VIAVIS střežíme podstatné

CACIO

# Outsourcing IS v „cloudu“ jako prevence kybernetického útoku?

Jan Bonczek

## Jak definujeme cloud?

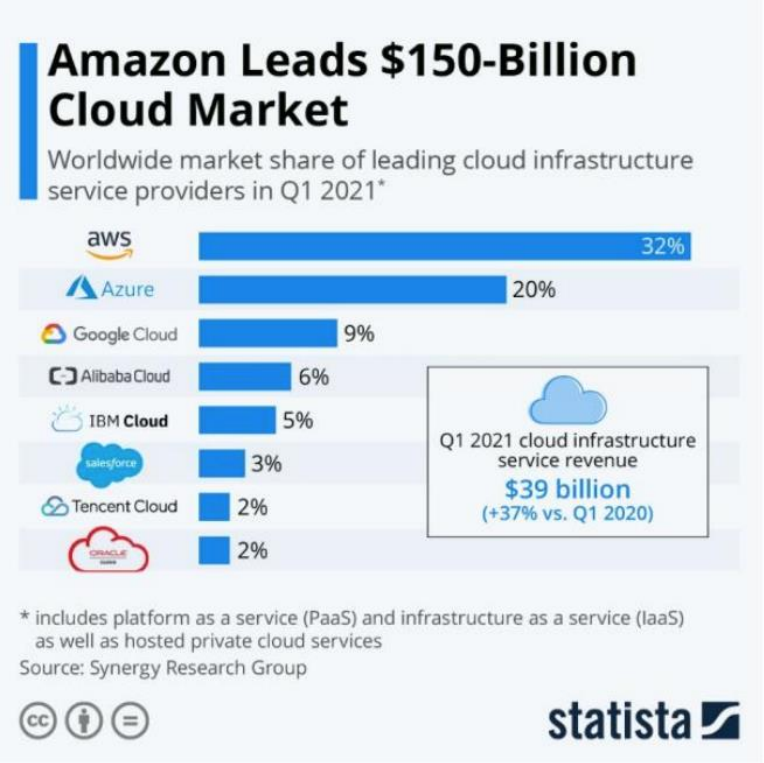
Poskytování prostředku IT za určitou cenu.
Poskytování serverů ke kterým se přistupuje přes internet.
Služby umožňující samoobslužný přístup.

## Výhody a nevýhody?

Největší rizika jsou ztráta úplně kontroly a zpracování na územích jiných států.
Soudní spor USA vs Microsoft vs Dublin

