Milyen protokollokat és megoldásokat akarunk használni a hálózatunkban? És mi kell hozzájuk?

Linux:

|  |  |
| --- | --- |
| **Protokoll / megoldás** | **Hogy és miként?** |
| Hálózat automatizáció | Python szerver futtatás (utána kell nézni) (LIN)  Ansible szerver futtatás  - VLAN-ok létrehozása, alkalmazása (MainHQ switchek)  - Port-security beállítása (MainHQ switchek)  - ADDS, (ADDS, RODC)  - ADDFS (ADDS, RODC)  - FSRM (ADDS, RODC)  - DHCP (ADDS) |
| LibreNMS | SNMP, Syslog (LIN)  - Hogyan lehet telepíteni? |
| OpenVPN | Egy sima VPN szerver, amire be lehet csatlakozni XY eszköznek (LIN)  - Egyszer összerakni, és kimenteni a config fileokat és a kulcsokat  - SSL/TLS |
| Apache2/Nginx webszerver | A pythonos hálózatautomatizáció futtatása (LIN)  - El kell dönteni, hogy melyik service  - Esetleg ADDS auth?  - SSL/TLS |
| Postfix/Dovecot | Email megoldások a szervezetnek (LIN)  - Konfig fileok kimentése  - ADDS user szinkron?  - SSL/TLS |
| Proxy | A Tűzfal mögötti szerveren (Proxy)  - Benti LIN nevű szerver szolgáltatásainak elérése |

Windows:

|  |  |
| --- | --- |
| **Protokoll / megoldás** | **Hogy és miként?** |
| ADDS, RODC, Sub domain | Megfelelő helyeken a megfelelő megoldások alkalmazása (összes)  - domain név: kkk.com (debrecen.kkk.com, szeged.kkk.com) |
| DNS | Magáért beszél (ADDS, RODC)  - Szerverek DNS elérésének beállítása  - PC-k regisztrálása DNS-be DHCP-vel  - Forwarder beállítása |
| ADDFS | Fileszerver, elosztott elrendezéssel, redundanciával (ADDS, RODC)  - Kapcsolat felépítése  - Replikáció |
| FSRM | Milyen és mennyi kerülhet hova fileoknál (ADDS, RODC)  - Kvóták megfogalmazása  - File screenek megfogalmazása |
| WDS | Kliensek automatikus telepítése (ADDS) |
| DHCP | - AD-ba regiszrálja a DNS rekordokat (ADDS) |
| Radius szerver | Hálózati eszközök bejelentkezése, és Wi-Fi hitelesítés, ha Enterprise-t akarunk (ADDS) |
| Group Policy | Automata alkalmazások telepítése, nyomtató megosztás, Jelszó erősség, asztal testreszabhatóságának korlátozása, háttér beállítása, hálózati meghajtó felcsatolása, fiók kizárása hibás bejelentkezésnél, vezérlőpult hozzáférés korlátozás |

Hálózat: (konfigurációk felküldése eszközönéként GitHub-ra)

|  |  |
| --- | --- |
| **Protokoll / megoldás** | **Hogy és miként?** |
| L2 (minden switchen) | |
| STP + Root Guard | L3-switcheknek kell lennie a Root-nak és ne mehessen le a L2-switchekhez ez a szerep  - BPDU + Portfast (Kliens portokon bekapcsolás) |
| LACP | Mindig a magasabb rétegbeli vagy a kisebb számú (ugyanabban a rétegben) a kezdeményező |
| Port-Security | - sticky  - 1 mac  - shutdown |
| DHCP Snooping + DAI | Csak a szerver felé megbízható minden más irányból nem megbízható |
| VLAN | Használt VLAN-ok:  - KIADO (csak MainHQ)  - ADMINISZTRACIO (csak MainHQ)  - HR (csak MainHQ)  - MARKETING  - PENZUGY  - ZENE  - IT  - SRV  - VEZETO  - WIFI  - MANAGEMENT  - NATIVE  - BLACKHOLE |
| L3, internetkapcsolat (MLS, Router, ASA, ISP, DualStack) | |
| HSRP (Tracking) | - Trackelni a felfele vezető kapcsolatot (sla-val) és játszani a prioritással  - authentikálni  - IPv4, IPv6 (ver2) |
| OSPFv2, OSPFv3 | - Authentikáció (v3 utánanézés)  - MultiArea  - EIGRP redistribute |
| EIGRP | - Authentikáció  - DMVPN-ek közti megosztás  - OSPF redistribute |
| BGP | - Peer az ISP-vel  - Prefix List?  - Authentikáció |
| ACL | - SSH-val csak LIN és rendszergazda érheti el a hálózati eszközöket  - Rendszergazda alhálóját semmi nem érheti el  - Wi-Fi-s alhálózat nem érhet el semmit a hálózaton belül, csak internetelérés |
| NAT | Proxy natolása |
| PAT | Minden más kipatolása a maradék címekre |
| PPPoE | - Utánanézni, hogy pontosan, hogy kell  - IR <-> ISP |
| DMVPN Phase 3 | - Site-to-Site VPN felépítése a branchek, és MainHQ között  - Titkos kulcsok a LIN szerveren lesznek legenerálva hozzá |
| **Protokoll / megoldás** | **Hogy és miként?** |
| Biztonság | |
| Hitelesítés |  |
| SSH |  |
| CDP, servicek letiltása | CDP, http(s) |
| WLAN biztonság | WPA2/3-Enterprise |
| Banner | „--------------------------------------------------  | Az [XY-eszköz] eszköz előtt ül éppen. |  | Kérem ne használja illetéktelenül az |  | eszközeinket! |  --------------------------------------------------” |
| Exec-timeout, jelszó próbálkozások száma | 5 perc  5 próbálkozás 10 perc |

Felhők (webshop):

|  |  |
| --- | --- |
| **Protokoll / megoldás** | **Hogy és miként?** |
| Adatbázis | Webshop termékek rekordjainak |
| FileServer | Képek tárolása termékekhez |
| Webszerver | Webshop hosztolása |