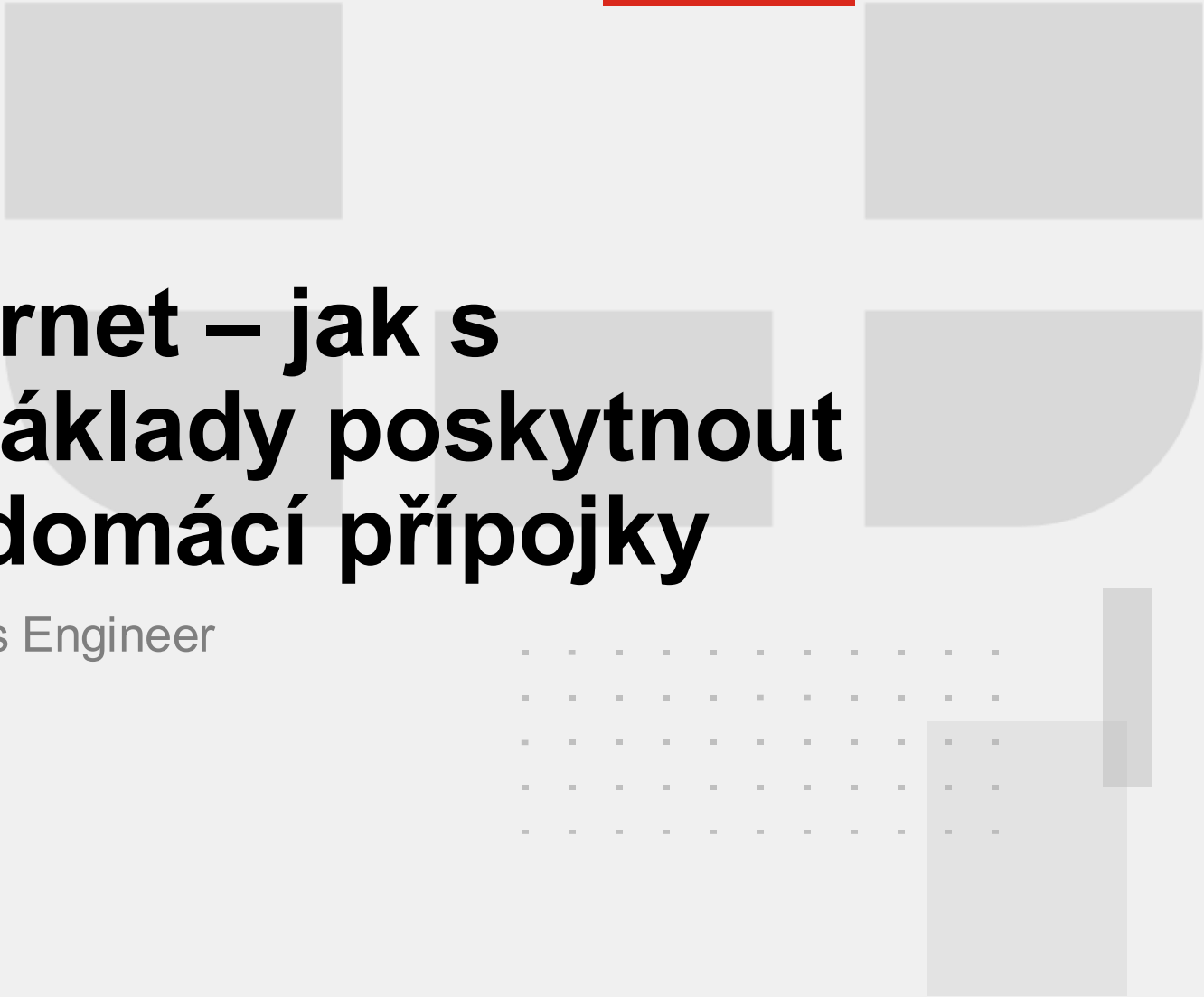


FORTINET

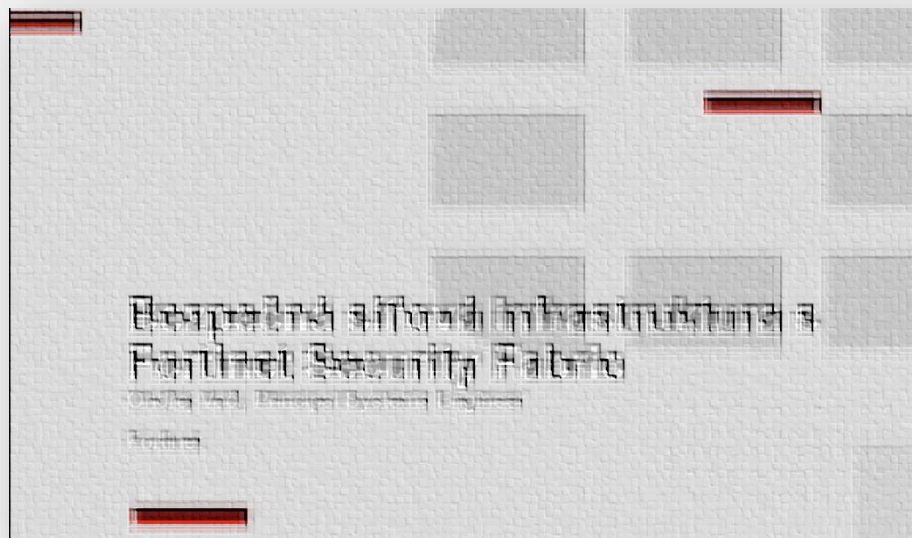
Bezpečný internet – jak s minimálními náklady poskytnout zabezpečené domácí přípojky

Ondřej Večl, Principal Systems Engineer

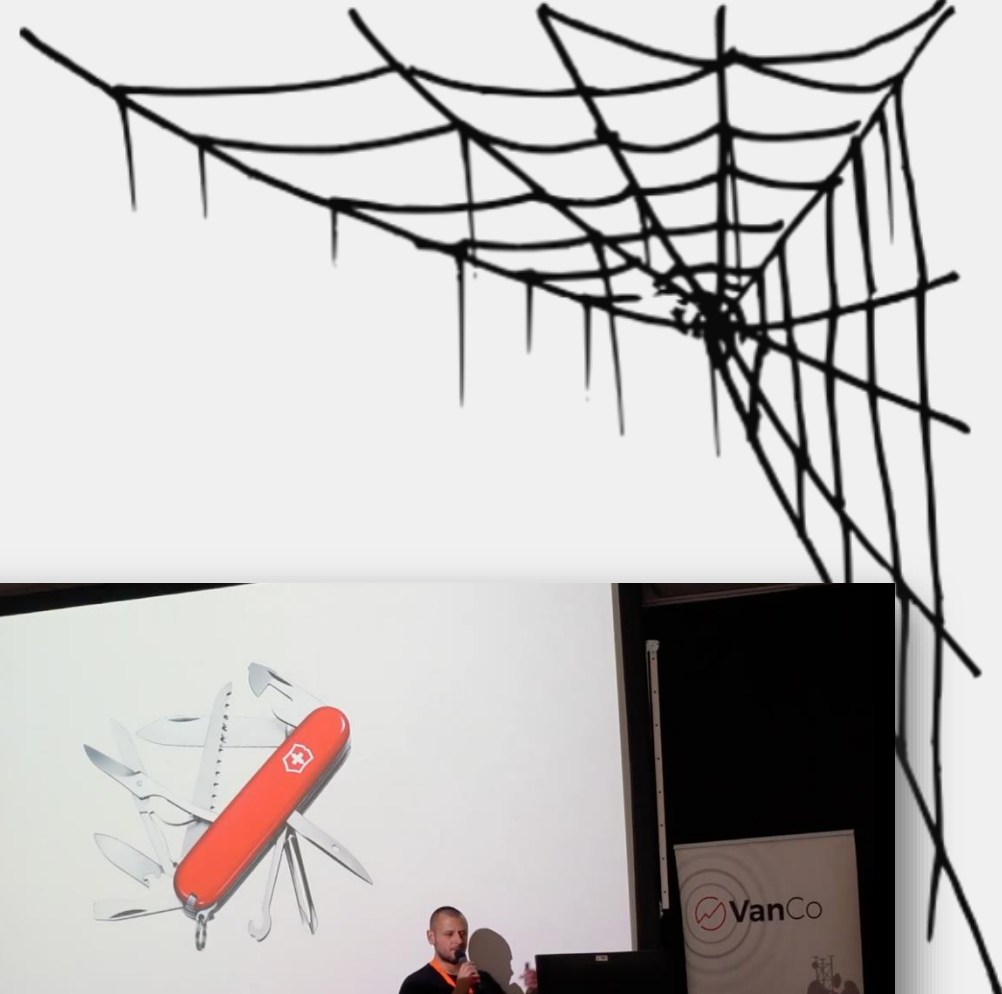
Fortinet



Cca před rokem ~~touto~~ dobou...



