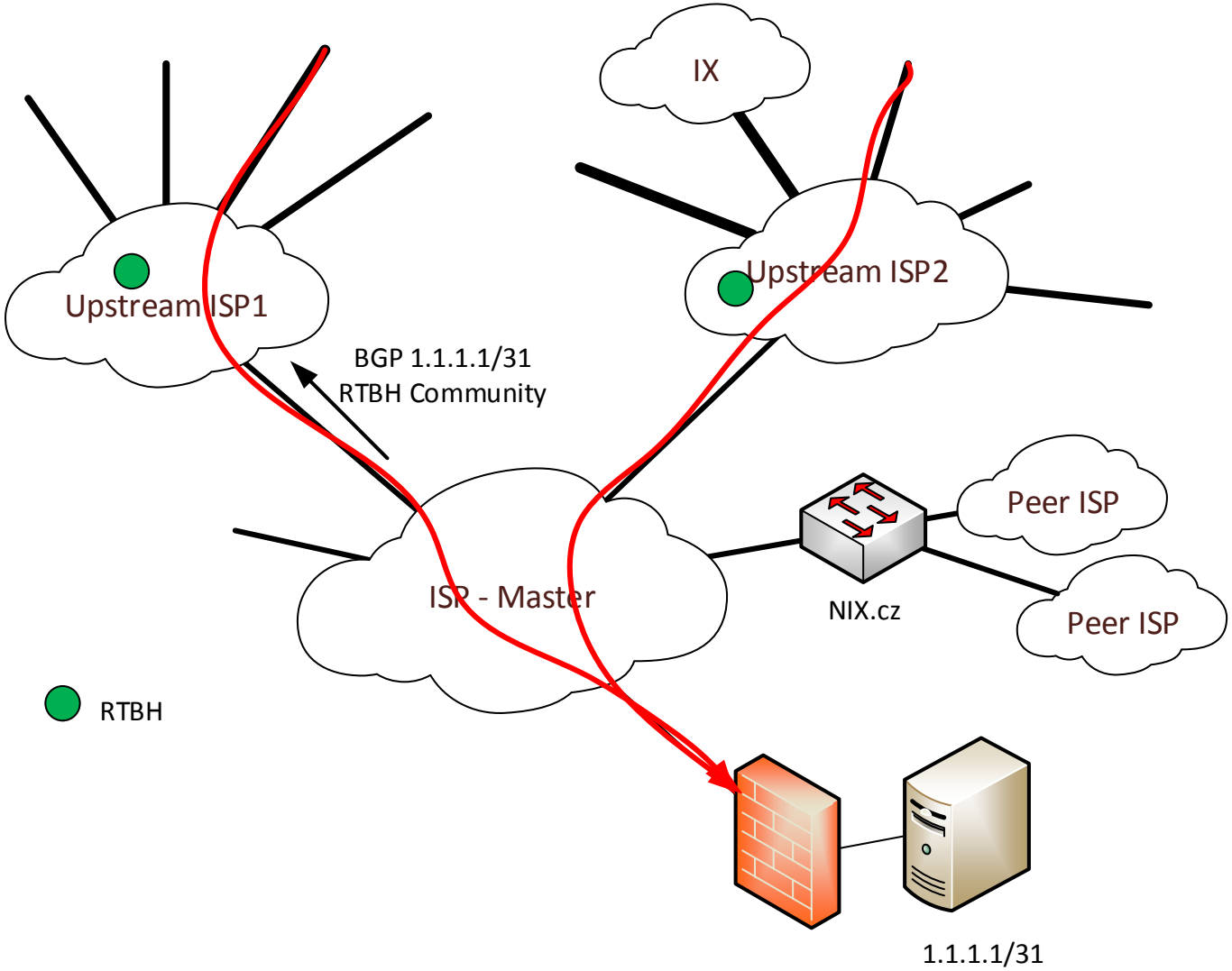
Filtrace

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

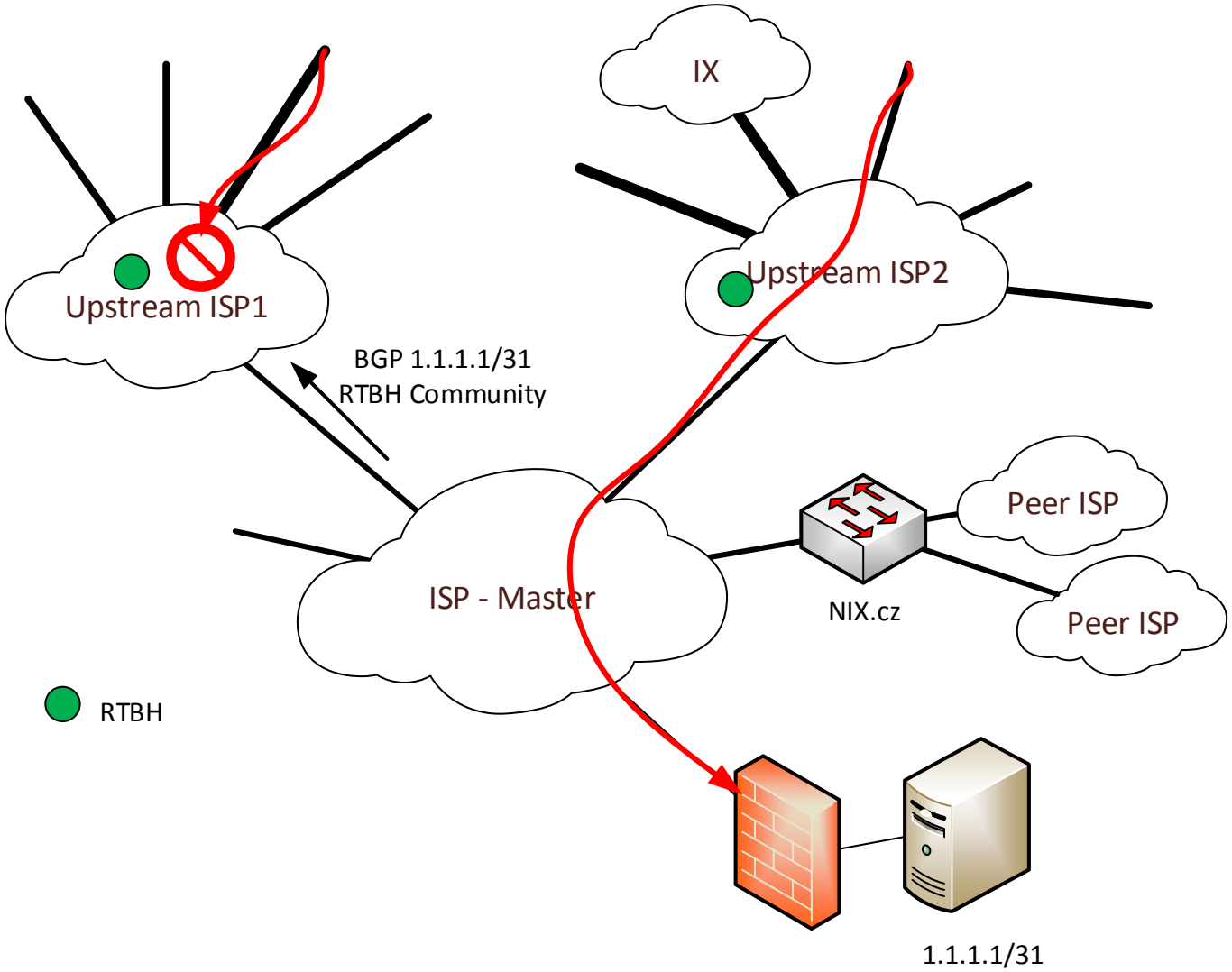
Filtrace – BGP RTBH

- 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



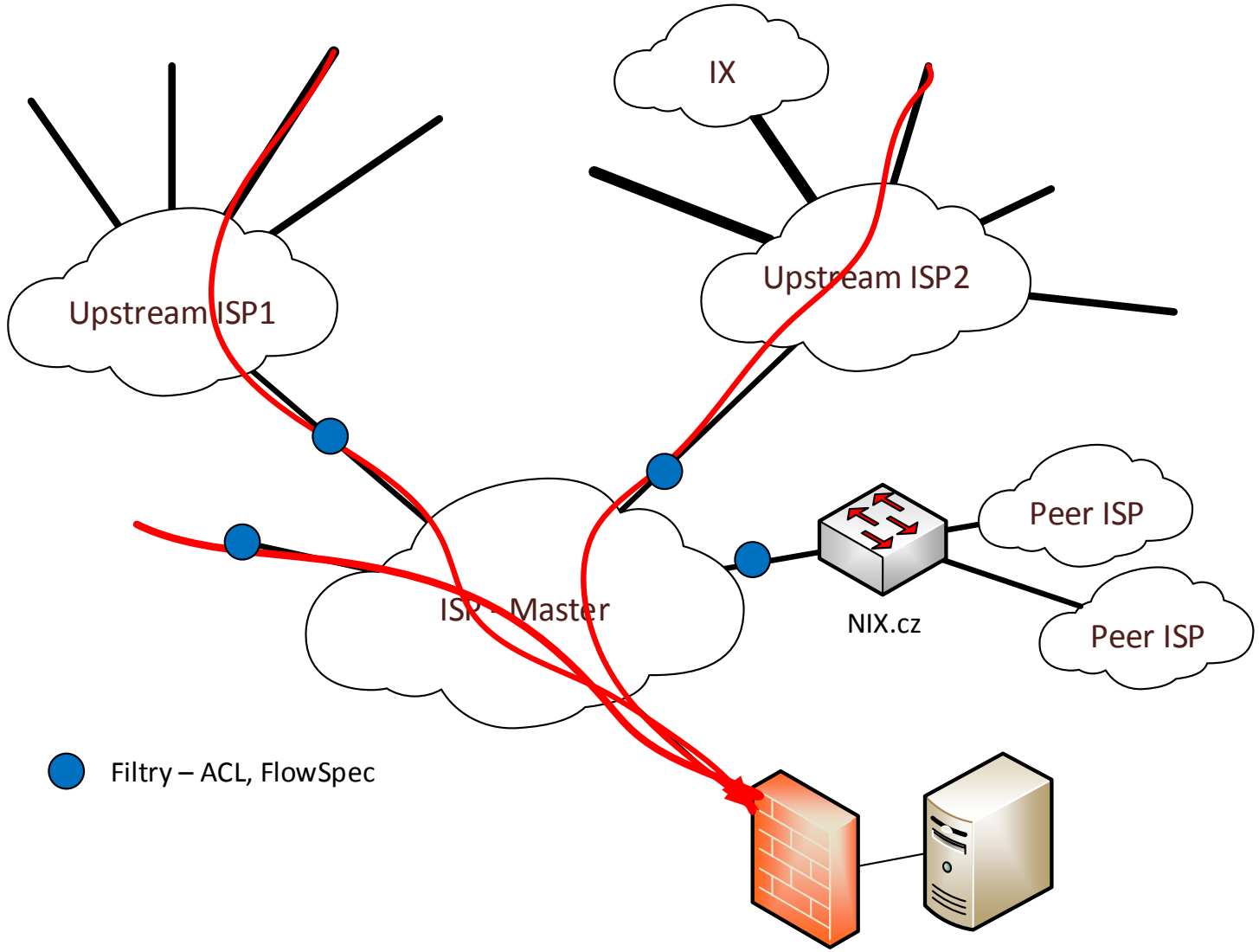
Filtrace - ACL

Nestavové

deny udp192.168.190.100 0.0.0.1 host 192.168.190.200 eq 53

Nevýhoda – ruční konfigurace přes NOC

Filtrace - ACL

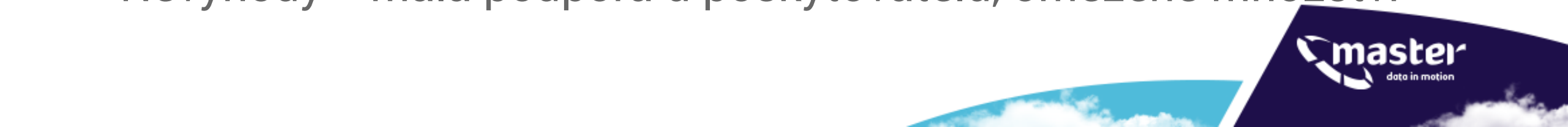


Filtrace – BGP Flowspec

Signalizace filtrů pomocí BGP / RFC5575

Akce
- Trafic 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.

