VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

DELO OD DOMA IN NAČINI VPN POVEZAV DO PODJETIJ

Kandidat: Aljaž Cekić

Vrsta študija: študent izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Lektor: Erna Leš, prof. slov. jez.

Maribor, 2022

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Aljaž Cekić sem avtor diplomskega dela z naslovom »Delo od doma in načini VPN povezav do podjetij«, ki sem ga napisal pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, november 2022 Podpis študenta:

POVZETEK

Navidezna zasebna omrežja ali VPN omogočajo uporabniku varen prenos podatkov, ki potujejo skozi javni internet. Uporabnik je lahko posameznik ali podjetje, ki želi svoje podatke zaščititi na način, da se prepreči njihova seznanitev ali sprememba. VPN povezave se razlikujejo glede na to, ali je potrebno povezati dve ali več ločenih poslovnih lokacij (angl. site-to-site VPN), ustvariti povezavo med službenim računalnikom in podjetjem (ang. client-to-server VPN) ali pa ustvariti povezavo med napravo, ki jo ima v lasti posameznik, in podjetjem (angl. SSL VPN). VPN povezava ne zagotavlja zadostne varnostne zaščite. Za popolno zaščito podjetje potrebuje tudi požarni zid za zaščito omrežja in protivirusni program.

Požarni zid, s katerim upravlja IT oddelek, omogoča, da se nove zaposlene doda v omrežje, se jim dodeli pravice v okviru njihovega delovnega mesta in delovnih nalog ali pa se uporabnike izbriše iz sistema ob prenehanju delovnega razmerja. Prav tako je mogoče s požarnim zidom preverjati odhodni in dohodni promet, nastaviti politiko filtriranja, zaščititi strežnik e-pošte in sumljivo e-pošto prestaviti v karanteno, pregledovati zaznane nevarnosti v tekočem dnevu in ustvariti varnostno kopijo požarnega zidu.

Protivirusni program razširja funkcije požarnega zidu, saj lahko ta preverja datoteke pri dohodnem in odhodnem prometu ter pregleduje računalnik ali napravo podjetja, iz katere se pošiljajo podatki in kamor se podatki shranjujejo.

Kljub vsem varnostnim mehanizmom pa je pomembno, da podjetje svoje zaposlene redno izobražuje na področju varovanja informacij, skladnosti v zvezi s politiko poslovanja in vodenjem podjetja, s tem se prepreči varnostni incident (npr. zaposleni ob prejetju sumljive e-pošte obvesti nadrejenega ali IT oddelek).

Za obvladovanje tveganj imajo podjetja uveden standard ISO. Najnovejši ISO standard 31000 je z načeli in smernicami namenjen obvladovanju tveganj. Standard je primeren za katerokoli podjetje ne glede ne njegovo dejavnost ali velikost. Njegovi temelji so, da vsako podjetje ali organizacija obstaja z namenom doseganja ciljev, da na doseganje ciljev vplivajo notranji in zunanji dejavniki, kar povzroči negotovost pri doseganju ciljev.

Ključne besede: *VPN, požarni zid, protivirusni program, standard ISO, zaščita podatkov*

SUMMARY

Virtual private network or VPN allows the user to securely transfer data traveling through the public Internet. The user can be an individual or a company that wants to protect their data in a way that prevents their disclosure or modification. VPN connection differs depending on whether it is necessary to connect two or more separate business locations (site-to-site VPN), to create a connection between a work computer and a company (client-to-server VPN) or to create a connection between device owned by individual and a business (SSL VPN).

A VPN connection, however, does not provide sufficient security protection. For complete protection, the company also needs a firewall to protect the network and an antivirus program. The firewall managed by the IT department allows new employees to be added to the network, rights are assigned to them within the framework of their workplace and work tasks, or users are removed from the system upon termination of the employment. It is also possible to use the firewall to check outgoing and incoming traffic, set a filtering policy, protect the email server and quarantine suspicious emails, review the current day's detected threats and create a firewall backup.

An antivirus program extends the functionality of a firewall, it can check files for incoming and outgoing traffic and examine the company's computer or device from which data is sent and to which data is stored.

Despite all the security mechanisms, it is important that the company regularly educates its employees in the field of data protection, compliance with business policy and company management, thereby preventing a security incident (e.g., an employee notifies a superior or the IT department upon receiving a suspicious e-mail).