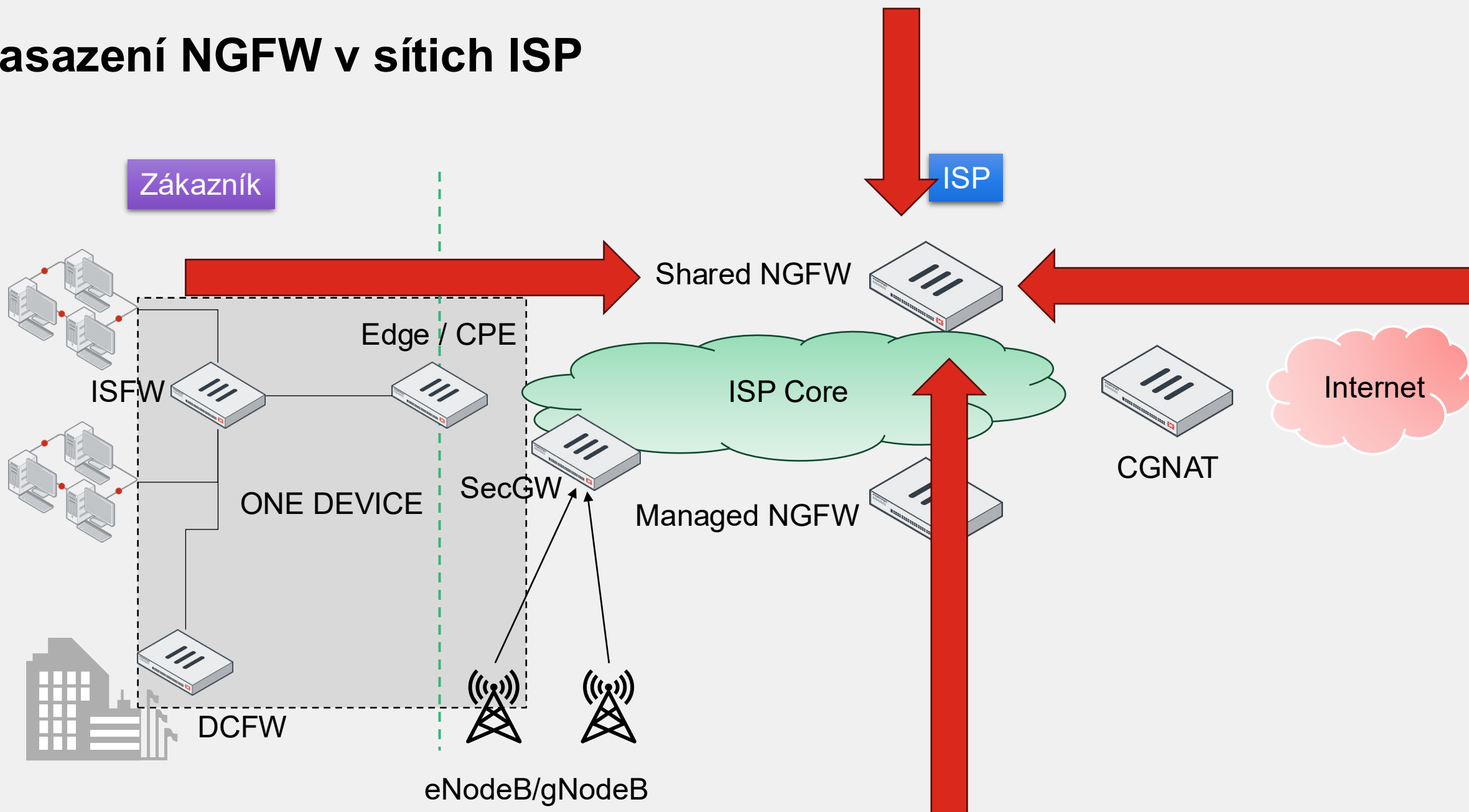
Cca před rokem 2 lety touto dobou...



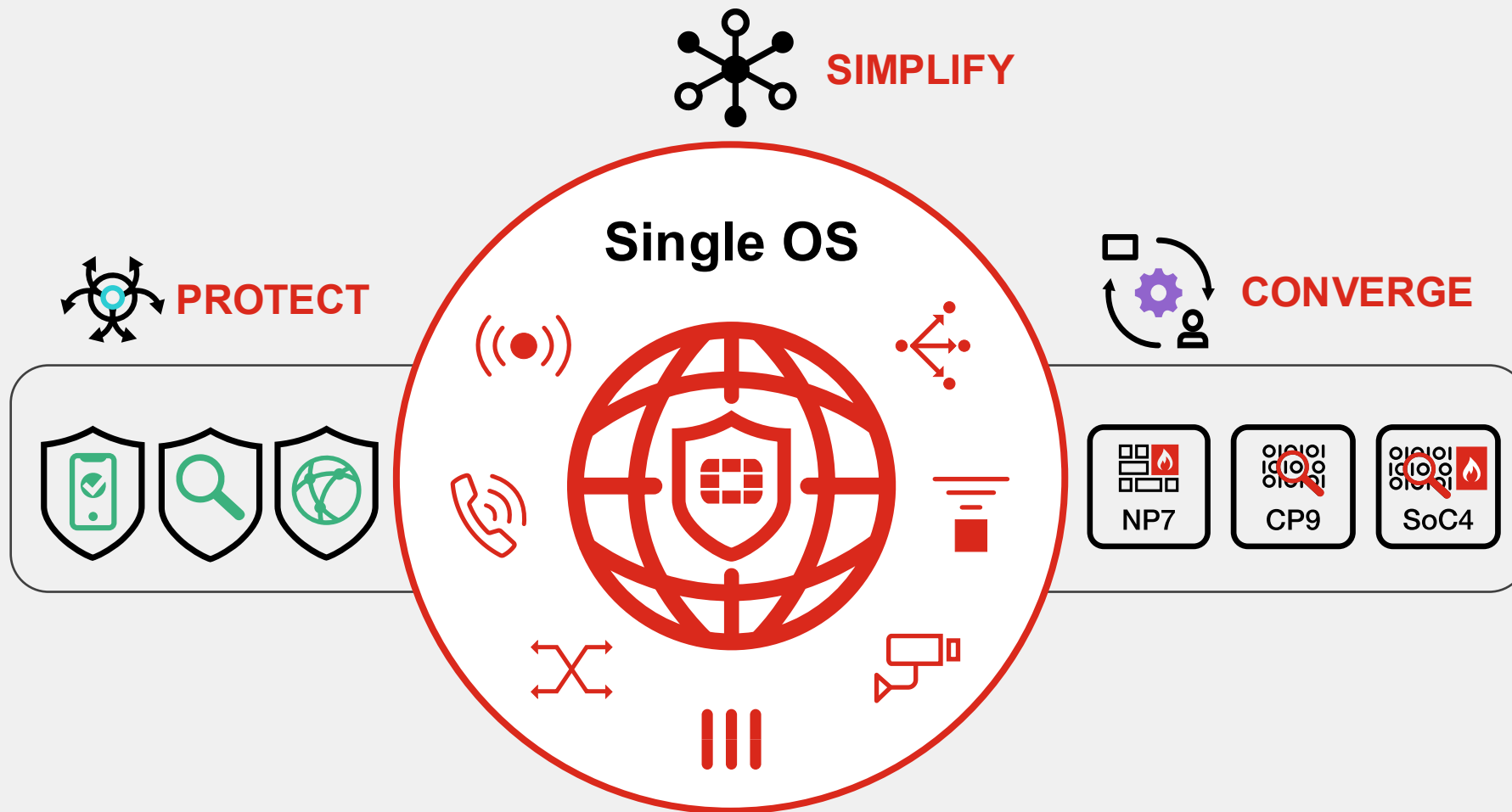
... co by měl umět dobře vychovaný firewall



Nasazení NGFW v sítích ISP



The World's **Most Deployed** NGFW





Digital Wellness



Family Digital Wellness

Challenges

Increased Malware attack awareness

80 % všech uživatelů internetu bylo zasaženo spywarem

Parental Control

Děti jsou vystaveny riziku, že narazí na nevhodný obsah; rodiče potřebují pomoc při kontrole a prosazování bezpečných internetových návyků dětí

Avoidance of complex solutions

Pouze ~5 % spotřebitelů si skutečně správně nasadí bezpečnostní aplikace

Většina zákazníků potřebuje s nasazením asistenci

Data and Identity Protection

Jeden ze tří spotřebitelů, nebo někdo z jejich domácnosti, měl ukradené osobní údaje

Increase in attack surface with IOT and smart home devices

Nárůst počtu zařízení v domácnosti zvyšuje riziko útoků na chytrá zařízení, která jsou zranitelná a využívána útočníky

STRATOS

PřehledTarifBezpečnostFakturyPodpora

+420 777 214 908

OCHRANA SÍTĚ

Bezpečnostní profil

Ochrana probíhá na naší síti, takže platí pro všechna zařízení připojená k této přípojce. Změna se propíše do 5 minut, přeinstalovat nic nemusíte.

PROFIL 00

Čistý internet

Bez filtrování. Provoz jde přímo, nic za vás neblokujeme.

BLOKUJE 0 / 8 KATEGORIÍ

PROFIL 01

Bronze

Základní bezpečnost: blokování phishingu, škodlivých stránek a ochrana před botnety.

BLOKUJE 3 / 8 KATEGORIÍ

AKTIVNÍ

PROFIL 02

Silver

Vše z Bronze a navíc extremismus, zneužívání dětí, terorismus a stránky obsahující násilí.

BLOKUJE 7 / 8 KATEGORIÍ

PROFIL 03

Gold

Vše ze Silver a navíc pornografie.

BLOKUJE 8 / 8 KATEGORIÍ

AKTIVNÍBronze

VYBRÁNOČistý internet

Změna se propíše do 5 minut.

Uložit profil

9:41

Bezpečnost

OCHRANA SÍTĚ

Ochrana platí pro všechna zařízení na přípojce 0P-44 118 902.

Čistý internet

Bez filtrování. Provoz jde přímo, nic za vás neblokujeme.

BLOKUJE 0 / 8 KATEGORIÍ

ZOBRAZIT DETAIL

Bronze

Základní bezpečnost: blokování phishingu, škodlivých stránek a ochrana před botnety.

BLOKUJE 3 / 8 KATEGORIÍ

ZOBRAZIT DETAIL

Silver

Vše z Bronze a navíc extremismus, zneužívání dětí, terorismus a stránky obsahující násilí.