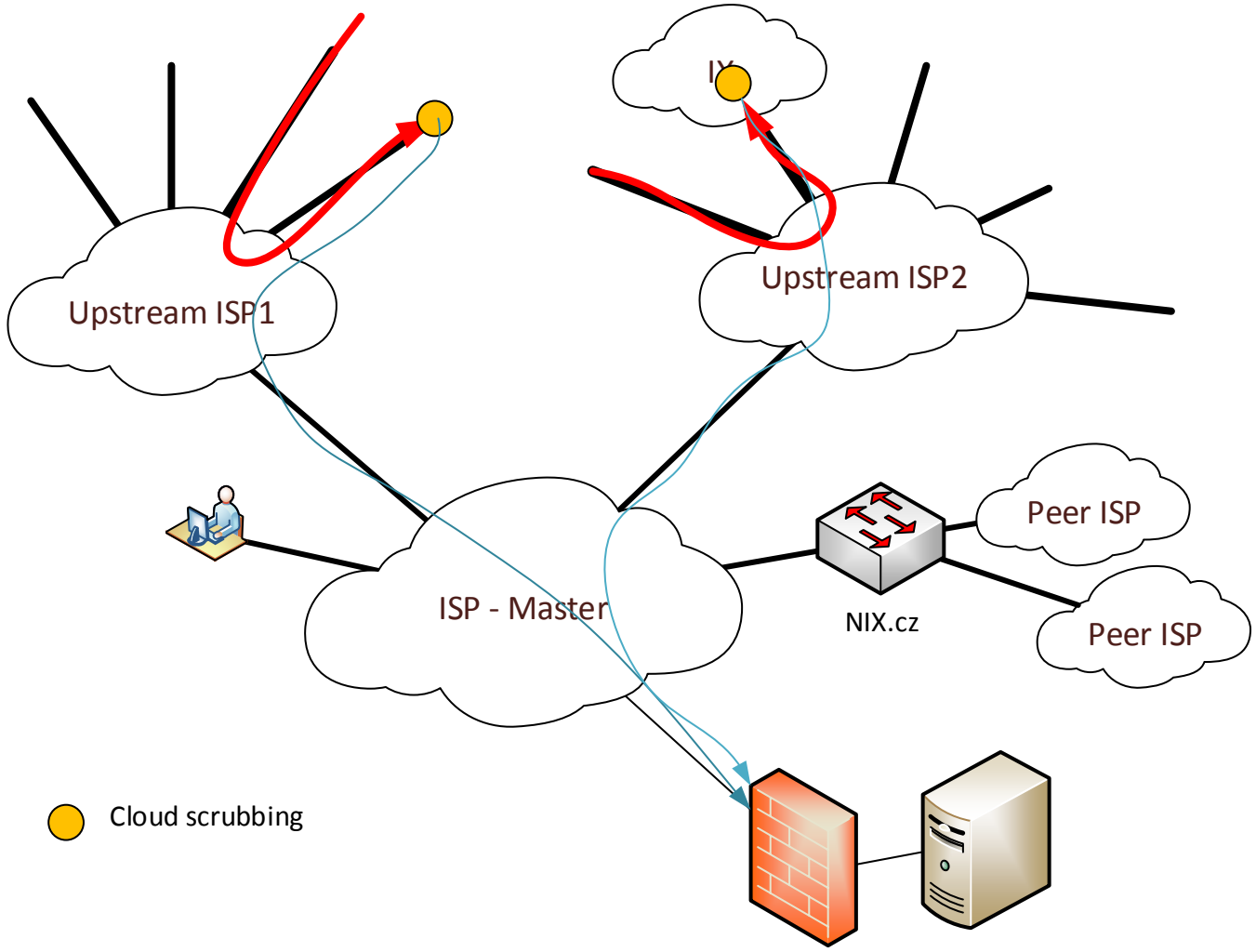
Princip CDN.

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 specifičtějšího prefixu od providera

Rychlost reakce