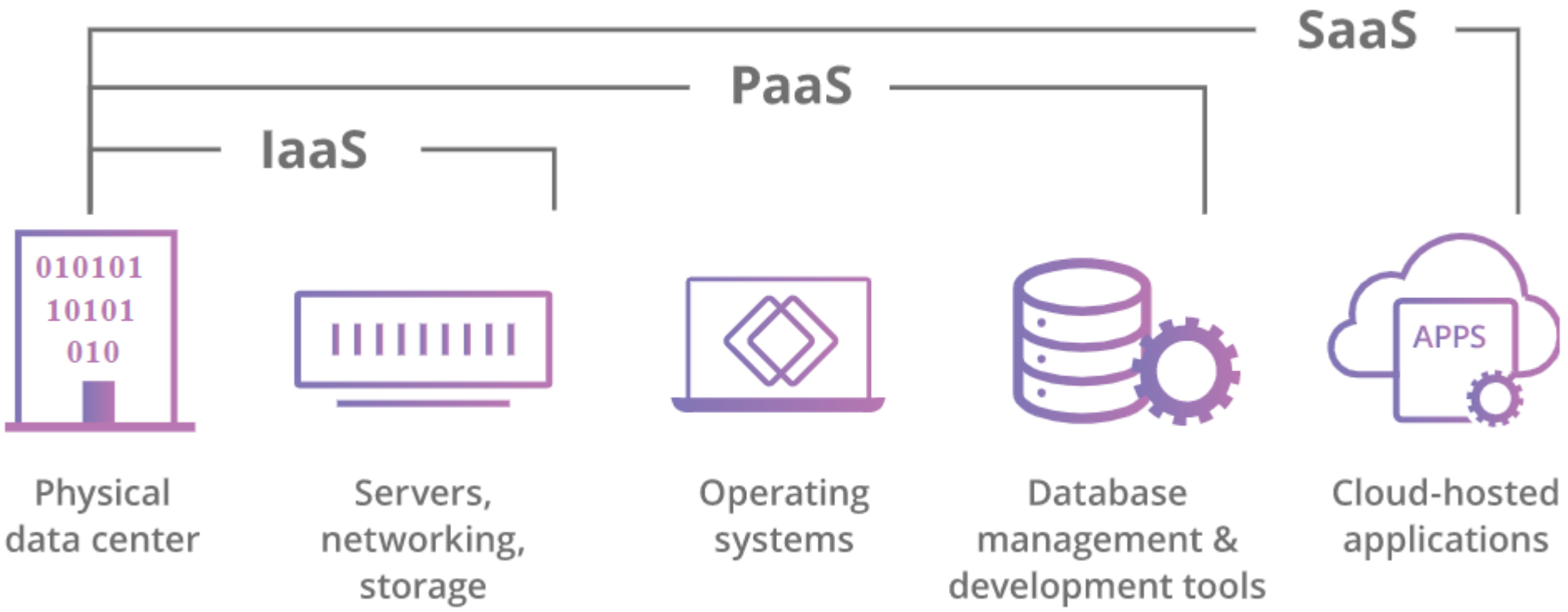
## Není cloud jako cloud

Důsledná analýza před výběrem cloudu.
Přehled o fyzickém umístění dat a jejich pohyb.
Do 2013 přesvědčení, že data patří výhradně uživateli.




Zdroj: Statista