BLOKUJE 7 / 8 KATEGORIÍ

ZOBRAZIT DETAIL

Gold

AKTIVNÍSilver

VYBRÁNOBronze

Aktivovat Bronze

© Fortinet Inc. All Rights Reserved. 9

Digital Wellness

CUSTOMER PROFILE (example):

Application Control:

- SocialMedia ✓
- Collaboration ✓
- Game ✗
- Video/Audio ✗
-

WebFiltering:

- Gambling ✓
- Malicious ✗
- Weapons ✓
- Phishing ✗
-

AntiMalware & Botnet Protection:

- Enable ✓
- Disable

Zákazník má možnost vybrat požadovaný profil pro celou svou síť a to na základě kombinace různých profilů:

- Application Control
- Web Filtering / DNS Filtering
- AntiMalware Protection
- BotNet Protection

Každá kombinace profilů bude nakonfigurována do specifického FW pravidla, který je vázán na konkrétní Radius skupinu. RSSO umožňuje mapování IP adres zákazníků a odebíraných služeb na příslušné Radius skupiny

Rule 01 (RSSO Group 01):

- Block Video/Audio and Game (APPCONTROL PROFILE 1)
- Block Malicious (WEBFILTER PROFILE 1)
- Protection Enabled (IPS PROFILE 1 + ANTIVIRUS PROFILE 1)

Digital Wellness – App Control

Example A

Block All Social Media Applications

Při výběru tohoto profile nebude uživatel schopen procházet a používat všechny aplikace kategorizované jako Social Media.

Name: Block_SocialMedia
Comments: 0/255

Categories: All Categories

- Business (153, 6)
- Email (77, 12)
- Mobile (3)
- Proxy (180)
- Storage.Backup (161, 19)
- VoIP (24)
- Cloud.IT (66, 1)
- Game (86)
- Network.Service (333)
- Remote.Access (95)
- Update (49)
- Web.Client (24)
- Collaboration (268, 16)
- General.Interest (235, 9)
- P2P (56)
- Social.Media (117, 30)
- Video/Audio (153, 17)
- Unknown Applications

Network Protocol Enforcement: [ON]

Application and Filter Overrides

Priority	Details	Type	Action
No results			

Example B

Block All Social Media Applications except LinkedIn

Nakonfigurováním override umožníte uživateli přístup k LinkedIn, zatímco všechny ostatní sociální sítě budou blokovány.

Name: Block_SocialMedia_Except_Linkedin
Comments: 0/255

Categories: All Categories

- Business (153, 6)
- Email (77, 12)
- Mobile (3)
- Proxy (180)
- Storage.Backup (161, 19)
- VoIP (24)
- Cloud.IT (66, 1)
- Game (86)
- Network.Service (333)
- Remote.Access (95)
- Update (49)
- Web.Client (24)
- Collaboration (268, 16)
- General.Interest (235, 9)
- P2P (56)
- Social.Media (117, 30)
- Video/Audio (153, 17)
- Unknown Applications

Network Protocol Enforcement: [ON]

Application and Filter Overrides

Priority	Details	Type	Action
1	LinkedIn LinkedIn_File.Download LinkedIn_File.Upload LinkedIn_Login	Application	Allow

Example C

Allow All Social Media Applications except Facebook

Při výběru tohoto profilu uživatel již nebude mít přístup k Facebooku; všechny ostatní sociální media jsou povoleny.

Name: DPI-BlockFacebook
Comments: DPI Block Facebook 18/255

Categories: All Categories

- Business (179, 6)
- Email (87, 12)
- Mobile (3)
- Proxy (106)
- Storage.Backup (296, 16)
- VoIP (31)
- Cloud.IT (31)
- Game (124)
- Network.Service (332)
- Remote.Access (91)
- Update (48)
- Web.Client (18)
- Collaboration (293, 6)
- General.Interest (241, 9)
- P2P (85)
- Social.Media (150, 31)
- Video/Audio (206, 13)
- Unknown Applications

Network Protocol Enforcement: [ON]

Application and Filter Overrides

Priority	Details	Type	Action
1	Facebook Facebook.App Facebook.App_AngryBirds Facebook.App_AvengersAlliance	Application	Block

Example D

Block All Video/Audio Applications except Netflix

Netflix je jediná povolená Video/Audio aplikace. Žádná jiná aplikace není povolena (např. Spotify, Youtube atd.).

Name: AllowNetflix
Comments: Allow Only Netflix 18/255

Categories: All Categories

- Business (179, 6)
- Email (87, 12)
- Mobile (3)
- Proxy (106)
- Storage.Backup (296, 16)
- VoIP (31)
- Cloud.IT (31)
- Game (124)
- Network.Service (332)
- Remote.Access (91)
- Update (48)
- Web.Client (18)
- Collaboration (293, 6)
- General.Interest (241, 9)
- P2P (85)
- Social.Media (150, 31)
- Video/Audio (206, 13)
- Unknown Applications

Network Protocol Enforcement: [ON]

Application and Filter Overrides

Priority	Details	Type	Action
1	Netflix Netflix.Login Netflix.Search Netflix.Video.Access Netflix.Video.Play	Application	Allow



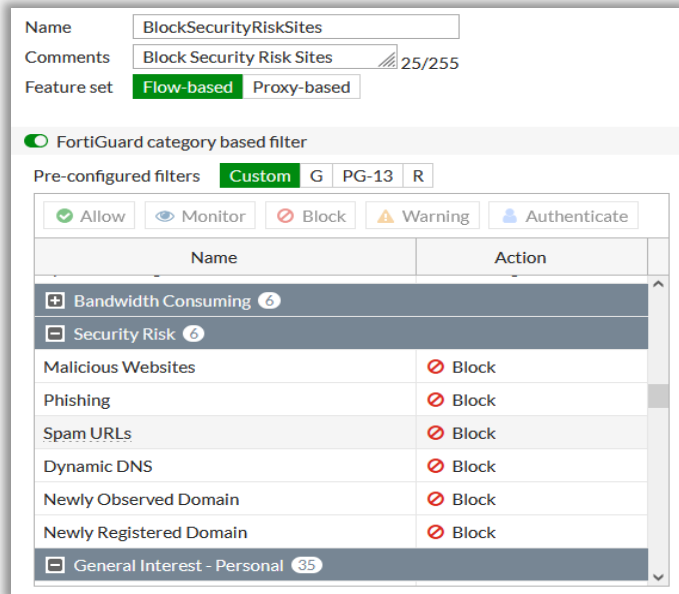
Digital Wellness – Web Filtering

Web Filtering omezuje nebo kontroluje přístup uživatelů k webovým stránkám. FortiGuard vylepšuje funkce webového filtru tím, že třídí miliardy webových stránek do 8 kategorií (a 90 podkategorií), které uživatelé mohou povolit, zablokovat, sledovat nebo povolit s varováním.

Example Profile 1

*Blocking All Sites
in “Security Risk” Category.*

Obsahuje také Malicious Website, Phishing, Spam URLs, ale také všechny Newly Observed Domain



Name: BlockSecurityRiskSites
Comments: Block Security Risk Sites 25/255
Feature set: Flow-based Proxy-based

FortiGuard category based filter

Pre-configured filters: Custom G PG-13 R

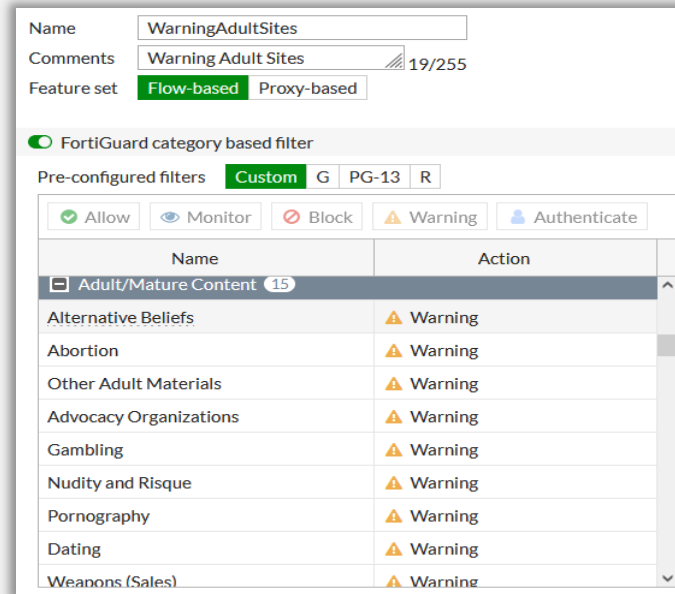
Actions: Allow Monitor Block Warning Authenticate

Name	Action
Bandwidth Consuming 6	
Security Risk 6	
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block
Newly Observed Domain	Block
Newly Registered Domain	Block
General Interest - Personal 35	

Example Profile 2

*Warning All Adult Sites
in “Adult/Mature Content” Category.*

Uživatel obdrží varování, než bude moci přistoupit na stránky týkající se gamblingu, pornografie, seznamky atd.



