OpenAlt 2026

Neděle 8. 11.

ISP router vs OPNsense

Jak a proč převzít plnou kontrolu nad vlastní domácí sítí

Praktická ukázka co se dá, využití je na vás

Odkaz na všechny materiály bude na konci přednášky

Tadeáš Nosek

PŘEDSTAVENÍ

whoami



- Student 2. ročníku SŠ oboru IT Cybersec
- IT se věnuju od malička
- Hlavní zaměření: sítě a systémy, dále desktop & web dev

PROBLÉMY

ISP router: Proč ho nemám rád

- často není moc spolehlivý
- po výpadku elektřiny nemusí naběhnout
- je uzamčený
- jakmile dojde k EOL, ISP na vás kašle
- další individuální potíže

MŮJ SETUP

OPNsense u mě doma

- moje síť je kompletně izolovaná
- u mě je to extension existující sítě
- mám soukromí
- přístup do celé sítě

HARDWARE

Na čem OPNsense rozjet

- starý laptop nebo desktop
- levný mini PC (třeba z Aliexpressu)
- ve VM (v určitých případech to může být bolest)
- na homelab serveru

> nemá ARM podporu, na Raspberry Pi ne

INSTALACE

Instalace OPNsense

1. Stáhneme ISO ze stránek
2. Bootneme z něj
3. Přihlásíme se do uživatele installer
4. Projedeme instalačku

KONFIGURACE

Prvotní konfigurace



Musíme nastavit WAN a LAN

FILTROVÁNÍ

Blocklisty přes Unbound DNS

- možnost network-wide AdBlocku
- DNS filtrování nepochytí všechny reklamy (AdBlock v browseru se hodí)
- můžete si nastavit vyjímky
- lze blockovat jakékoliv domény
- může se hodit i pro rodičovskou kontrolu nebo firemní restrikce

STRUKTURA

Organizace sítě



- Různé subnety (`10.0.0.x`, `10.15.1.x`, …)
- VLAN tagging (třeba `VLAN 20`)
- Virtuální a fyzické interfacy
- DNS názvy
- Firewall pravidla

BEZPEČNOST

Zabezpečení sítě a monitoring

- Firewall pravidla (Default Deny Policy)
- Oddělení veřejné a privátní sítě (VLAN)
- Intrusion Detection (zabudovaná Suricata)
- Živé sledování trafficu
- Blokování malicious stránek přes DNS blocklisty

VZDÁLENÝ PŘÍSTUP

Mesh VPN

- Tailscale (jako plugin v OPNsense)
- dá se použít pro remote access na celou síť,
- ale i opačně kde síť bude mít přístup k remote zařízením

ANONYMITA

Privacy VPN



- WireGuard, OpenVPN
- možnost schovat traffic (i před ISP)
- možnost se vydávat za jinou lokalitu (třeba na sledování geo-blocked filmů/seriálů)

INCIDENTY

Co když mi to spadne?



nejspíš vám nepůjde síť



hodí se fyzický přístup k mašině



kernel panic se reportuje



logy jsou k dispozici



jde udělat FS check

PREVENCE

Jak předejít pádu, na co si dát pozor

- doporučuji dělat backupy (jdou i na Google Drive nebo Nextcloud)
- nedělat nic zasahujícího v kritických momentech
- dají se dělat boot environmenty (pokud instalujete na ZFS)

Všechny materiály zde:



tadeasnosek.cz/openalt26

Děkuji za pozornost.

nyní máte prostor na dotazy