GRE/IPsec tunel k cílovému serveru

Scrubbing – Out of path

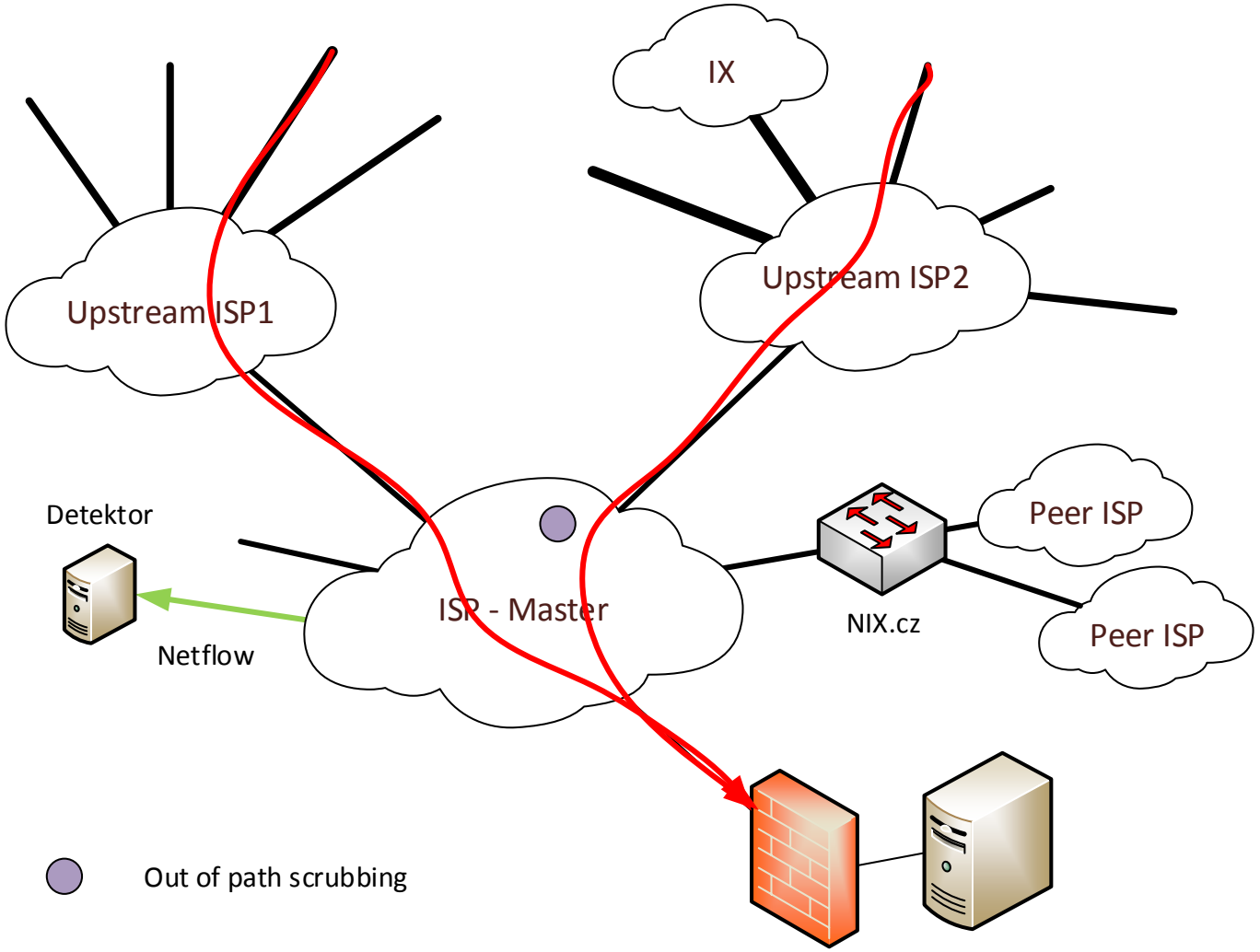
Přesměrování provozu do scrubbing centra, distribuovaný scrubbing