For risk management, companies have introduced the ISO standard. The latest ISO standard 31000 is aimed at risk management with principles and guidelines. The standard is suitable for any company, regardless of its policy or size. Its foundations are that every company or organization exists for the purpose of achieving goals, that the achievement of goals is influenced by internal and external factors, which causes uncertainty in achieving goals.

Key words: *VPN, firewall, antivirus, standard ISO, data protection*

KAZALO VSEBINE

KAZALO SLIK

1 UVOD

1.1 Opis področja in opredelitev problema

Varnost podatkov velja za pomemben korak pri prenosu podatkov od pošiljatelja do prejemnika še pred izumom računalnika. Do izuma računalnika je bilo dobro fizično varovanje podatkov zadosten ukrep. Z razvojem tehnologije (računalnikov in z izumom interneta) pa je postalo fizično varovanje podatkov le eden izmed ukrepov pri zagotavljanju varnosti. Vedno večji pomen se je začel pripisovati elektronski varnosti podatkov. Prenos ali pošiljanje podatkov preko javnega interneta ni varno, saj javni internet ni bil ustvarjen kot varno omrežje, ampak kot način prostega dostopa do podatkov. Podjetja se zavedajo, kako pomembni so podatki, ki jih shranjujejo v centraliziranih informacijskih sistemih, saj v večini vsebujejo informacije, ki so namenjene le zaposlenim v podjetju (npr. interni podatki) ali določenemu sektorju (npr. strogo zaupni podatki so na voljo le vodstvu podjetja). Razkritje takšnih podatkov bi podjetju povzročilo materialno škodo v obliki zmanjšanja ugleda podjetja, podjetje bi izgubilo konkurenčno prednost na trgu, stranke itd. Čeprav se je dela od doma in oddaljenega dostopa do podatkov do leta 2020 posluževalo manjše število zaposlenih v vseh podjetjih, je to od leta 2020 postalo pravilo in ne več izjema. Oddaljen dostop je omogočil, da lahko zaposleni kadarkoli in kjerkoli dostopajo podatkov s pomočjo različnih elektronskih naprav (računalnikov, tabličnih računalnikov in pametnih telefonov).

Večje kot je število vzpostavljenih povezav do centraliziranega informacijskega sistema, večje je tveganje, da se sistem okuži s škodljivo programsko opremo (npr. z vohunsko programsko opremo Pegasus), se prestrežejo informacije zaupne narave ali se zgodi vdor v informacijski sistem. Zaradi navedenega se podjetja ne želijo posluževati t.i. politike BYOD (angl. Bring Your Own Device), ki omogoča uporabniku, da se poveže v informacijski sistem z lastno elektronsko napravo, nad katero podjetje nima nadzora (uporabniku ne more npr. preprečiti namestitve vohunske programske opreme ali jo odstraniti).

Podjetja se zavarujejo pred nepooblaščenim dostopom do podatkov s pomočjo varovanega oddaljenega dostopa zaposlenih z uporabo navideznega zasebnega omrežja oz. VPN (angl. Virtual Private Network) in z dodelitvijo lastnih nadzorovanih elektronskih naprav (npr. lastnik oz. administrator lahko nadzoruje in spremlja mobilne naprave s pomočjo programske opreme, ki omogoča evidenco mobilnih naprav v podjetju, ki dostopajo do podatkov podjetja, mobilne naprave konfigurira v skladu s varnostno politiko podjetja, določi, katere aplikacije bo uporabljala določena skupina zaposlenih v podjetju, izbriše podatke podjetja v primeru izgube, kraje ali uničenja elektronske naprave, s kakšnimi uporabniškimi pravicami se bodo aplikacije izvajale,…).

1.2 Namen, cilji in osnovne trditve

Cilj diplomske naloge je ovreči ali potrditi naslednje hipoteze s pomočjo zgoraj navedenega programa Sophos UTM Home in s komercialno VPN povezavo ponudnika Surf Shark:

H1: Z ustrezno VPN tehnologijo dosegamo več kot 99,9% zaščite omrežja pred vdori v omrežje.

H2: Za vzpostavitev VPN povezave in omrežja ni potrebno dodatno poznavanje omrežja in njegove varnosti.

H3: Uporaba VPN povezave ne zahteva dobrega poznavanja VPN tehnologije.

H4: Vzpostavitev VPN povezave je zadosten ukrep pri varovanju zaupnih podatkov podjetja brez dodatnih varnostnih mehanizmov (požarni zidovi, protivirusni programi itd.).

H5: Vzpostavitev VPN povezave je cenejša rešitev v primerjavi s SD-WAN.