Name: WarningAdultSites
Comments: Warning Adult Sites 19/255
Feature set: Flow-based Proxy-based

FortiGuard category based filter

Pre-configured filters: Custom G PG-13 R

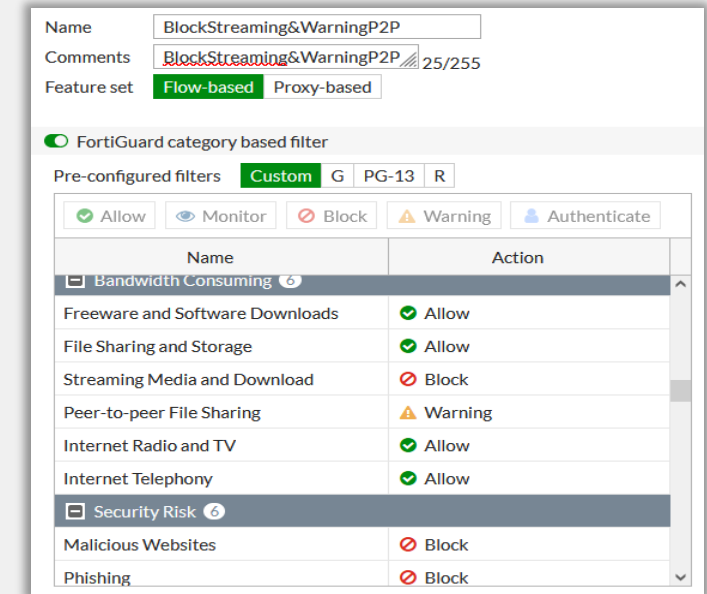
Actions: Allow Monitor Block Warning Authenticate

Name	Action
Adult/Mature Content 15	
Alternative Beliefs	Warning
Abortion	Warning
Other Adult Materials	Warning
Advocacy Organizations	Warning
Gambling	Warning
Nudity and Risque	Warning
Pornography	Warning
Dating	Warning
Weapons (Sales)	Warning

Example Profile 3

*Blocking Streaming and Warning P2P Site
in “Bandwidth Consuming” Category.*

V rámci stejné kategorie lze provést více výběrů u každé jednotlivé sub-kategorie



Name: BlockStreaming&WarningP2P
Comments: BlockStreaming&WarningP2P 25/255
Feature set: Flow-based Proxy-based

FortiGuard category based filter

Pre-configured filters: Custom G PG-13 R

Actions: Allow Monitor Block Warning Authenticate

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Block
Peer-to-peer File Sharing	Warning
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block
Phishing	Block



Digital Wellness – DNS Filtering

FortiGuard DNS Filtering Service - Defend against DNS-based attacks

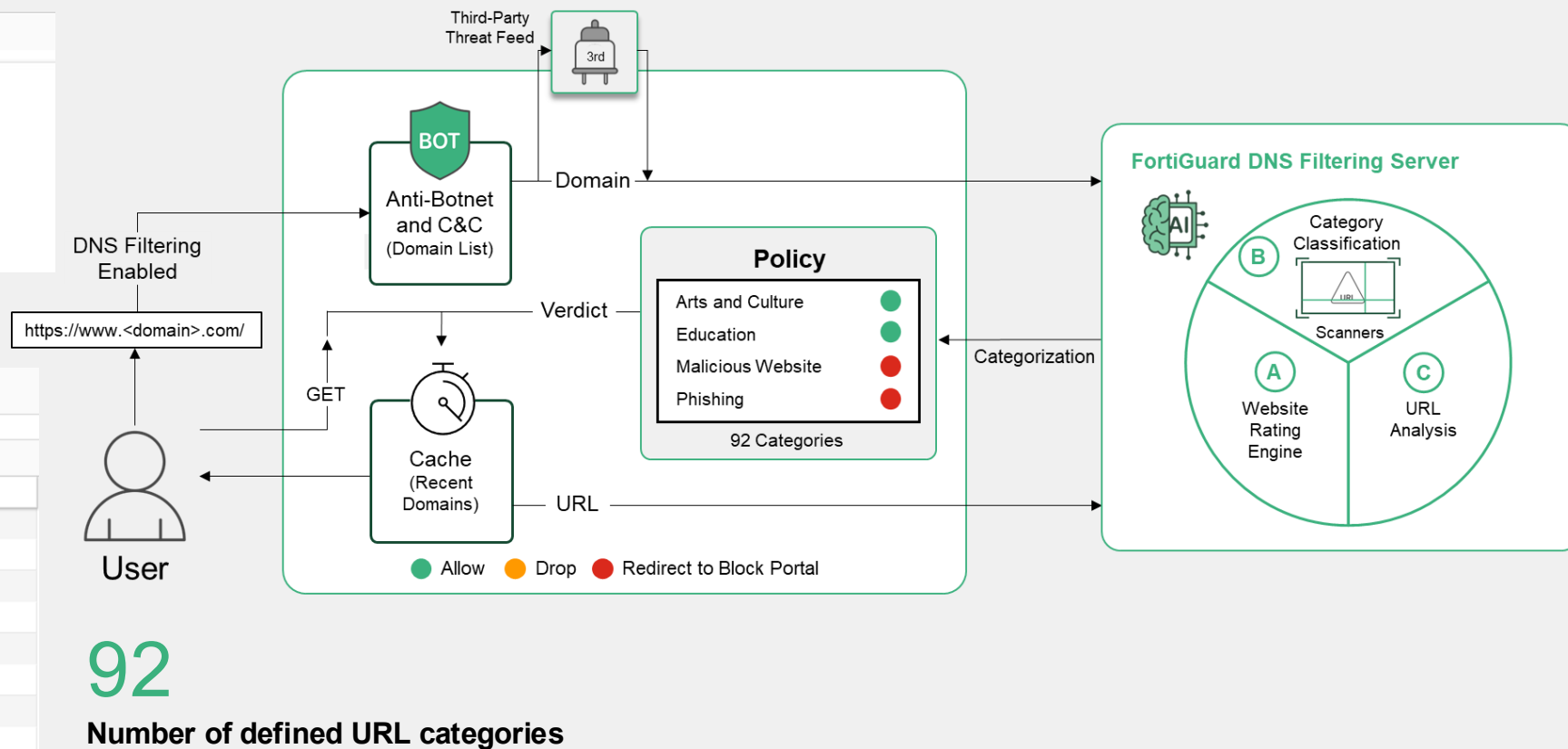
Edit DNS Filter Profile

Name: default
Comments: Default dns filtering. 22/255
Redirect botnet C&C requests to Block Portal: ☒
Enforce 'Safe Search' on Google, Bing, YouTube: ☒

79997 domains in botnet package

Botnet C&C Domain Definitions

FQDN	Name
cloud4box.ru	Regretlocker
bitcoincasino.name	Gunra
cloudcontents.info	Gunra
absshop-ping.xyz	Potemkin
d3qx7quq68rdce.cloudfront.net	Astarionrat
tgzh.club	Redosdru
dysphoria.androiddebugbridge.su	Jackskid
ipmoyu.com	Jackskid
jerusalem.androiddebugbridge.su	Jackskid



Cloud

Endpoint

Network

OT*

IoT*

Digital Wellness – Anti-Botnet

FortiGuard Labs poskytuje síťovým zařízením informace o hrozbách v reálném čase — data o škodlivých IP adresách a doménách, získávaná z distribuované sítě senzorů hrozeb Fortinet a z dalších sdílených a globálních zdrojů sledujících

[Edit IPS Sensor](#)

Name

Block_Botnet

Comments

Write a comment... 0/255

Block malicious URLs

☒

IPS Signatures and Filters

+ Create New

Edit

Delete

Details	Exempt IPs	Action	Packet Logging
No results			

0

Botnet C&C

Scan Outgoing Connections to Botnet Sites

Disable

Block

Monitor

3533 IP Addresses in botnet package.

Botnet C&C IP Definitions			
Search		Q	
IP	Port	Protocol	Name
8.18.145.33	443	TCP	Sunburst
8.18.145.36	443	TCP	Sunburst
8.18.145.131	443	TCP	Sunburst
8.18.145.134	443	TCP	Sunburst
8.18.145.136	443	TCP	Sunburst
8.18.145.139	443	TCP	Sunburst
8.18.145.150	443	TCP	Sunburst
8.18.145.157	443	TCP	Sunburst
8.18.145.181	443	TCP	Sunburst
8.212.145.71	80	TCP	Malware.Botnet.Phishing
8.212.179.217	80	TCP	Malware
13.57.184.217	443	TCP	Sunburst
13.59.205.66	443	TCP	Sunburst
13.65.211.207	80	TCP	AveMariaRAT
13.66.29.191	80	TCP	Malware
13.66.153.98	80	TCP	AsyncRAT
13.77.222.211	80	TCP	Vjw0rm
13.78.202.41	80	TCP	Ousaban
13.82.24.228	80	TCP	AveMariaRAT
13.92.159.78	80	TCP	Vjw0rm
13.236.109.147	80	TCP	FormBook
13.251.184.205	80	TCP	FormBook
14.17.115.109	80	TCP	DCRat
14.32.99.105	80	TCP	QuasarRAT
14.98.62.84	16,471	UDP	ZeroAccess



Digital Wellness – ISDB

FortiGuard Internet Service poskytuje komplexní seznam internetových aplikací s jejich IP adresami, číslem portu a hodnocením bezpečnosti. Tento seznam je pravidelně aktualizován tak, aby odpovídal nově publikovaným informacím o službách, včetně ASNs, geografické polohy, IP reputation, popularity atd.