Pomalá reakce – nutnost zásahu NOC

Výhoda – provoz neprochází ochranou

Nevýhoda – pomalost detekce

Scrubbing – Out of path

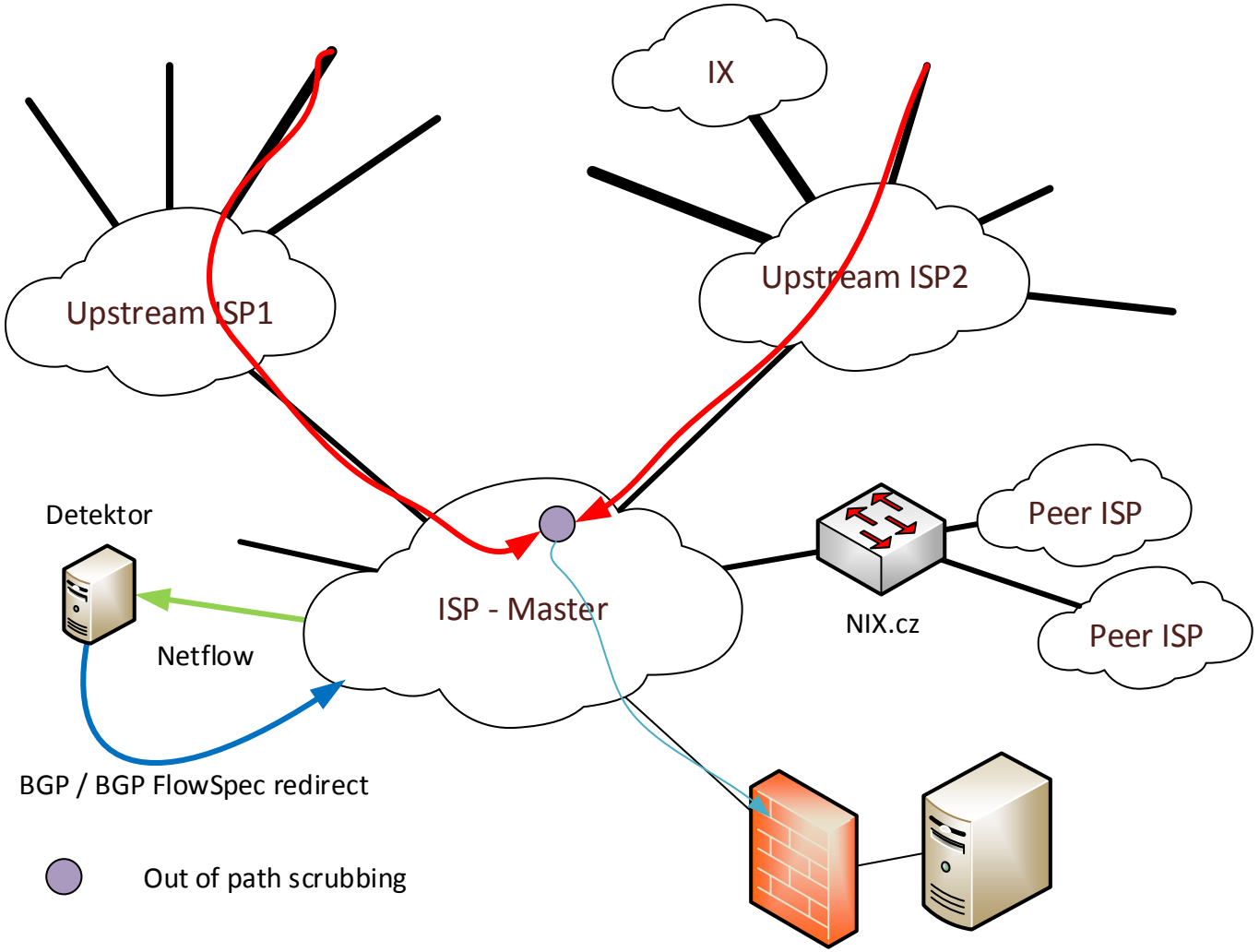


FlowMon DDoS Defender

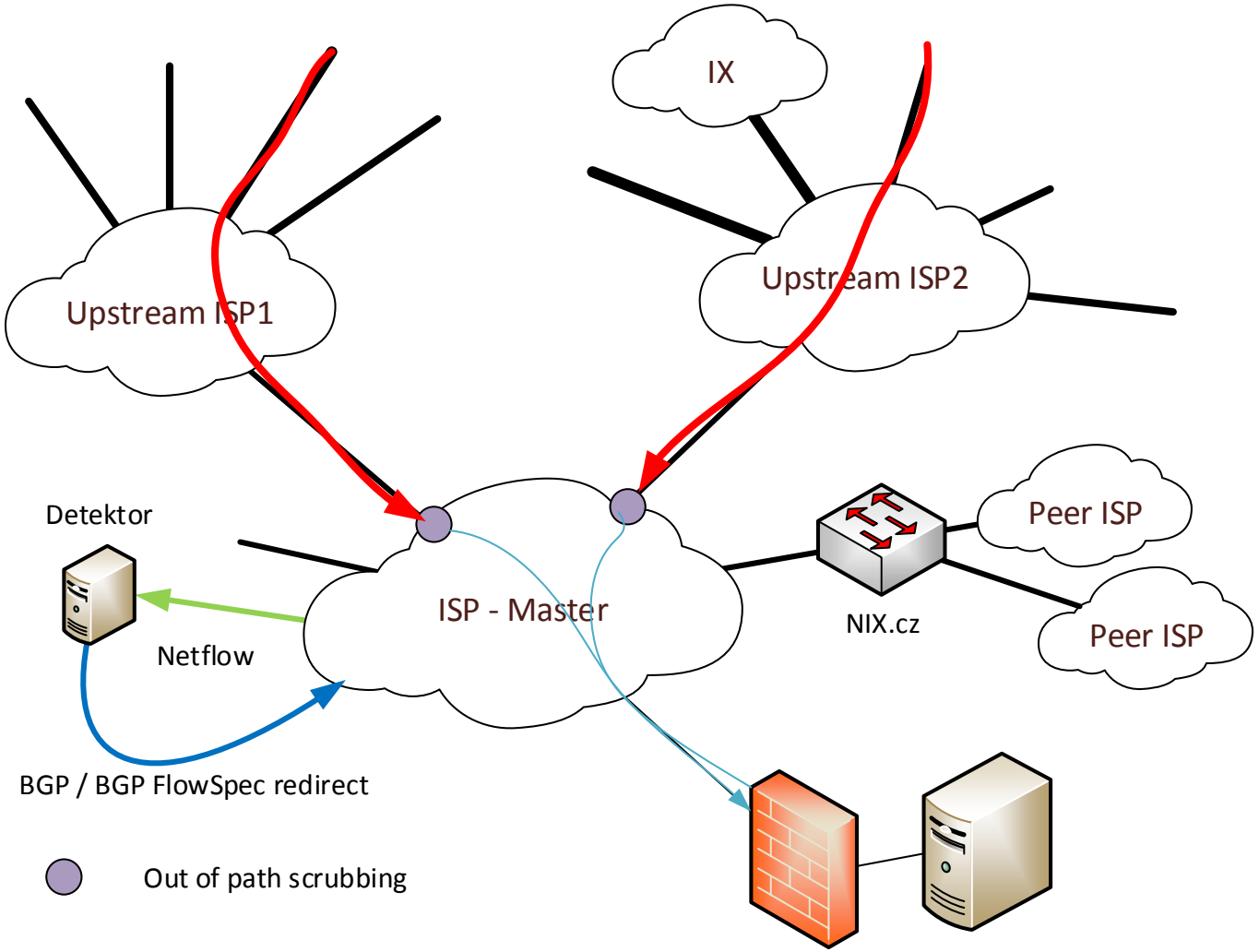