H6: Uporaba rešitev različnih ponudnikov storitev lahko privede do nezdružljivosti in tehničnih težav (večji stroški vzpostavitve VPN povezave).

H7: Prenosna hitrost je pri vzpostavljeni VPN povezavi počasnejša kot brez vzpostavljene VPN povezave.

H8: Obhodni čas (ping) se pri vzpostavljeni VPN povezavi podaljša v primerjavi, ko VPN povezava ni vzpostavljena.

1.3 Predpostavke in omejitve

Omejitev diplomskega dela se nanaša na praktični del diplomskega dela, saj zaradi označitve podatkov kot poslovna skrivnost organizacije ni bilo mogoče testirati VPN povezave na konkretnem primeru v podjetju, pregledati pravice in omejitve posameznikov, ki so zaposleni v različnih oddelkih in priložiti ustrezne dokumentacije.

1.4 Uporabljene raziskovalne metode

Raziskovalna metoda je kvantitativna, saj je v uvodu napovedano, kakšni so cilji raziskovanja in njihov opis. Na koncu so s testiranjem hipoteze potrjene ali ovržene.

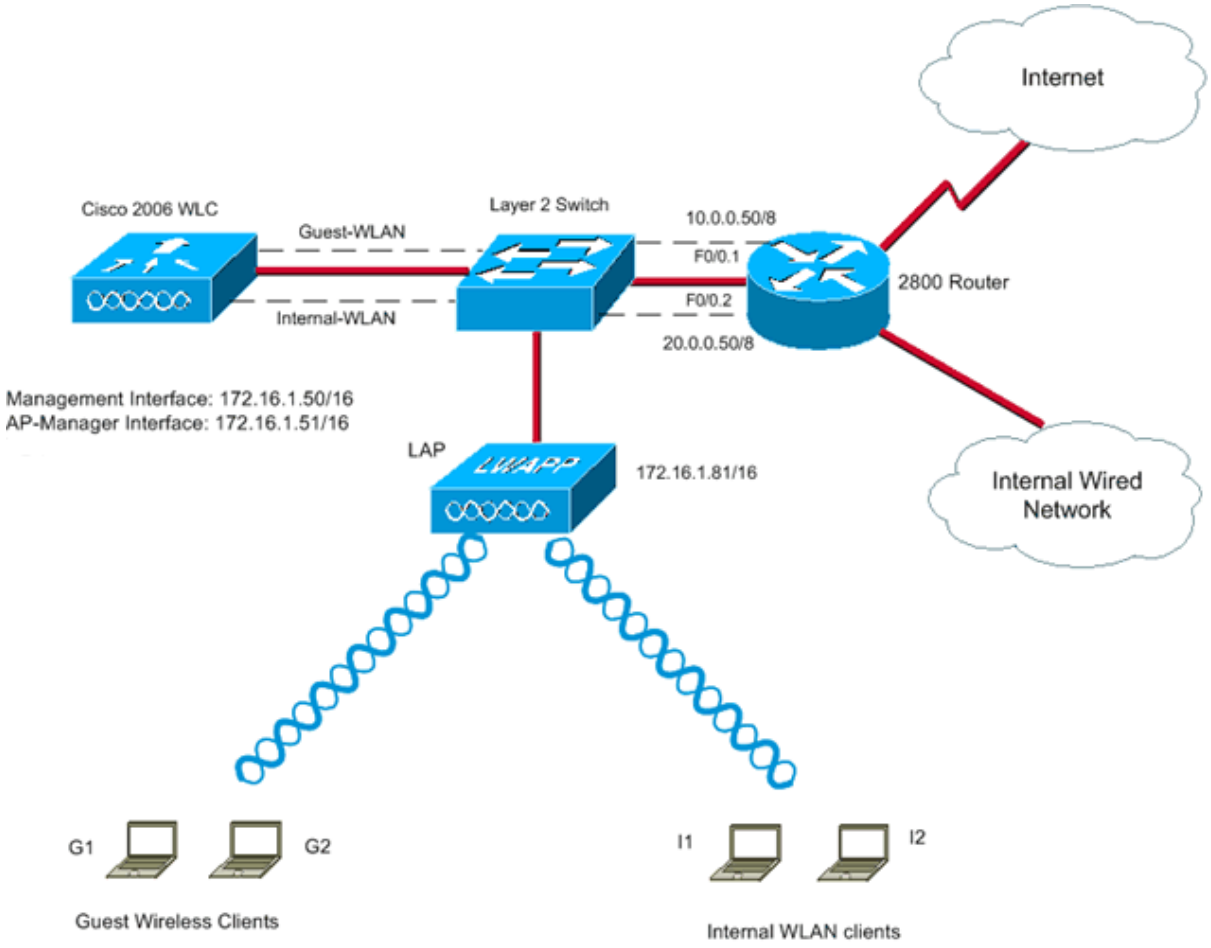
2 VARNOST PODATKOV V PODJETJU

Podjetja lahko ob prihodu delavcev na kraj podjetja ali podružnice varuje informacijsko varnost s svojo varnostno politiko, ki se deli na:

- fizično varovanje,
- varovanje podatkov in naprav,
- varovanje omrežja in
- varovanje in uporaba oblačnih storitev.

Pri zagotavljanju fizičnega varovanja delovnih območij se večja podjetja poslužujejo varovanja s pomočjo varnostne službe. Slednja uvede varnostne prepreke, s katerimi nepooblaščenim osebam onemogoči vstop do varovanih območij v podjetju. Prva takšna varnostna prepreka s strani varnostne službe je pogosto uvedba receptorja, ki vsakega obiskovalca (tako zunanjega kot tudi zaposlenega) vpiše v evidenco na podlagi osebnega dokumenta in povpraša o namenu obiska in s kom so dogovorjeni. Zagotavljanje varnosti v velikih podjetjih je veliko bolj kompleksno, kot le uvedba receptorja, zaradi tega se prostori, ki vsebujejo interne, zaupne in strogo zaupne podatke, varujejo tudi s karticami dostopa, s katerimi IT oddelek vsakemu posamezniku glede na njegovo delovno mesto dodeli dostope do različnih nivojev in oddelkov v podjetju, do katerih lahko zaposleni dostopa oz. se v njih prosto giblje. Hkrati se lahko uvede tudi dodatno varovalo, na podlagi katerega smejo zaposleni dostopati do varovanih območij (npr. serverski prostor) samo v določenem časovnem obdobju npr. med delovnim časom podjetja, za dostop po delovnem času pa potrebujejo zaposleni pooblastilo nadrejenega. Upravljanje, shramba in varovanje podatkov je naloga podjetja, ki omejuje dostope do prostorov z internimi, zaupnimi in strogo zaupnimi informacijami (npr. serverski prostori) s pravicami uporabnikov v obliki kartic dostopov in v obliki prijave v informacijski sistem (seja, ki jo zaposleni lahko uporablja med delom).

Podjetje varuje omrežje s tem, da tudi na napravah (zelo podobno kot pri karticah s pravicami dostopa do različnih območij v podjetju) dodeli IT oddelek različnim uporabnikom, različna upravičenja glede na nujnost in potrebe njihovega delovnega mesta (seja, ki jo zaposleni lahko uporablja med delom). Uporabnikom se dodeli uporabniško ime in geslo z različnimi pravicami, s katerim se vpišejo npr. na službeni računalnik. S tem se varuje dostop do LAN omrežja in drugih omrežnih nastavitev in preprečuje potencialna nevarnost vdora v omrežje. Preverjanje identitete uporabnika oz. pristnost uporabnika v omrežju, prikaz LAN omrežja v podjetju z usmerjevalniki in končna povezava na internet.je razložena s spodnjo shemo:



Slika 1: preverjanje identitete uporabnika v omrežju podjetja

(Cisco, 2009)

3 VARNOST PODATKOV PRI ODDALJENEM DOSTOPU

Ob spremembi lokacije opravljanja dela (delo od doma ali na terenu) zgolj fizično varovanje ne zadostuje in v tem primeru se podjetja poslužujejo zadnjih treh področij varnostne politike: varovanja podatkov in naprav, varovanja omrežja in varovanja in uporabe oblačnih storitev.

3.1 Požarni zid

Požarni zid je pomembna prepreka tako na domačih omrežjih kot tudi na omrežjih v podjetjih. Predstavlja eno izmed najosnovnejših zaščit na omrežju, ki ga podjetje ima in s katerim se varuje pred vdori. Požarni zid v obliki programske ali strojne opreme deluje kot prepreka med napravami v podjetju in internetom. Za dnevna opravila vsa podjetja uporabljajo internetno povezavo. S požarnim zidom se vhodni in izhodni promet filtrira, tako da je prepustnost požarnega zida odvisna od njegovih nastavitev oz. od želje podjetja, katere informacije naj pošilja in sprejema. Požarni zidovi se tako razčlenijo še na navadne in pametne požarne zidove. Navadni požarni zid služi kot osnovna zaščita in omogoča zaščito le do določene mere.