Internet Service			Internet Service Group	Network Service
Internet Service			Internet Service FQDN	
+ Create new			IP Address Lookup	
			Search	
			Name	Direction
			Total IP Ranges	
			Predefined Internet Services 1,764	
			IP Reputation Database 10	
			Blockchain-Crypto.Mining.Pool	
			Destination	177
			Botnet-C&C.Server	
			Both	3,533
			Malicious-Malicious.Server	
			Both	48,789
			Phishing-Phishing.Server	
			Both	10,963
			Proxy-Proxy.Server	
			Both	6,008
			Spam-Spamming.Server	
			Both	4,995
			Tor-Exit.Node	
			Both	900
			Tor-Relay.Node	
			Both	5,484
			Tor-Tor.Node	
			Both	0
			VPN-Anonymous.VPN	
			Both	9,444

Internet Service

Internet Service FQDN

+ Create new

IP Address Lookup

Predefined Internet Services 1,764

IP Reputation Database 10

Blockchain-Crypto.Mining.P

Botnet-C&C.Server

Malicious-Malicious.Server

Malicious-Malicious.Server

NameMalicious-Malicious.Server

TypePredefined

Primary Internet Service ID11337935

DirectionBoth

Total IP ranges48,789

Total IPs50,000

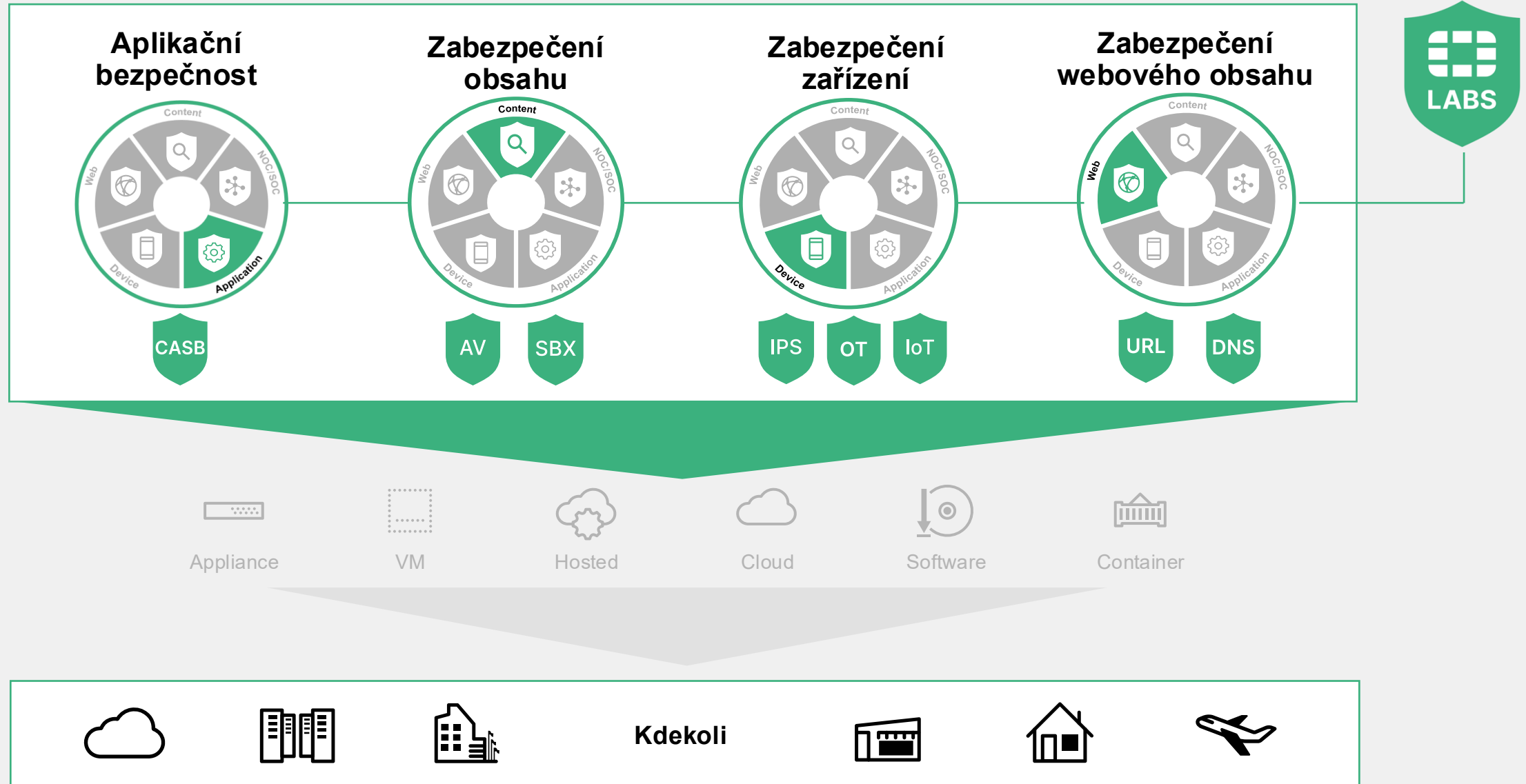
References1

View/Edit Entries

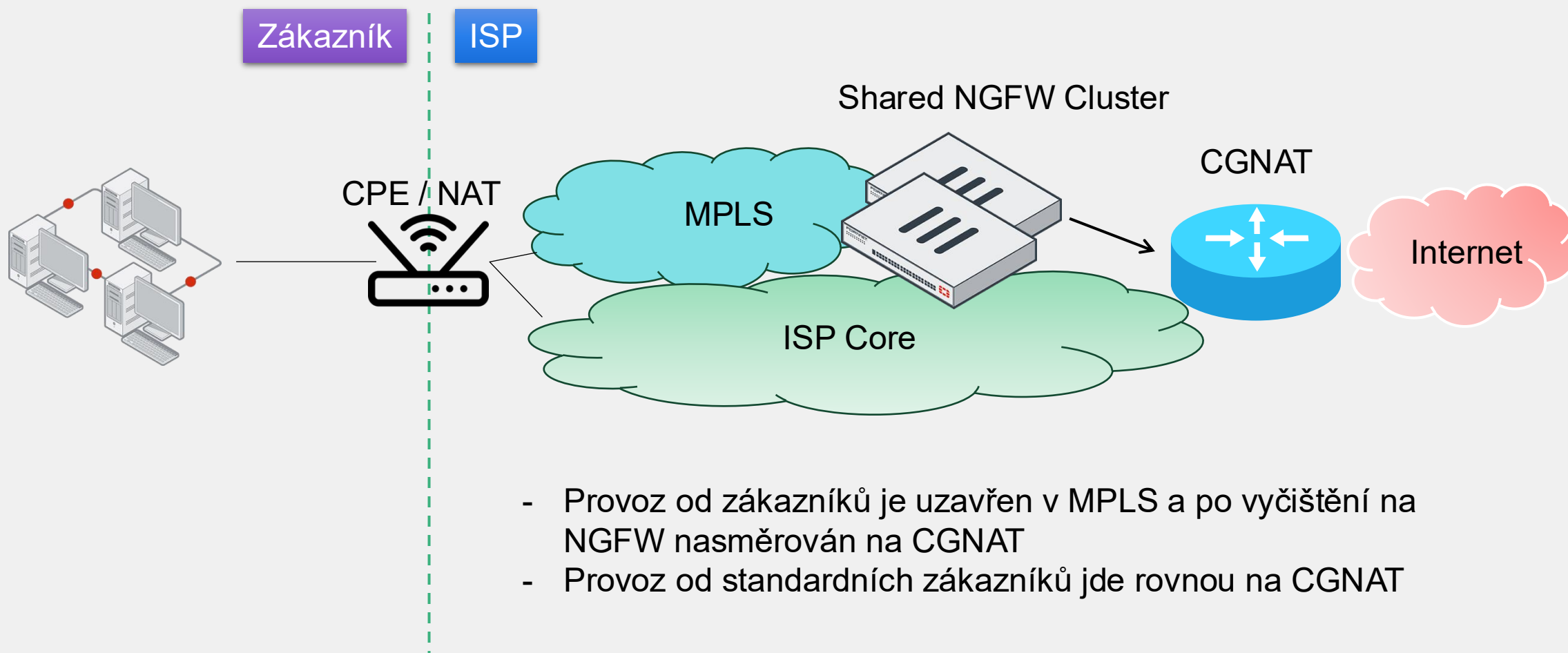
Malicious-Malicious.Server				
Enable Disable				
IPPortProtocolStatus				
☐	1.0.211.122		ICMP	Enabled
☐	1.0.211.122	80443	TCP	Enabled
☐	1.0.211.122	443	UDP	Enabled



