

Zabezpečení digitálních zařízení a dat

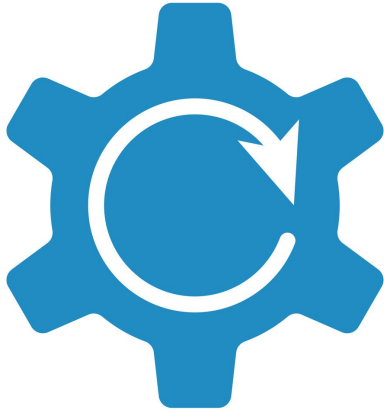
Obsah

- 1/ Fyzické zabezpečení**
- 2 / Aktualizace**
- 3 / Antivirový software**
- 4 / Firewall**
- 5 / Ochrana před uživatelem**
- 6 / Sandbox**

1 / Fyzické zabezpečení

- Ochrana počítače před neoprávněným zacházením a nechtěnému poškození.
- Doporučení:
 - Nenechávat zařízení bez dozoru
 - Použití zámků a bezpečnostních kabelů na veřejnosti
 - Chráněný vstup do budovy

2 / Aktualizace



Update....



- Aktualizace softwaru a operačního systému jsou klíčové pro zajištění bezpečnosti a stability vašich zařízení.
- Obsahují:
 - Opravy chyb
 - Bezpečnostní záplaty
 - Nové funkce ochrany



3 / Antivirový software

- Počítačový software sloužící k identifikaci, odstranění a eliminaci počítačových virů a jiného škodlivého software (malware)
- Metody:
 - Virové slovníky/databáze
 - Nebezpečné chování

