How one ISP in switzerland tries to protect customers

Threat model

BGP and Peering

RPKI

DNSSEC

Adblocking/Malware blocking (not enforced on users)

tunneling

Abuse handling

$spam (IXP)

Threat model

Special legal situation, not just a private entity

no discussion: compliant with local govt, no lies about beeing exempt (looking at you, $mailprovider)

Can (never 100% tho) protect against hijacking (crypto wallet website scenario etc),

- BGP, DNS,

Malware protection (sinkholes) – if they want

Ad filtering (looking at you, 20minutes)

Own customers (Incompetence, or accidential – or malicious?)

Tradeoff

Increasing vulnerability to censorship (NL court, RIPE in NL; RPKI...)

More Network overhead

More CPU Resources => energy consumption

More complexity => needs more skilled staff

Routing

Measure 1: Peering, Peering, Peering...

- Latency
- Spying
- Censoring
- Capacity
- Costs

BGP Path Selection

- Weigh
- Local pref (set because of source, or RPKI)
- network or aggregate
- pathlength
- origin type
- … (is commonly documented)

RPKI

Signed routes via a PKI (e.g RIPE)

VyOS as OS; FRR as Routing engine

RPKI = routinator right now

Route map checks if valid, tags 58299:91xx if valid, 58299:9199 if invalid

My default local pref = 200, no signature, with signature, +20 local pref. IXP/Downstream differ

can’t yet blackhole invalid routes => Free.fr has invalid more specifics – needs more understanding. Throwing away => DefRoute?

DNS

DNSSEC validation

Protects e.g sshfp, public key in dns etc.

Done in pihole

Resolver: 3x pihole-cluster, internally anycasted.

Authoritative Zones: Cpanel: Unclear? Webmin: automatic rollout pending with switch (tbd)

Piholes

Easy to setup script (curl | bash … I know)

passthrough with dnssec, resolv via authoritative dns as upstreams, then root

Adblocking no censoring (via Auth-DNS)

Adblocking + malware censoring (via Quad9)

All: Disabled statistics, logging, and EDS

Query - Forwarding via v6 only, whenever possible.