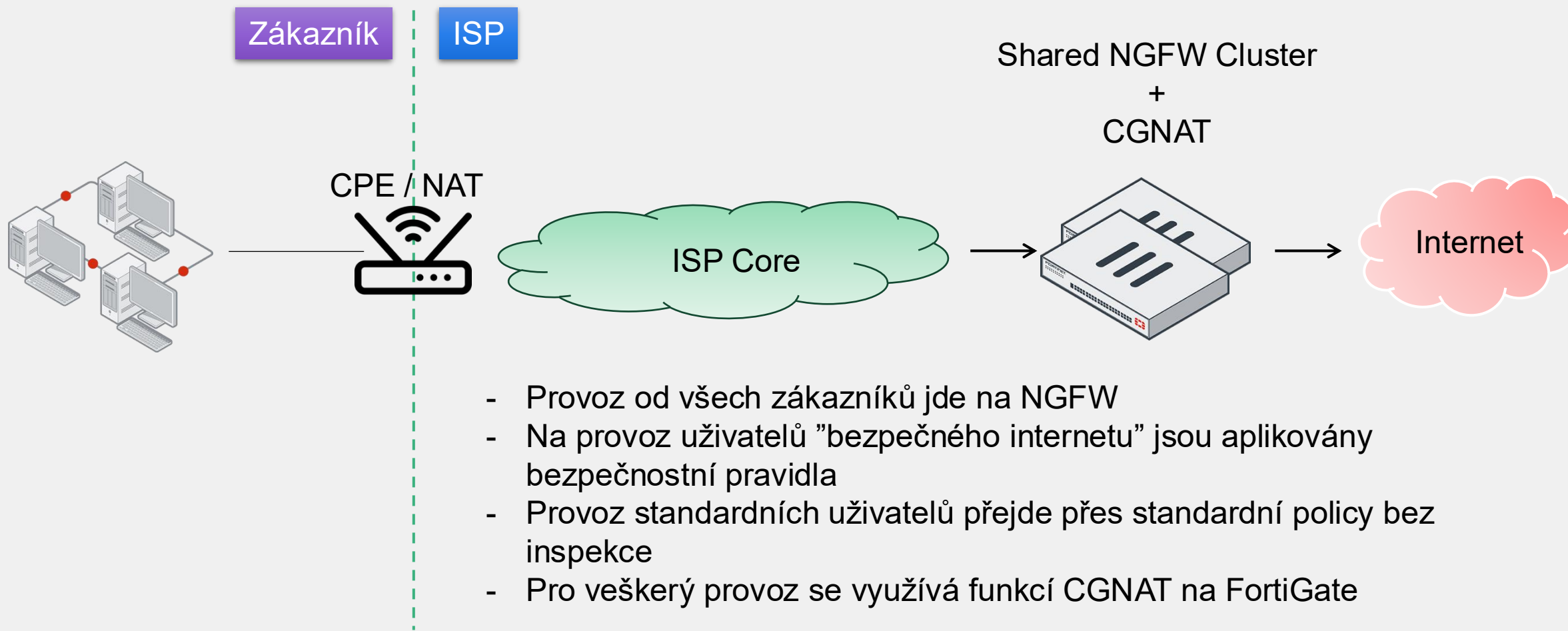
FortiGuard: Detekce hrozeb



Umístění sdíleného NGFW varianta 1

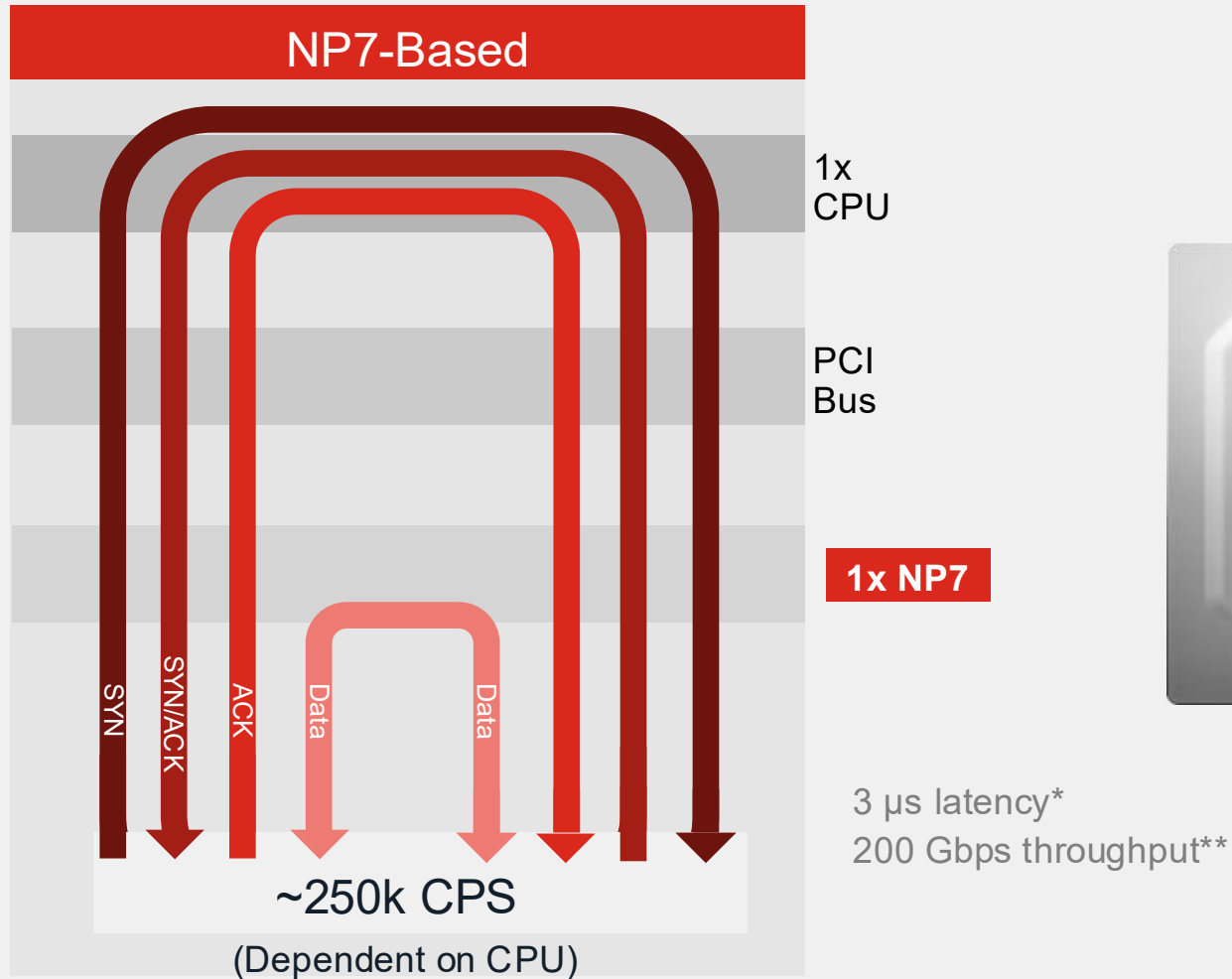


Umístění sdíleného NGFW varianta 2



CGNAT Throughput: NP7

Simplified FortiGate Session Flow for CG-NAT



 2 X 100 G NETWORK PORTS	 100 M CONCURRENT SESSIONS	 HARDWARE LOGGING	 2 M/SEC SESSION SETUP RATE
 200 GBPS FORWARDING THROUGHPUT	 75 GBPS IPSEC THROUGHPUT	 ELEPHANT FLOWS	 20 W POWER ESTIMATION

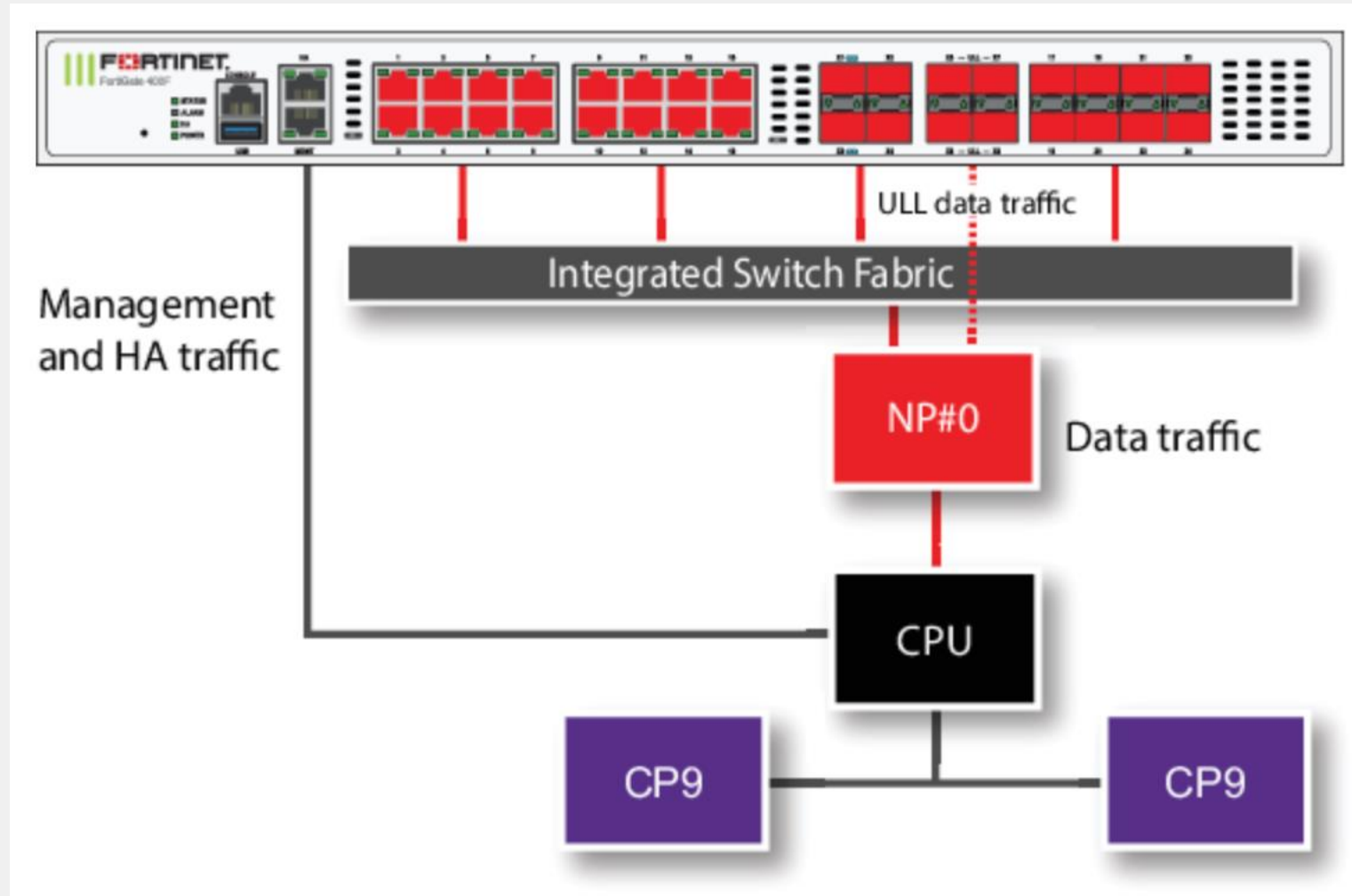


* With session logs enabled

** for UDP firewall (1518 Byte/pkt)

NP7 Architecture

FortiGate 400F



Mobile and Fixed Subscribers Provisioning

Subscribers Provisioning Methods

- Zařazení IP adresy na bezpečnostní profily je možné provádět více způsoby:
 - **Address Groups:** dají se na FortiGate nastavit (i přes API) tak, aby obsahovaly IP adresy těch zákaníků, kteří využívají nějaký ze security profilů. Add-Group-01 bude například obsahovat IP adresy zákazníků, kteří chtějí používat POLICY-01-BRONZE s příslušným profile.
 - **External IP Address List:** dá se na FortiGate nastavit jako externí URL zdroj, který si FortiGate každou minutu stahuje; obsahuje seznam IP adres jednotlivých skupin zákazníků
 - **RADIUS Accounting:** funguje na základě Start Accounting Radius requests s následujícími parametry:
 - User-Name: identifikace zákazníka
 - Framed-IP-Address: IP adresa CPE
 - Class: jméno Radius Group (tak jak je nastaveno na FortiGate)