# Hlavní modely




Zdroj: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

# Příklad útoku na „SaaS“

## Můžete mít IS v našem cloudu

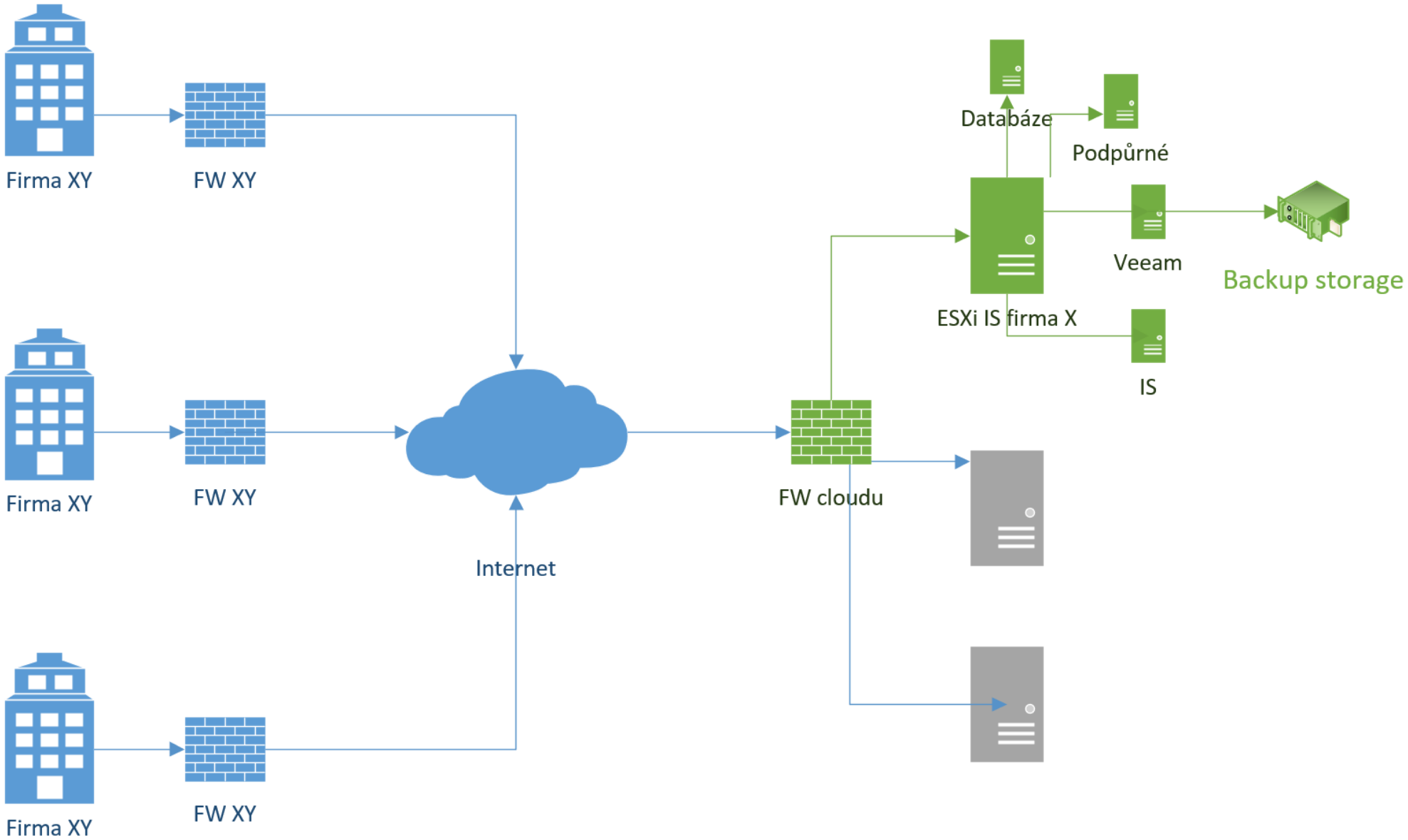
Nabídka například od tvůrce IS nebo vašeho Outsourcingu. Argumenty často šetření nákladů.