Tunnels

Wiretapping

Experiment from Pennuator to tap: works

Migrating to VyOS as edge-OS

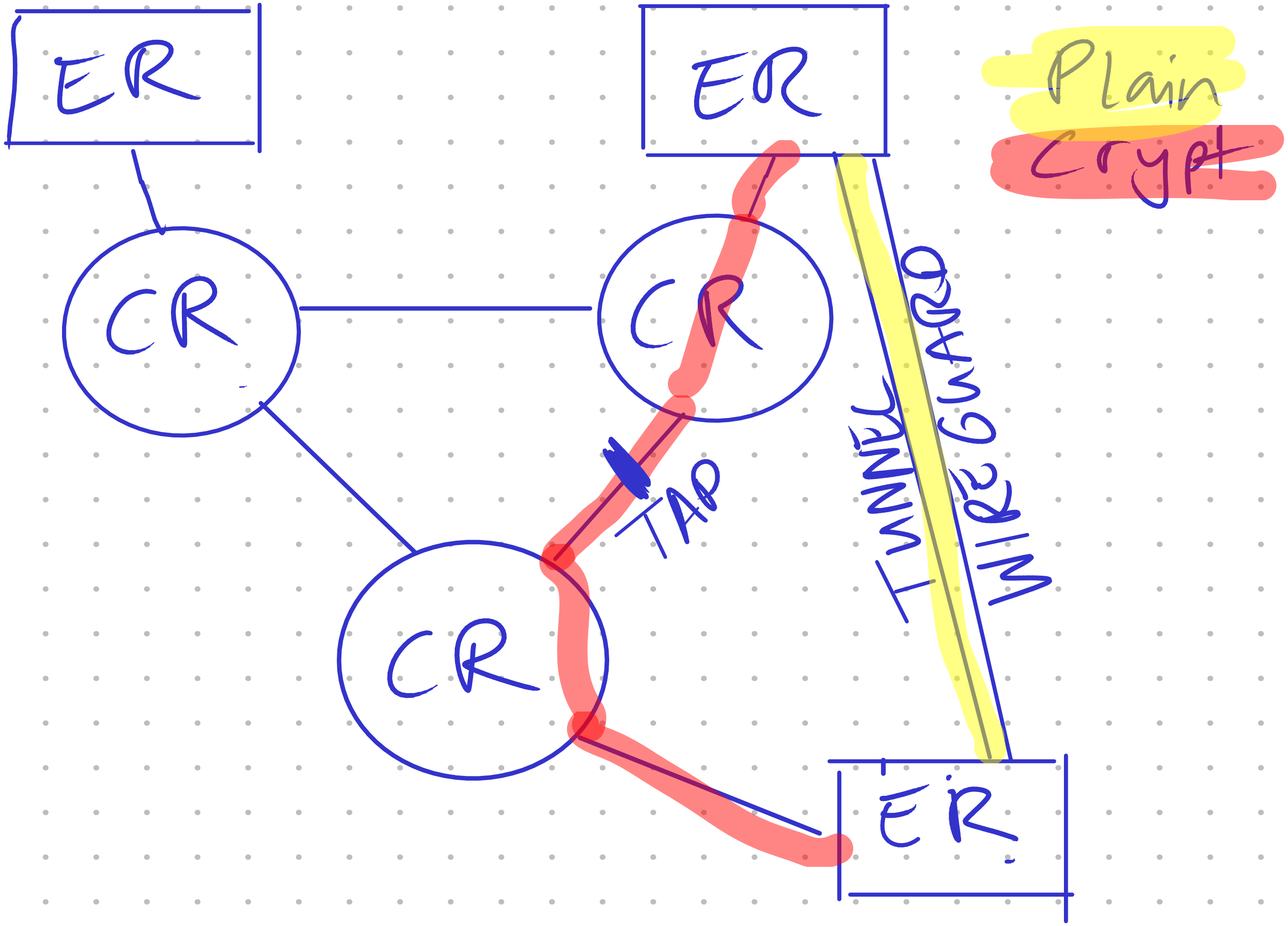
Moving default-free to VRF

Enabling Wireguard tunnels between Edge Routes

No services from core, downstream edge as tunnel endpoint

DDM monitoring and extrapolating with RRD (potentially) – not helping on pre-tapped lines

Asking for Patch details, run own OTDR; confront vendor (wrong documentation might be reason?)


ER
ER
Plain
Crypt
CR
CR
TAP
TUNNEL
WIREGUARD
CR
ER

Side note: Network setup

Minimal standard for us

PPPoE-IA (Access networks)

DHCP Snooping

Multicast snooping

MUX VLAN, BGP Unnumbered CPE for business customers (IP legacy waste)

Byod: be annoying about patching

Collect MNDB; CDP etc and nag customers

Abuse + security alert handling

Abuse.io

Webfrontend to automatically parse vuln as well as abuse. No jurisdiction on DMCA → Spam.

Partial disagreement with the discussion on RIPE78

Subscribed shadowservers.org, Switch Cert(tbd)

Switch cert => hacked Server => ~1h takedown notice

FUP includes “no vulnerable services”*

(IPMI; NTP; open DNS without limits, etc)
* led to lengthy political discussions

Side note #2: CHIX

CH-IX

Funded in 2018, Swiss Association

Available in Steinhausen, Equinix

Based on Nexus 3064

Received /48 IP Space, and /24 IP Legacy

No Route-Servers for now*

No Port-Fee at the Moment.

Mission

Add new POPs (Smaller ones)

Encourage Peering

Support projects like Community-IX (Allow members to deliver full table)

Less interconnects

Potential Sites

- eShelter ZH
- Kloten (Town) via Power Company
- Layer1-Networks via FTTH
- Locations around other towns
- Germany? Austria? Baltics? Scandinavia?

ToDO

IXP Manager

Website Updates

Add Peers

Scaling & Sizing (Limits of 3064)

Your Site?

Questions to the Audience – who here

- knows what BGP is
- knows how BGP works
- runs BGP
- runs an IXP