ARBOR NETWORKS

master data in motion

Scrubbing – Out of path



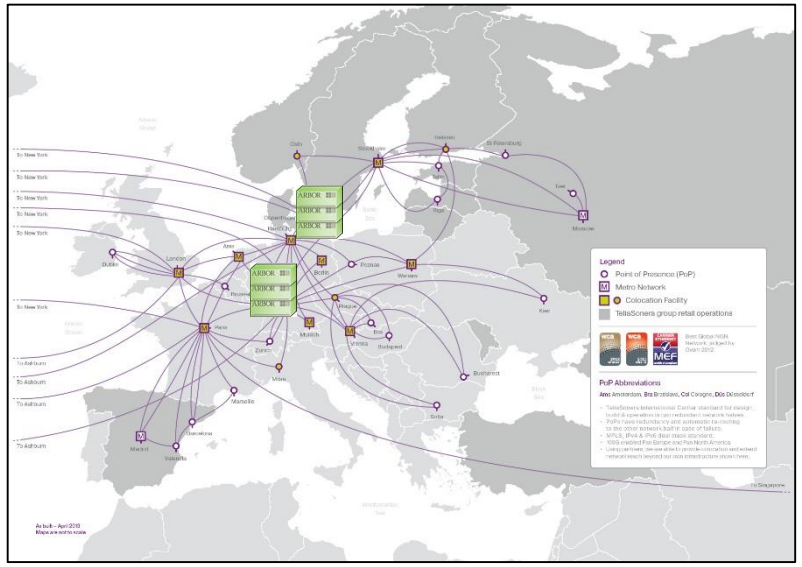
Scrubbing – Out of path

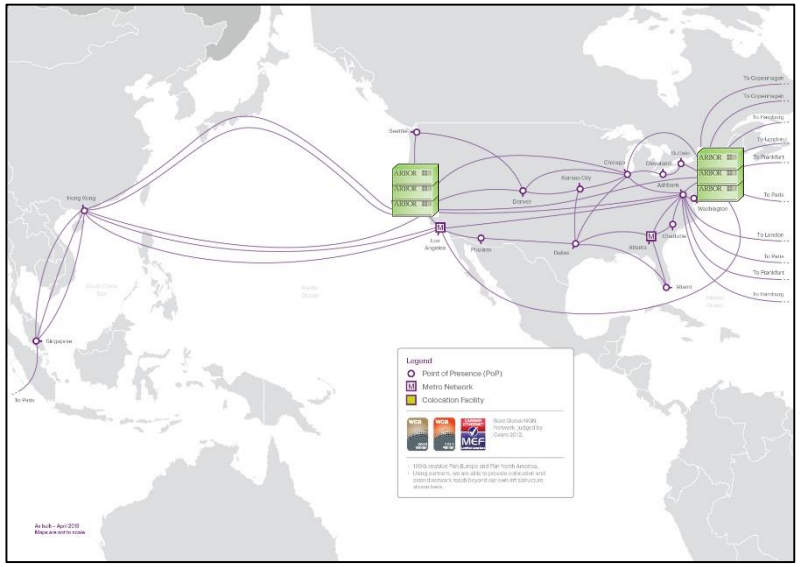


Scrubbing – Out of path