## Typicky nulová znalost infrastruktury

Pokud se nejedná o renovované datacentrum tak prakticky nemáte ponětí o jeho stavu.

## Žádné reálné ponětí o zabezpečení

Jak vlastně řeší zabezpečení? Oddělení od jiných IS? Zálohovaní, HA, a jak je nastavena samotná sít?


Firma XY
FW XY
Firma XY
FW XY
Firma XY
FW XY
Internet
FW cloudu
Databáze
Podpůrné
ESXi IS firma X
Veeam
Backup storage
IS

# Na co se ptáme?

## Jaký je rozsah?

Většinou „totálka“. Někdy se zachrání technologická síť.

## Jaké vznikají škody?

Dělám si představu hlavně o tom, jak moc velký tlak to bude na IT.

## Co jste už udělali?

Většinou samé chyby. Smazání logů. Připojení záloh do napadených systémů. Malá obezřetnost.

## Kde máte zálohy?

Nejsou? Aha. To se stane, tak jdeme dál.

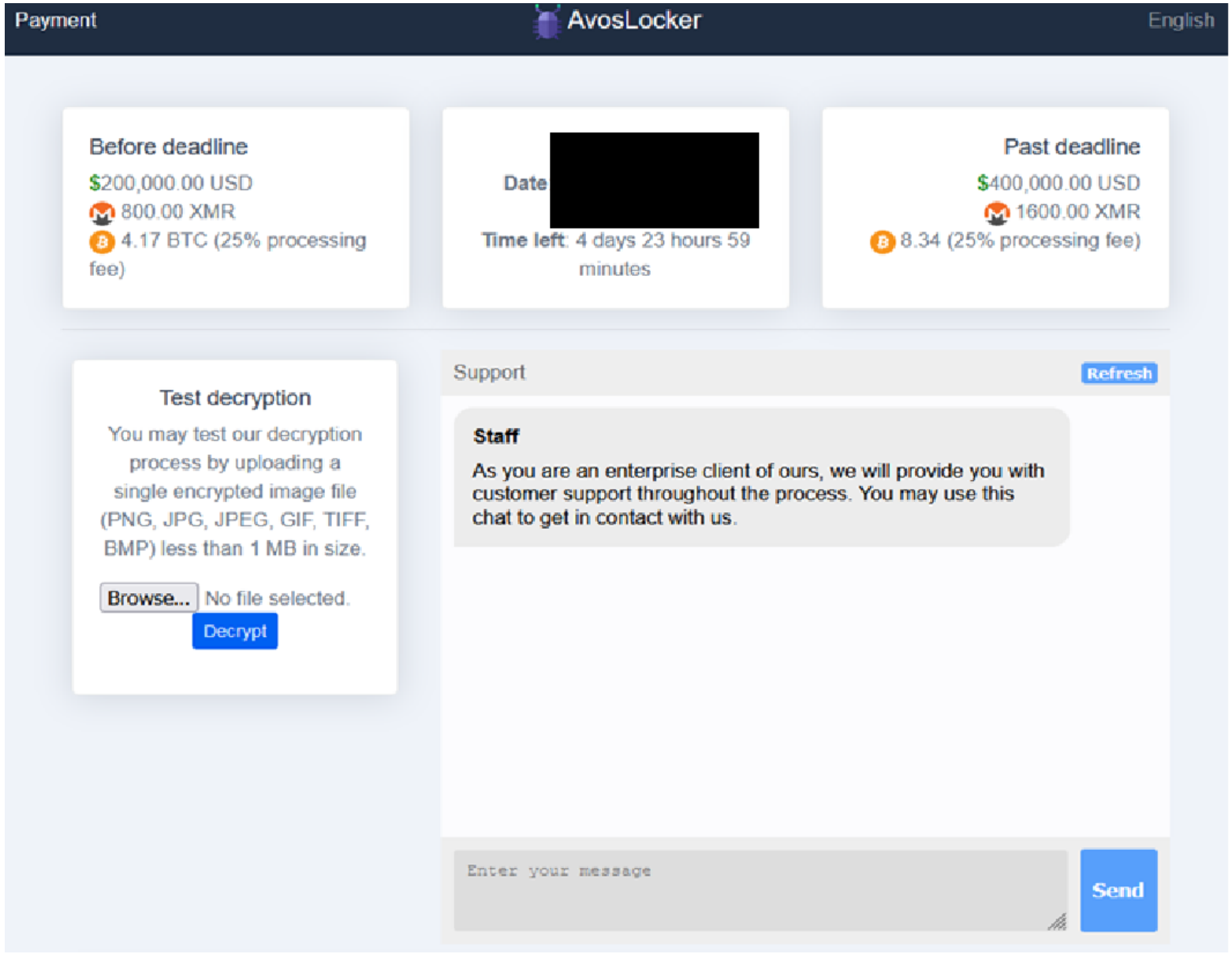
## A off-line zálohy jsou kde?