Podjetje, ki ima pameten požarni zid ponudnika Palo Alto, ki omogoča mnogo več:

- Definiranje in uveljavljanje učinkovitih pravilnikov za rabo aplikacij, ki temeljijo na aplikacijah, njihovih značilnostih, določenih skupinah ali uporabnikih in poskuse izkoriščanj ranljivih mest.
- Nadzor, ki temelji na aplikacijah in omogoča določanje pravilnikov aplikacij; ta kasneje omogoča skrbnikom vpogled v aplikacije, kategorije in podkategorije. Značilnosti aplikacij nam povedo možnosti prenašanj datotek za posamezno aplikacijo in ranljiva mesta ter potencialne možnosti izogibanja preverjanju ranljivosti in širjenja zlonamerne kode.
- Filtriranje URL omogoča skrbnikom uporabo natančno določenih pravilnikov za brskanje po spletu, ki dopolnjuje pravilnike za vpogled v aplikacije in nadzor nad njimi.
- Program »FlashMatch« nadgrajuje vpogled v aplikacije, ki generira identifikacijo aplikacij (App-ID) ter na ta način blokira viruse, vohunske programe, črve in ostalo zlonamerno programsko opremo. (Brglez, 2019)

3.2 Zaupanja vredna omrežja v podjetjih (Ekstranet)

Zaupanja vredna omrežja v podjetjih se izvajajo z t.i. Ekstranet. Ekstranet je skupek intranetov, ki so del infrastrukture interneta, vendar je dostop do njega onemogočen javnosti. Intraneti, ki sestavljajo ekstranet, so lahko geografsko oddaljeni. V večini primerov uporabljajo VPN tehnologijo. Zaposleni in podjetje pričakujejo od ekstraneta predvsem bistvo – varnost, ki jo omogočajo: požarni zidovi, VPN tuneli (virtualna privatna omrežja), šifriranje informacij, digitalni certifikati za identificiranje vseh uporabnikov in ustrezna strežniška politika.

3.3 Varovanje oblačnih storitev

Oblačne storitve kot način za shranjevanje podatkov postajajo vse bolj priljubljena storitev. Dostop do oblačnih storitev se varuje z enako prepreko kot varovanje omrežja – s pravicami uporabnikov, do katerih ima v podjetju dostop samo IT oddelek. Vsem ostalim zaposlenim so pravice zaradi varnostnih razlogov in potencialne nevarnosti razkritja podatkov onemogočene.

3.4 Urejen oddaljen dostop do podatkov podjetja

Podjetje, ki želi varovati svoje poslovne skrivnosti in podatke, ima vzpostavljeno VPN povezavo (npr. Sophos UTM), preko katere se uporabniki z omogočenimi pravicami s pomočjo prenosnih računalnikov ali mobilnih telefonov povežejo do internih, zaupnih in strogo zaupnih podatkov. To omogoča zaposlenim varno povezanost s podjetjem kjerkoli so. Promet je preko VPN povezave popolnoma šifriran. Varovanje prijave poteka z avtentikacijo z dvema avtentikacijskima elementoma.