TeliaSonera

ARBOR NETWORKS





master data in motion

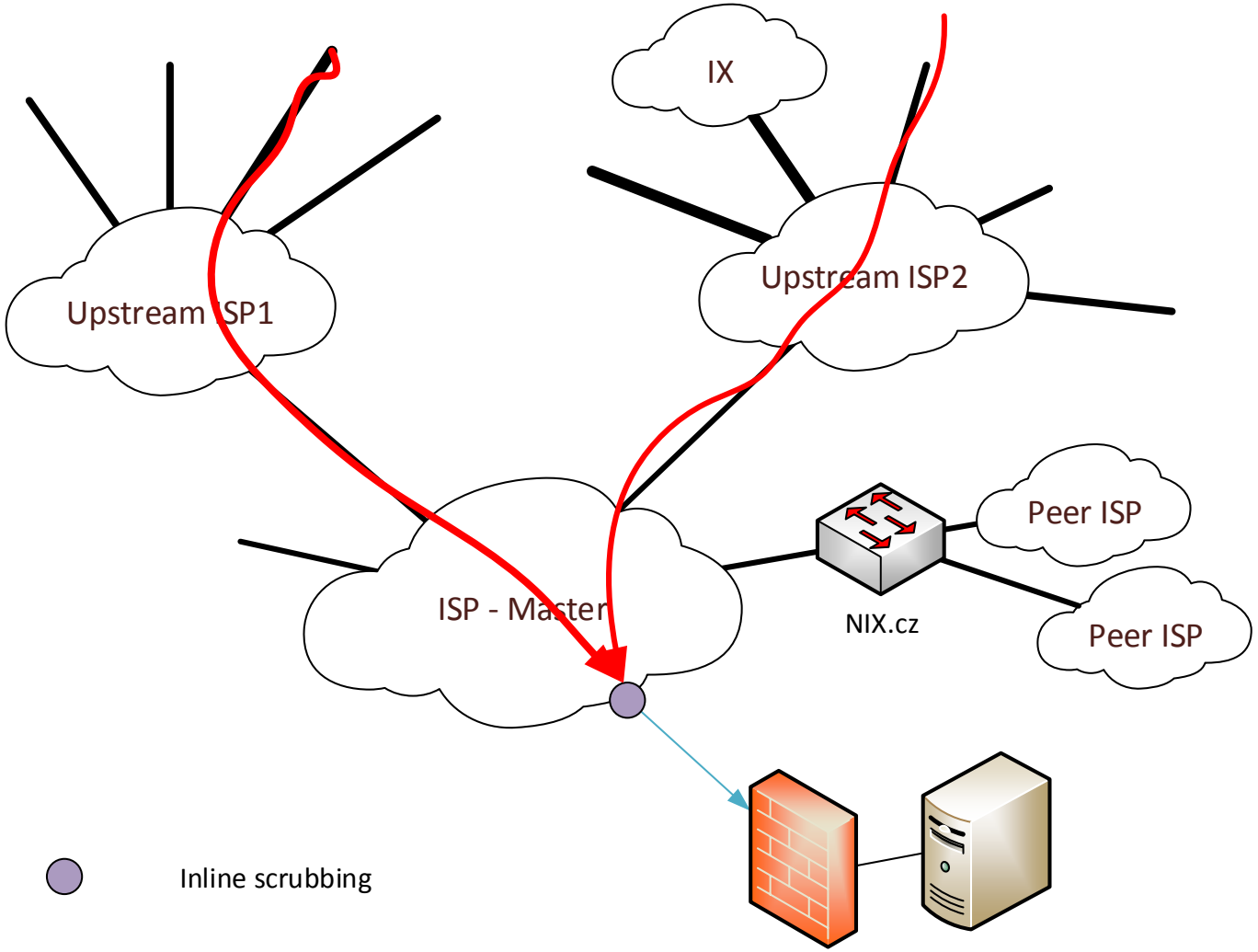
Scrubbing – Inline

Rychlá reakce

Funkce, které nelze u out of path implementovat

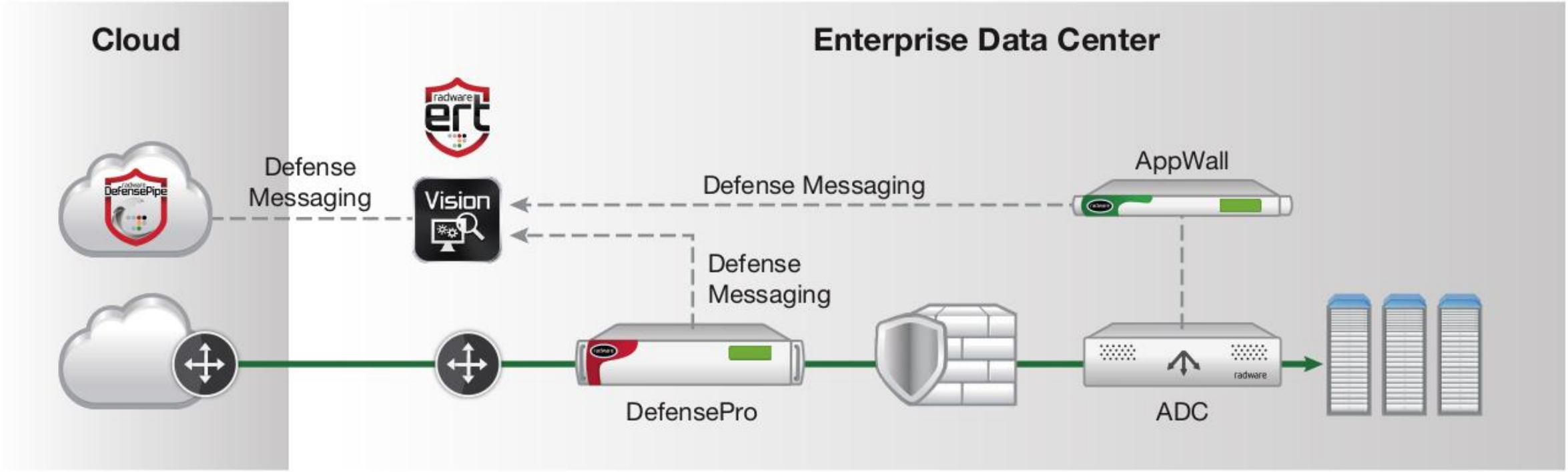
Nevýhoda – data musejí zařízením procházet

Scrubbing - Inline



Scrubbing - Hybrid

Kombinace scrubbingu



Dotazy ?

MasterDC

master
data in motion

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