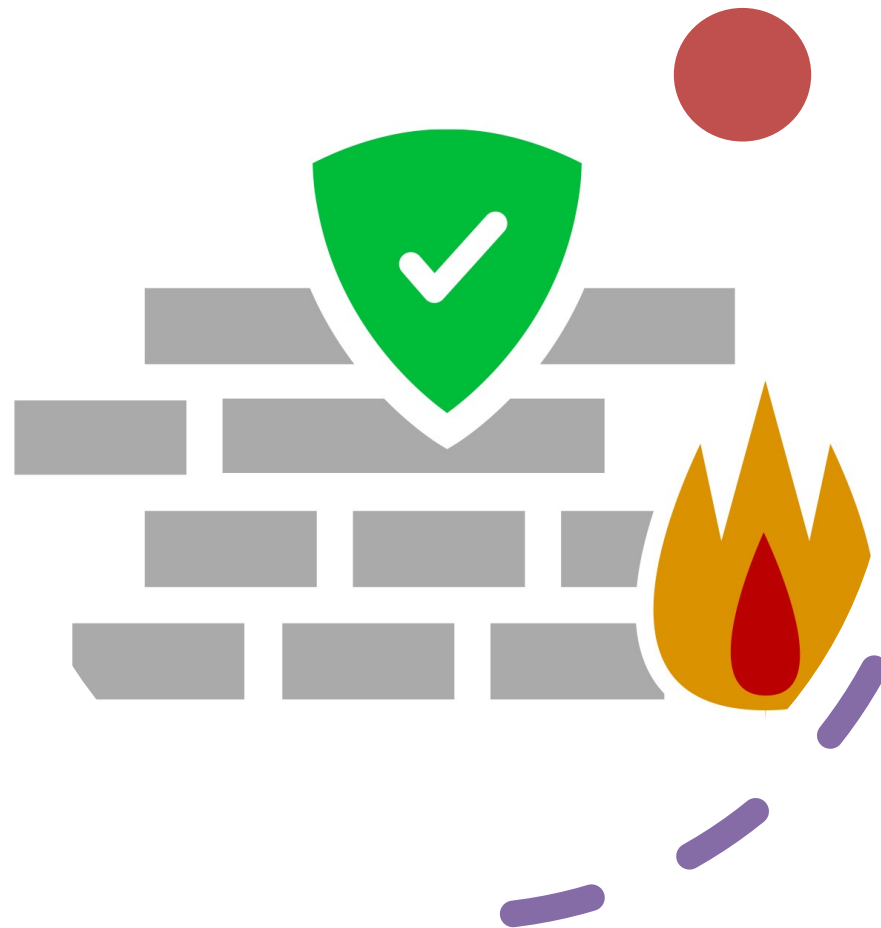
4 / Firewall

- Bezpečnostní síťové zařízení
- Slouží k řízení síťového provozu
- Definuje pravidla pro komunikaci mezi sítěmi
- Odděluje sítě
- Dělení podle umístění:
 - Síťový firewall – samostatné hardwarové řešení pro ochranu počítačové sítě
 - Personální firewall – na koncových stanicích (počítačích)