Tady se rozhoduje.

## Logy nějaké máte?

Většinou zatím všude super. Vybavení z pohledu kybernetické bezpečnosti bylo na vyšší úrovni.

# Zjistit, kdo útočil



# Jaké služby jsou vidět z venku?



# Pokusy o spojení s AnyDesk



All FortiGate | Custom... [redacted]

Service = RDP | Source IP = [redacted]

| # | ▼Date/Time | Device ID | Action | Source | User | Destination IP | Service | Application | Sent/Rec |
|---|---|---|---|---|---|---|---|---|---|
| 1 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |
| 2 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |
| 3 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |
| 4 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |
| 5 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |
| 6 | [redacted]00:11 | FG100E[redacted] | Policy violation | W[redacted] | | 10[redacted] | RDP | RDP | 0 B/0 B |

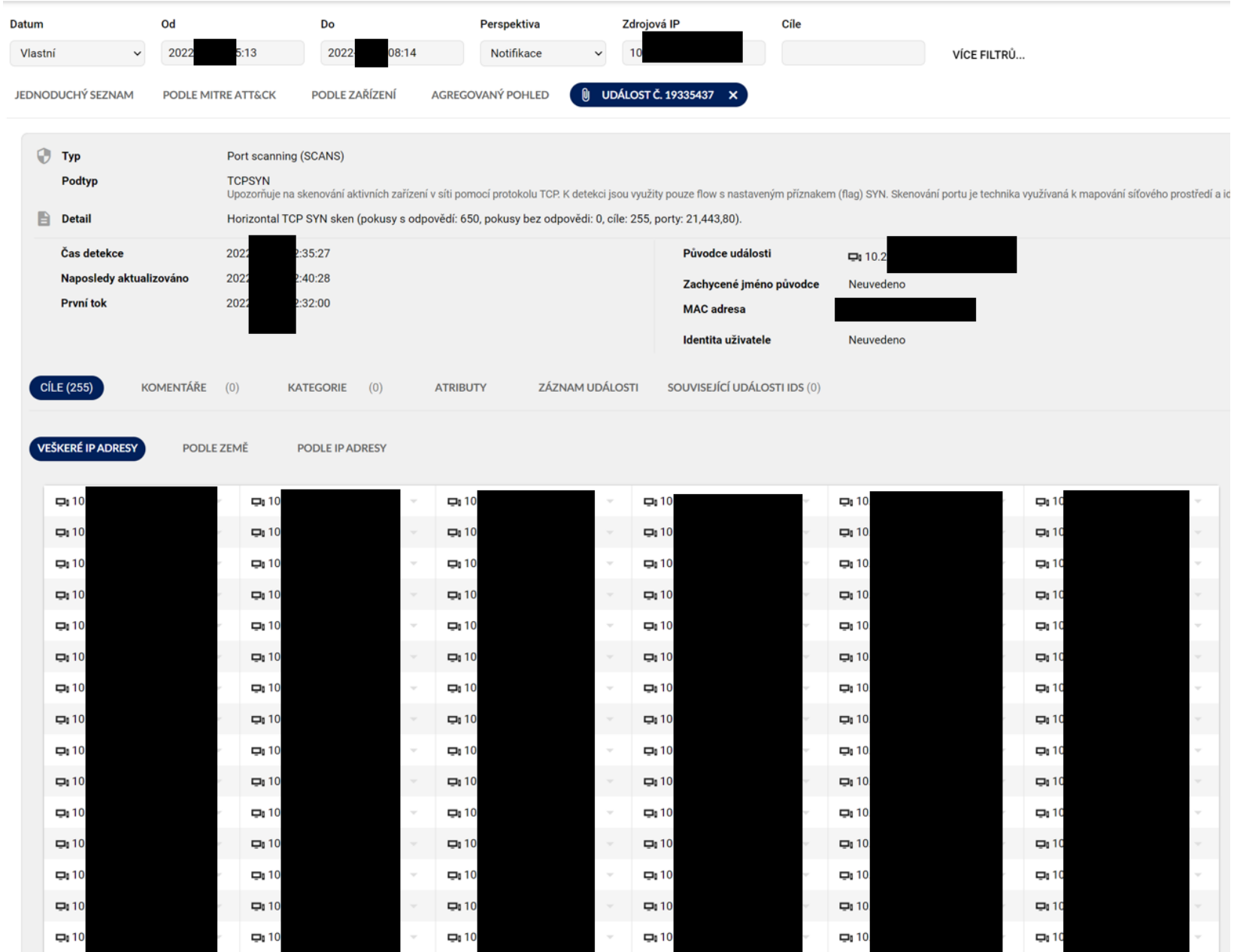
All FortiGate | Custom... | Sep 09 To Sep 11