Adress Grpup /API Call Method

Add an address to a group via API Call

STEP 1 → API CALL TO CREATE AN ADDRESS

```
{
  "method": "POST",
  "url": "/api/v2/cmdb/firewall/address",
  "params": {
    "datasource": 1,
    "vdom": "root"
  },
  "data": {
    "name": "IP-01",
    "subnet": "10.10.10.100/32",
    "color": "0"
  }
}
```



Matching Condition
Members of the
Source Group

STEP 2 → API CALL TO INSERT AN ADDRESS TO AN EXISTING GROUP

```
{
  "method": "POST",
  "url": "/api/v2/cmdb/firewall/addgrp",
  "params": {
    "datasource": 1,
    "vdom": "root"
  },
  "data": {
    "name": "GROUP-01",
    "member": [
      {
        "name": "IP-01"
      }
    ],
    "color": "0"
  }
}
```

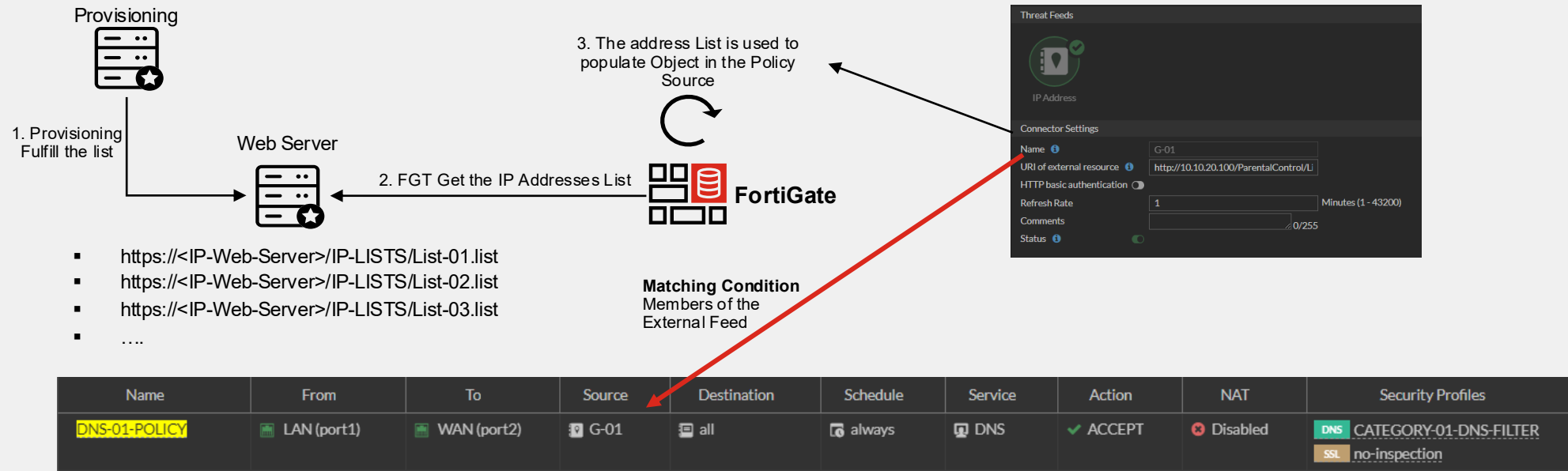
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
DNS-01-POLICY	LAN (port1)	WAN (port2)	GROUP-01	all	always	DNS	ACCEPT	Disabled	DNS CATEGORY-01-DNS-FILTER SSL no-inspection

- Pro přidání IP do existující Address Group je potřeba vytvořit dvě API volání:
- API volání pro vytvoření Address s Name (pole name) a IP Address (pole subnet)
- API volání pro vložení právě vytvořeného Address Object (pole name v member) do Address Group (pole name v data)
- Nevýhodou této metody je, že počet member (IP adres) povolených v address group je omezený; to představuje problém se škálovatelností a **nejedná se o doporučovanou metodu**.

Object	FortiGate 1800F	FortiGate 4800F	FortiGate 600F	FortiGate VM4	FortiGate VM8
firewall.addgrp.member	5000	5000	600	600	5000

IP Feed Method

Add Subscriber IP to an External IP Address List

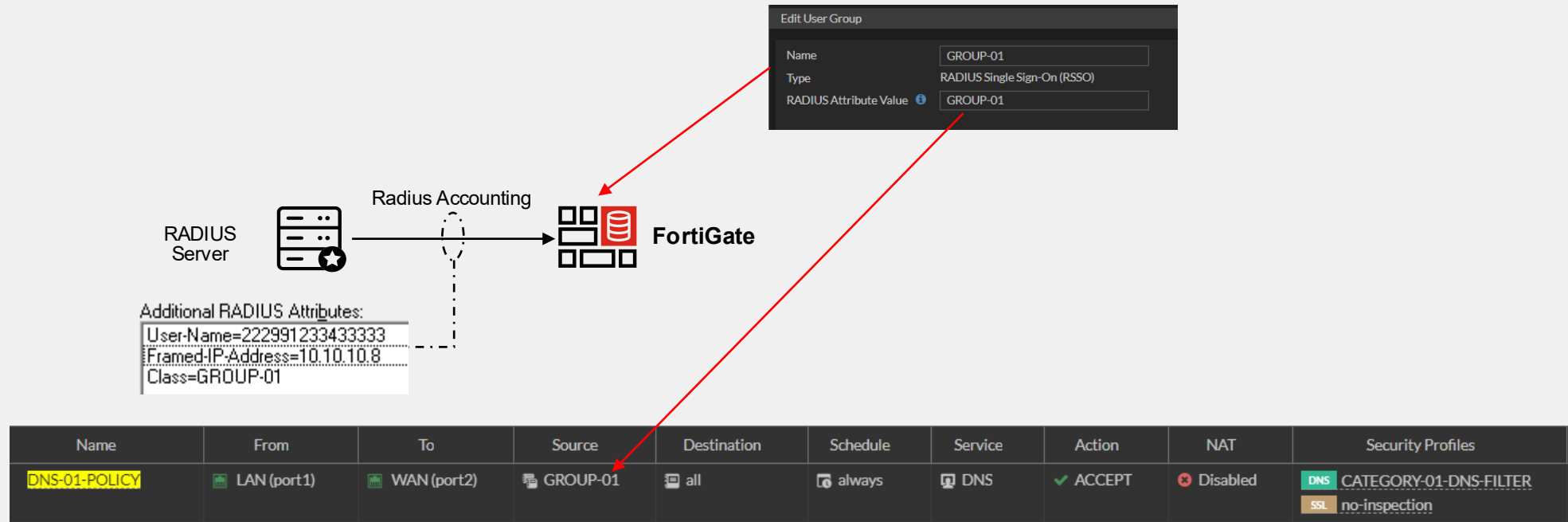


- Provisioning system/admin nahraje/upraví seznam IP adres zákazníků na web server (každý seznam odpovídá jiné skupině a je namapovaný na jinou policy).
- FortiGate si minimálně jednou za minutu stáhne seznam z web serveru a načte ho do paměti.
- FortiGate pak tyto External IP Feeds použije v policy jako matching condition.
- Z pohledu škálovatelnosti zvládne FGT obsloužit až 511 (global limit), resp. 256 (VDOM limit) external IP feeds. Každý externí soubor může mít maximálně 10 MB (jedna IPv4 adresa = 16 bajtů, takže jeden soubor pojme přibližně 600 tisíc IP adres).



RADIUS Acct Method

Using RADIUS Server as the Provisioning System



- Provisioning System (RADIUS server) generuje pro FortiGate Radius Accounting request (start/stop/update) na základě změn v samoobsluze nebo pro udržení platnosti ve skupině
- FortiGate vloží Framed-IP-Address zákazníkado skupiny určené atributem Class Radius.
- FortiGate pak najde shodu v policy tím, že Framed-IP-Address se nachází v příslušné skupině.
- Tato metoda maximalizuje škálovatelnost navrhovaného řešení a je **doporučovaným způsobem identifikace subscribers**.