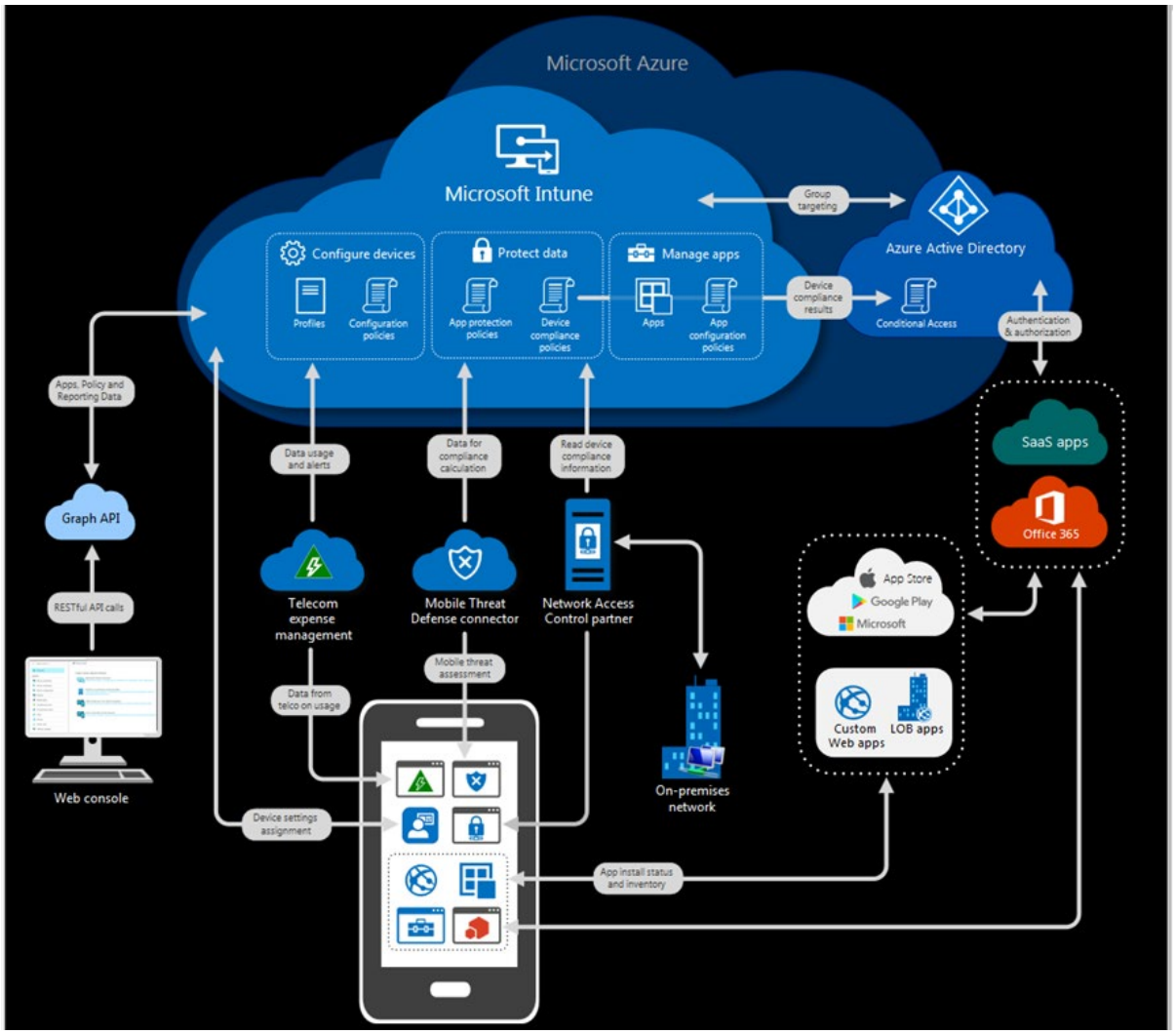
3.5 Nadzor mobilnih naprav v podjetju

Mobilni telefoni so postali del našega vsakdana in si življenja brez njih skoraj ne moremo predstavljati, saj nam služijo kot vir zabave (socialna omrežja, YouTube, videoigre…) kot tudi sredstvo za opravljanje službenih obveznosti (e-pošta, dostop do serverja,…), saj so manjši in zaradi tega priročnejši od računalnikov. S tehnološkim napredkom in razvojem boljših mobilnih naprav se je premo sorazmerno povečala tudi nevarnost vdora in kraje omenjenih podatkov.

Izguba podatkov ali njihovo nedovoljeno razkritje bi za večino ljudi pomenilo nepopravljivo škodo, še posebej, če so podatki zaupne narave tako na osebnem ali službenem področju (npr. delo v finančni instituciji). Varnost mobilne naprave je tako učinkovita, kot je njen najšibkejši člen, to je pa v večini primerov neozaveščen uporabnik, ki zaradi svojega neznanja ogrozi njeno varnost, npr. naloži domnevno varno aplikacijo iz neznanega vira, ta pa opravlja v ozadju zlonamerna dejanja, se poveže na javno brezžično omrežje in/ali uporablja nezaščitene certifikate. Zaposlene v podjetju se mora redno izobraževati na področju varovanja zaupnih informacij in skladnosti v zvezi s politiko poslovanja in vodenjem podjetja. Izobraževanja v večini potekajo preko e-poštnih sporočil, intraneta ali sestankov, kjer se zaposleni seznanijo z novimi smernicami in določili podjetja, hkrati pa se lahko s pisnim preizkusom znanja preverja njihovo znanje po izobraževanju. Izobraževanja organizira lastnik posameznih informacij. To je odgovorna oseba, ki glede na svoje področje oz. položaj v podjetju upravlja s podatki na tem področju.