Application = AnyDesk | Add Filter

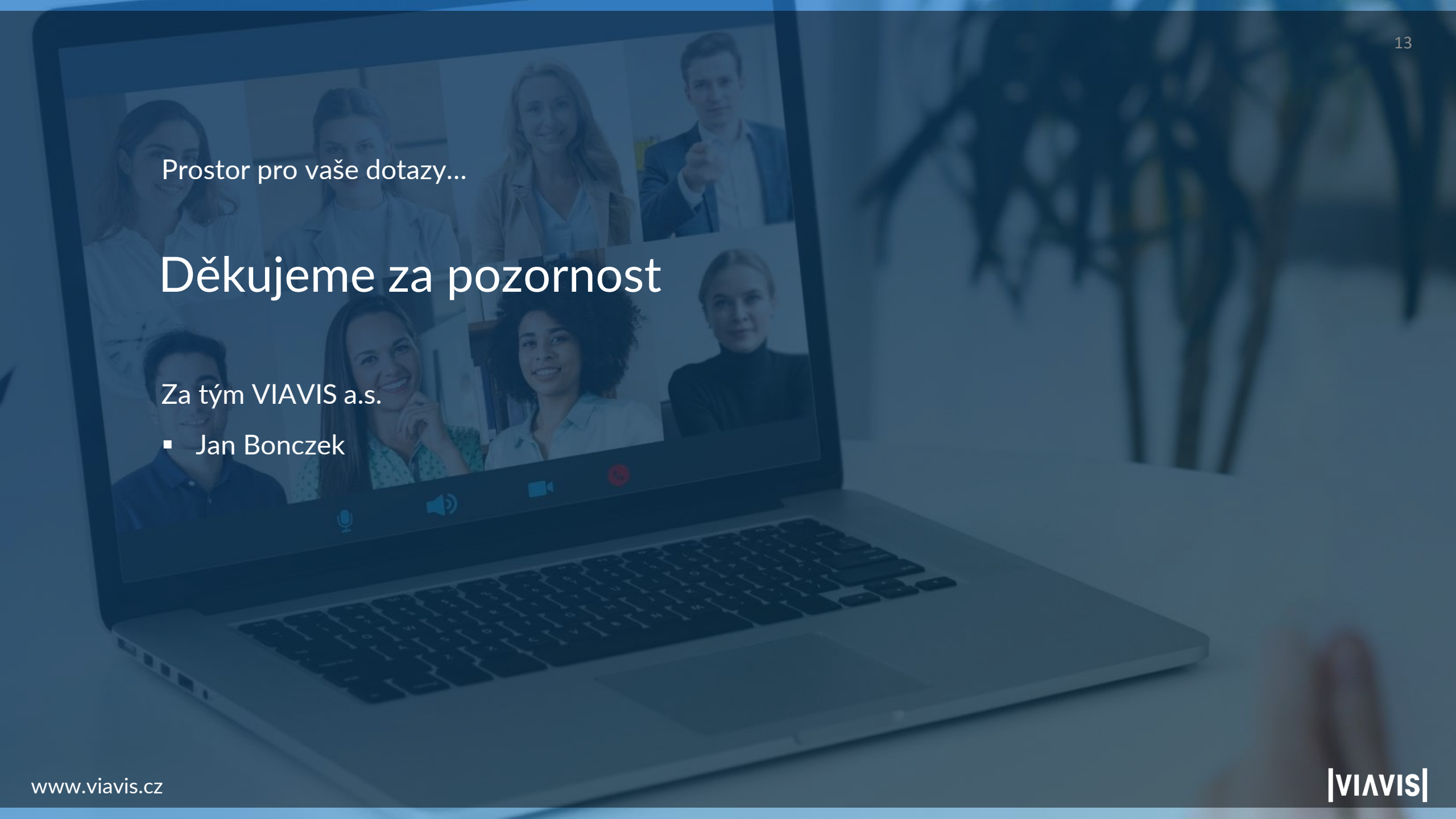
| # | ▼Date/Time | Device ID | Action | Source | User | Destination IP | Service | Application | Sent/Received |
|---|---|---|---|---|---|---|---|---|---|
| 217 | [redacted]1 00:44 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 218 | [redacted]1 00:44 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/2.6 KB |
| 219 | [redacted]1 00:43 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 220 | [redacted]1 00:42 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 221 | [redacted]1 00:42 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 185.229.[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 222 | [redacted]1 00:42 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/92.0 B |
| 223 | [redacted]1 00:41 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 224 | [redacted]1 00:40 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/2.6 KB |
| 225 | [redacted]1 00:39 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 88.198.3[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 226 | [redacted]1 00:39 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 88.198.3[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 227 | [redacted]1 00:39 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 88.198.3[redacted] | tcp/6568 | AnyDesk | 406.0 B/92.0 B |
| 228 | [redacted]1 00:38 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 88.198.3[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 229 | [redacted]1 00:37 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 88.198.3[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 230 | [redacted]1 00:36 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 88.198.3[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 231 | [redacted]1 00:36 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 88.198.3[redacted] | tcp/6568 | AnyDesk | 406.0 B/1.6 KB |
| 232 | [redacted]1 00:36 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 233 | [redacted]1 00:35 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | tcp/6568 | AnyDesk | 406.0 B/84.0 B |
| 234 | [redacted]1 00:34 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 235 | [redacted]1 00:34 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 236 | [redacted]1 00:33 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | tcp/6568 | AnyDesk | 406.0 B/2.6 KB |
| 237 | [redacted]1 00:33 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 238 | [redacted]1 00:32 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 239 | [redacted]1 00:32 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | tcp/6568 | AnyDesk | 406.0 B/1.5 KB |
| 240 | [redacted]1 00:31 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 241 | [redacted]1 00:30 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 242 | [redacted]1 00:28 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 243 | [redacted]1 00:28 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/84.0 B |
| 244 | [redacted]1 00:28 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/1.6 KB |
| 245 | [redacted]1 00:28 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 246 | [redacted]1 00:27 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 247 | [redacted]1 00:27 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTP | AnyDesk | 958.0 B/92.0 B |
| 248 | [redacted]1 00:25 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | tcp/6568 | AnyDesk | 406.0 B/92.0 B |
| 249 | [redacted]1 00:25 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 185.229.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 250 | [redacted]1 00:25 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 251 | [redacted]1 00:24 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 252 | [redacted]1 00:23 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | tcp/6568 | AnyDesk | 406.0 B/92.0 B |
| 253 | [redacted]1 00:23 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | tcp/6568 | AnyDesk | 406.0 B/2.6 KB |
| 254 | [redacted]1 00:22 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTP | AnyDesk | 1010.0 B/92.0 B |
| 255 | [redacted]1 00:22 | FG100[redacted] | Deny:UTM Blocked | [redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |
| 256 | [redacted]1 00:22 | FG100[redacted] | Deny:UTM Blocked | 10[redacted] | | 195.181.[redacted] | HTTPS | AnyDesk | 1010.0 B/92.0 B |

# Flowmon taky řval





# Antivir na servery nepatří



Prostor pro vaše dotazy…

# Děkujeme za pozornost

Za tým VIAVIS a.s.

- Jan Bonczek