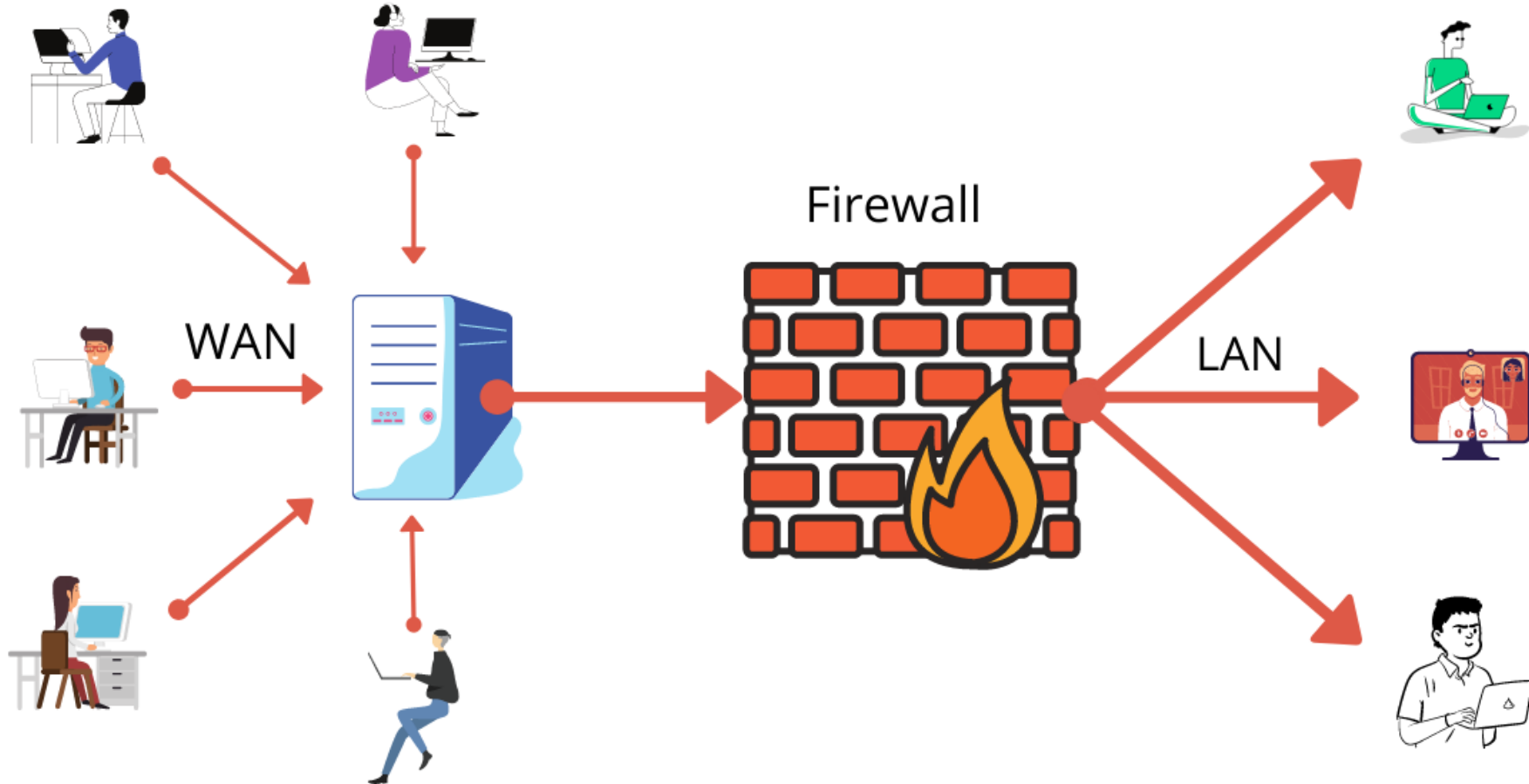


4 / Firewall

- Kategorie firewallů
 - Paketové filtry
 - Aplikační brány
 - Stavové paketové filtry
 - Stavové paketové filtry s kontrolou známých protokolů



4 / Firewall



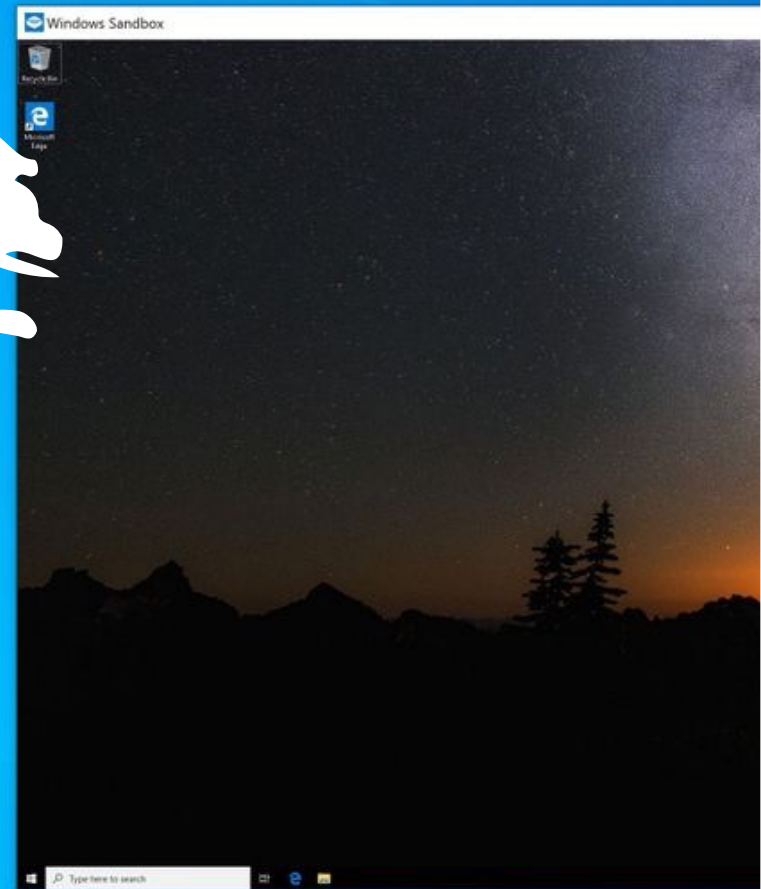
5 / Ochrana před uživatelem

- Zálohovat data!
- Používat koš
 - Správné nastavení maximální velikosti souborů v koši
- K práci nevyužívat administrátorský účet
- Sandbox



6 / Sandbox

- „Pískoviště“
- Izolované prostředí
 - Využívané ke spouštění neznámých a potenciálně nebezpečných aplikací
 - Nedojde k poškození vašeho počítače
- Chrání uživatele před sebou samým izolováním nebezpečných aplikací



6 / Sandbox

- Vytváří ohraničený prostor
 - Má omezený přístup ke zdrojům v hlavním OS
 - Nedochází k ukládání dat do hlavního OS

Pracovní list 5