V podjetju se nadzor in spremljanje naprav lahko izvaja z uporabo različnih programov in aplikacij (angl. MDM – mobile device management, MAM - mobile application management, MIM - Mobile information management in MEM Mobile E-mail Management), pogosto uporabljene so: Microsoft Intune, Azure Active in Sophos Mobile Control.

Microsoft Intune je oblačna storitev, ki omogoča varovanje podatkov podjetja med delom zaposlenih na mobilnih napravah. Z Azure Active Directory se kontrolira, kdo dostopa do podatkov in kakšne pravice dostopov ima posameznik, Azure Information Protection pa s povezavo aplikacije Office 365 skrbi za varnost datotek podjetja na mobilnih napravah zaposlenih. Prikaz delovanja programa Microsoft Intune je grafično predstavljen na spodnji sliki.



Slika 2: delovanje sistema Microsoft Intune in Azure

(Nomasis, 2022)

Z MDM lahko lastnik oz. administrator upravlja z mobilnimi napravami na naslednje načine:

- Vrši evidenco mobilnih naprav v podjetju, ki dostopajo do podatkov podjetja.
- Omogoči lažjo VPN ali Wi-Fi povezavo s pomočjo lastnih certifikatov.
- Vrši nadzor nad skladnostjo mobilnih naprav.
- Odstrani vse povezave do podatkov in dostopov podjetja ob uničenju, izgubi ali kraji mobilne naprave.

Z MAM se vrši nadzor nad aplikacijami:

- Določi, katere aplikacije bo uporabljala določena skupina zaposlenih v podjetju.
- S kakšnimi pravicami se bodo aplikacije zagnale (npr. prepoved kopiranja besedila v Microsoft Word dokumentu).
- Ima pregled nad naloženimi aplikacijami na mobilnih napravah in nadzoruje njihovo porabo.
- Lahko izbriše podatke podjetja iz aplikacij na mobilnih napravah.

Nadzor nad pretokom podatkov se vrši z MIM:

- Preprečuje se uhajane podatkov iz podjetja.
- Določa pravila za dostop do aplikacij.
- Mobilne naprave konfigurira v skladu s varnostno politiko podjetja (npr. posodobi mobilno napravo).

Elektronska pošta se na mobilnih napravah izvaja z MEM:

- Šifriranje elektronskih sporočil.
- Omejevanje pri odpiranju priponk glede na datotečno končnico.

Podatki se na mobilnih napravah v opisanem primeru delijo na službeni uporabniški račun in zasebni (privatni) uporabniški račun. Podatki so med seboj ločeni zaradi varnosti in zaradi različnega lastništva podatkov na napravi (službene podatke upravlja podjetje, zasebne pa uporabnik).

4 NAVIDEZNA ZASEBNA OMREŽJA – VPN

Navidezno zasebno omrežje (angl. virtual private network – VPN) je digitalno šifrirana povezava (t.i. tunel) skozi javni internet iz določene naprave na določeno omrežje[1]. Digitalno šifrirana povezava omogoča varen prenos podatkov in preprečuje nepooblaščenim osebam seznanitev s podatki ali spremembo podatkov, ki potujejo skozi javni internet. Na ta način lahko zaposleni opravljajo svoje delovne obveznosti izven pisarne in so hkrati varno povezani v omrežje podjetja.

Uporaba VPN povezave v poslovnem smislu temelji na povezavi oddaljenih poslovalnic oz. pisarn, mobilnih zaposlenih (npr. zaposleni na terenu) in zaposlenih pri delu od doma. Vsi izmed naštetih potrebujejo dostop do lokalnega omrežja podjetja, da lahko opravljajo svoje delo. Pri izmenjavi podatkov je zelo pomembna varnost in enostavnost vzpostavitve VPN povezave uporabnika.

Pri večjih podjetjih, ki imajo več podružnic oz. dislociranih enot, se lahko z VPN povezavami združijo lokalna omrežja dislociranih enot (razširitev intranetnega omrežja). Če podjetje posluje z drugimi organizacijami, npr. zaradi izvajanja različnih poslovnih procesov, se lahko lokalno omrežje podjetja deli z omrežji partnerjev podjetja. Takšen pristop olajša in avtomatizira delovne procese.