FW Policy příklad

Policy	ID	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	Bytes
INET_Security_NET_block (5)	5	CUST (port5)	WAN (port1)	all UGRP-Bronze UGRP-Gold UGRP-Silver	Botnet-C&C.Server Malicious-Malicious.Server Phishing-Phishing.Server Spam-Spamming.Server +3	always		DENY			Standard		All	252 B
INET_Bronze (1)	1	CUST (port5)	WAN (port1)	all UGRP-Bronze	all	always	ALL	ACCEPT	CGNAT	NAT	Standard	AC-Bronze Block_Botnet certificate-inspection WF-Bronze	All	12.86 MB
INET_Silver (2)	2	CUST (port5)	WAN (port1)	all UGRP-Silver	all	always	ALL	ACCEPT	CGNAT	NAT	Standard	AC-Silver Block_Botnet certificate-inspection WF-Silver	All	0 B
INET_Gold (3)	3	CUST (port5)	WAN (port1)	all UGRP-Gold	all	always	ALL	ACCEPT	CGNAT	NAT	Standard	AC-Gold Block_Botnet certificate-inspection WF-Gold	All	80.81 MB
no_security (4)	4	CUST (port5)	WAN (port1)	all	all	always	ALL	ACCEPT	CGNAT	NAT	Standard	no-inspection	All	0 B
Implicit Deny (0)	0	any	any	all	all	always	ALL	DENY					Disabled	284 B

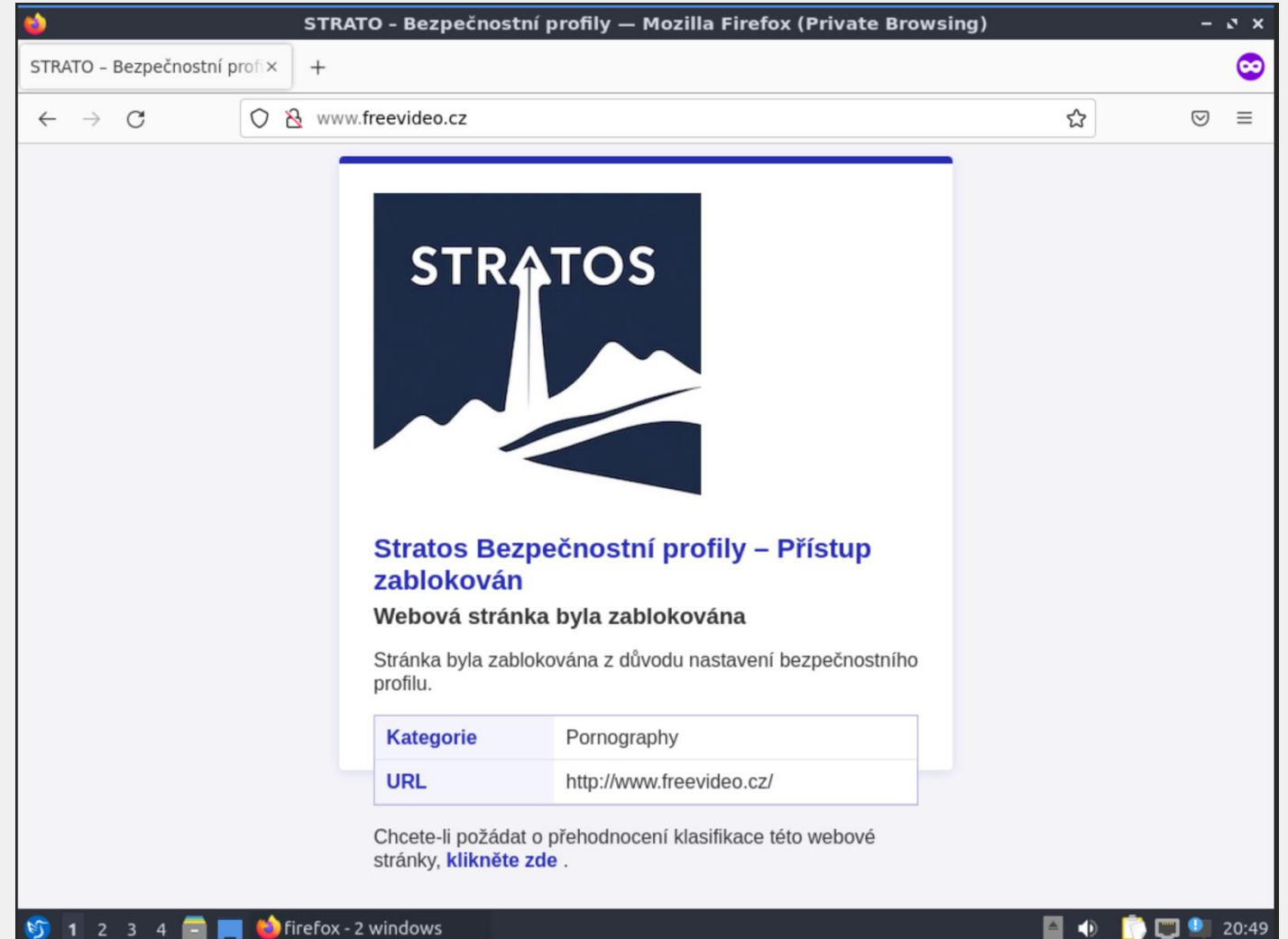
- Policy id_5 – blokuje provoz ze všech skupin na známé Botnet C&C, Malicious, Phishing, Spam... atd.
- Policy id_1 – 3 zachytí provoz dle skupin (Bronze, Silver, Gold) a na něj aplikují inspekci a NAT
- Policy id_4 je v podstatě catch_all, čistě NAT



Block Page

- Editovatelné
- Vlastní loga a texty

```
Message Format: text/html Message Size: 4.7 KB/32.0 KB
<!DOCTYPE html>
<html lang="cs">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <style type="text/css">
      body {
        height: 100%;
        font-family: 'Segoe UI', Roboto, Arial, sans-serif;
        color: #313132;
        margin: 0;
        display: flex;
        align-items: center;
        justify-content: center;
        background-color: #f4f4f8;
      }
      input[type=date], input[type=email], input[type=number], input[type=password] {
        color: #313132;
        vertical-align: baseline;
        margin: .2em;
        border-style: solid;
        border-width: 1px;
        border-color: #aeb0e2;
        background-color: #fff;
        box-sizing: border-box;
        padding: 2px .5em;
        appearance: none;
        border-radius: 0;
      }
      input:focus {
        border-color: #272cb2;
        box-shadow: 0 0 1px 0 #aeb0e2;
        outline: 0;
      }
      button {
        padding: .5em 1em;
        border: 1px solid;
        border-radius: 3px;
        min-width: 6em;
        font-weight: 400;
        font-size: .8em;
        cursor: pointer;
      }
      button.primary {
```



Log

```
date=2026-09-06 time=22:49:05 itime=2026-09-06 22:49:09 euid=1025 epid=3
dsteuid=3 dstepid=3 type=utm subtype=webfilter level=warning
action=blocked sessionid=4280 policyid=3 srcip=192.168.1.10
dstip=104.21.59.158 srcport=58732 dstport=80 proto=6 cat=14
logid=0316013056 service=HTTP user=kratos group=UGRP-Gold
eventtime=1788727745690794203 sentbyte=372 rcvdbyte=0 craction=4194304
crscore=5 crlevel=low srcintfrole=undefined dstintfrole=wan
direction=outgoing ratemethod=domain reqtype=direct
url=http://www.freevideo.cz/ hostname=www.freevideo.cz profile=WF-Gold
agent=Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/
catdesc=Pornography eventtype=ftgd_blk srcintf=port5 dstintf=port1
authserver=root msg=URL belongs to a denied category in policy tz=+0200
srcuuid=543825ac-a7e2-51ed-0184-7843ea5030f7 dstuuid=0fa9de4a-a7e1-51ed-
e375-32df569329ac policytype=policy srccountry=Reserved dstcountry=United
States poluuid=f11eb72e-aa30-51f1-fb3e-c808821e43fb httpmethod=GET
srccity=Reserved srcgeoid=1000000000 dstgeoid=6252001
devid=FGVMMLTM26016426 vd=root dtime=2026-09-06 22:49:05
srcuuid_name=LAN_1 dstuuid_name=all
```



Notifikace

SMS / Push Notifikace

```
date=2026-09-06 time=22:49:05 itime=2026-09-06 22:49:09 euid=1025 epid=3
dsteuid=3 dstepid=3 type=utm subtype=webfilter level=warning
action=blocked sessionid=4280 policyid=3 srcip=192.168.1.10
dstip=104.21.59.158 srcport=58732 dstport=80 proto=6 cat=14
logid=0316013056 service=HTTP user=kratos group=UGRP-Gold
eventtime=1788727745690794203 sentbyte=372 rcvdbyte=0 craction=4194304
crscore=5 crlevel=low srcintfrole=undefined dstintfrole=wan
direction=outgoing ratemethod=domain reqtype=direct
url=http://www.freevideo.cz/ hostname=www.freevideo.cz profile=WF-Gold
agent=Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/
catdesc=Pornography eventtype=ftgd_blk srcintf=port5 dstintf=port1
authserver=root msg=URL belongs to a denied category in policy tz=+0200
srcuid=543825ac-a7e2-51ed-0184-7843ea5030f7 dstuid=0fa9de4a-a7e1-51ed-
e375-32df569329ac policytype=policy srccountry=Reserved dstcountry=United
States poluid=f11eb72e-aa30-51f1-fb3e-c808821e43fb httpmethod=GET
srccity=Reserved srcgeoid=1000000000 dstgeoid=6252001
devid=FGVMMLTM26016426 vd=root dtime=2026-09-06 22:49:05
srcuid_name=LAN_1 dstuid_name=all
```

- User = jednoznačný identifikátor zákazníka ID
- Profil, kategorie, hostname

Poslání logu na Syslog > napárování se účtem
zákazníka dle ID (username) + doplnění
klíčových slov z logu > poslání na SMS bránu

Velmi ceněno zákazníky například v případě
zastavení komunikace na Phising, Botnet atd...



