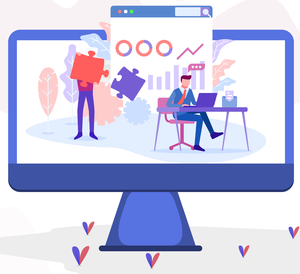
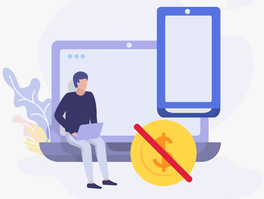
Rapid távmunka implementáció F5-tel

A helyzet gyors eszkalálódásával sok vállalkozás került lépéskényszerbe, hogy meg tudja oldani munkatársainak otthonról való munkavégzését.





Nem mindig és nem mindenhol megoldás a munkahelyi eszközpark bővítése (laptop vásárlás),

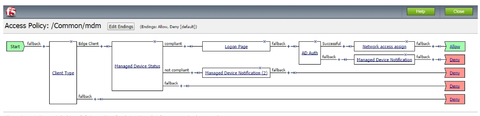
vagy a belső infrastruktúra/megoldások időigényes és korlátos átdolgozása/bővítése, mint pl.:

- **Terminal Server Farm:** erőforrás és időigényes, valamint nem minden alkalmazás futtatható ilyen környezetben
- **VPN:** otthoni gépek nem felelnek meg a VPN/belső security elvárásoknak, így nem lehet beléptetni őket a belső hálózatba

Gyorsan telepíthető, költségtakarékos és az adott igényekre szabható

Az F5 AAA megoldást kínál ügyfeleinek, amivel az otthonról dolgozó felhasználók otthoni eszközeikről (nem céges erőforrások) hozzáférhetnek a belső munkaállomásukhoz és azok minden lehetőségéhez, mintha bent volnának az irodában!

Az F5 APM modullal gyorsan és egyszerűen felépíthető a beléptetés módja és mélysége a jól használható és szemléletes Visual Policy Editorral:

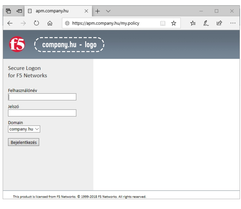


(Flowchart jelleggel építhető fel az ellenőrzési / döntési fa, Macro-k támogatása)

Kiszűrhetővé válnak a "veszélyes" eszközök

Igény esetén az F5 APM által végzett végpont vizsgálatokkal kiszűrhetők azok az otthoni eszközök, amelyek biztonsági szintje (vírusvédelem, tűzfal engedélyezése, stb.) nem vállalható a belső biztonsági protokollok szerint.

- Antivírus fut-e és kellően friss-e az adatbázisa (Windows / Mac / Linux)
- Tűzfal (Windows / Mac / Linux)
- Machine Certificate
- Workshift - munkaidő, munkaidőn kívül / hétvége
- IP Geolocation
- IP Reputation - Webroot BrightCloud service db
- Jailbrake-elt vagy Root-olt eszköz
- Landing URI
- Managed Endpoint - Airwatch / MaaS360 / Intune



Azonosítás, akár testre szabható beléptető oldalon

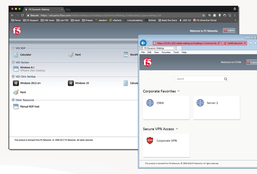
A felhasználó beléptetését és azonosítását szintén az F5 APM modulja végzi el, akár egy testreszabható beléptető oldalon keresztül, mielőtt a felhasználó hozzáférhetne a belső infrastruktúra bármely eleméhez.

- Logon Page - testre szabható, tetszőleges mezőkkel bővíthető
- Active Directory
- OAuth
- LocalDB
- One Time Password (SMS gateway-en keresztül kiküldhető)
- RADIUS, pl.: Cisco ISE, Cisco Duo Security, Azure MFA (on premise – Microsoft NPS / cloud), Okta MFA, OpenOTP
- Kerberos
- Client Certificate

Adatok megjelenítése egyedi feltételek alapján

A felhasználók által elérhető, a munkavégzésükhöz szükséges erőforrásokat hozzá tudjuk rendelni a folyamathoz. Ezeket egy webtop felületen tudjuk megjeleníteni a számukra. Minden felhasználó csak azokat az erőforrásokat látja, amelyekhez neki személyesen, vagy AD csoporttagsága alapján

- Webtop (landing page, amelyen megjelennek a felhasználó számára elérhető erőforrások)
- App Tunnel
- Remote Desktop - Citrix / VMware View / Microsoft RDP
- SNAT



Személyre szabott üzenetek

Ezen felül olyan személyre szabott üzeneteket, információkat tudunk megjeleníteni, ami segítheti a munkatársak otthoni munkavégzését, vagy az esetleges kapcsolódási problémák azonosítását (pl. nem rendelkezik a megfelelő csoporttagsággal, vagy nincs a felhasználói azonosítójához rendelt telefonszám).

Decision box / Message box

A végeredmény, hogy az akár **egy nap alatt telepíthető** megoldás implementációja után **munkatársaink az otthoni eszközeikről kapcsolódhatnak a benti munkaállomásukhoz**, mintha ott ülnének benn az irodában a gépük előtt. A munka nem marad elvégzetlenül, de a kollégák és családjaik **biztonságban lesznek**.

#maradjotthon

További információk:

Fejérváry-Gaál Balázs
Business Development Manager – F5
balazs.fejervary@alef.com
ALEF