Podjetja se odločajo za VPN povezave, ker so stroškovno cenejša alternativa kot npr. uporaba prostranega WAN (angl. Wide Area Network) omrežja, pri katerem bi morali oddaljene enote med seboj fizično povezati z različnimi tehnologijami (stroški povezave se večajo z večjo oddaljenostjo posameznih enot): ISDN (angl. Integrated Servicer over Digital Network), ADSL (Asymmetric Digital Subscriber Line), PSTN (Public Switched Telephone Network), PSPDN (Packed Switched Public Data Network) ali z OC3 (Optical Carrier-3)[2]. Za WAN lahko podjetje tudi najame obstoječe linije za prenos podatkov, vendar je tukaj lahko ogrožena varnost podatkov.

[1] VPN povezava uporablja javni internet, vendar poteka ločeno od internetnega prometa.

[2] Primerjava različnih hitrosti med različnimi tehnologijami: ISDN hitrost do 144 Kbps, ADSL hitrost do do 6 Mb/s, PTSN hitrost do 56 kb/s in OC3 hitrost do 155 Mbps.

Po drugi strani je delovanje VPN povezave enostavno, saj omrežje, ki ga varuje požarni zid, deluje običajno (ni pomembna oblika omrežja in koliko računalnikov ga sestavlja), komunikacija poteka s pomočjo internetna po navadni poti, ampak do druge lokacije. VPN in požarni zid predstavljata nedeljivo celoto, saj požarni zid na prvi stopnji varuje omrežje pred zunanjimi napadi in hkrati omrežne VPN pakete popolnoma prepušča, na drugi stopnji pa VPN nadzoruje in preprečuje spremembo vsebine omrežnega paketa ter popolnoma prikrije izpostavljenost podatkov nepooblaščenim osebam. VPN omogoča podjetjem večjo fleksibilnost, saj se lahko s spremembo VPN naprave in s spremembo nastavitev realizira povezava z novo lokacijo ali pa se nekaterim uporabnikom onemogoči dostop do privatnega omrežja.

Fleksibilnost VPN povezave se izraža tudi v tem, ker izpad dela interneta hkrati popolnoma ne prekine sistema in VPN povezave, omrežni paketi se bodo v tem primeru preusmerili na drugo pot. Težava, ki se lahko pojavi je, da se povezava iz določene lokacije na internet prekine ali da se pripeti neprepustnost povezave (uporabnik nima garancije za prepustnost povezave), kar zahteva dodatno previdnosti pri vzpostavitvi VPN povezave.

4.1 TIPI VPN POVEZAV

- **Povezava omrežja v omrežje VPN (angl. site-to-site VPN):** omogoča povezavo dveh ali več ločenih poslovnih lokacij (vsaka izmed poslovnih lokacij je s svojim LAN omrežjem povezana v WAN omrežje) in povezavo med dvema ločenima intranetoma, med katerimi si lahko uporabniki pošiljajo podatke, ne da imajo uporabniki prvega intraneta dostop do drugega intraneta in obratno.

  (Cisco, 2008)

- **Povezava odjemalec-server VPN (angl. client-to-server VPN):** zaposleni se lahko povežejo iz svojega domačega računalnika v omrežje podjetja s šifrirano povezavo ob predpostavki, da je VPN naložen in konfiguriran na njihovem računalniku. S takšno povezavo uporabnik ni povezan na internet preko svojega ponudnika internetnih storitev, ampak vzpostavi neposredno povezavo s pomočjo VPN. Ta način VPN povezave prepreči tretjim osebam, da bi dostopale do povezave in šifrira povezavo vse do ponudnika internetnih storitev (hkrati prepreči tudi ponudniku internetnih storitev, da bi ta dostopal do podatkov, ki bi lahko ostali nešifrirani in obide omejitve, ki bi jih uporabnik lahko imel zaradi državne zakonodaje).

- **SSL VPN (angl. Secure Sockets Layer):** ta vrsta VPN povezave je doživela svoj razcvet na začetku leta 2020, ko se je večina podjetij soočala s pomanjkanjem službenih prenosnih računalnikov, ki bi jih lahko zagotovili svojim zaposlenim za delo od doma. SSL VPN povezava poteka na obstoječem fizičnem omrežju in je sestavljena iz ene oz. več naprav VPN, te pa povezujejo svoje uporabnike na podlagi vgrajenih spletnih brskalnikov (običajno so to brskalniki, ki podpirajo HTML5).
    - **SSL VPN (portal):** omogoča enotno SSL povezavo (enoten SSL standard) do spletne strani, preko katere lahko uporabnik dostopa do različnih storitev, ki jih zasebno omrežje ponuja. Portal pomeni povezavo iz spletne strani do drugih virov. Uporabnik za takšno povezavo potrebuje sodoben brskalnik, opraviti mora identifikacijo in vnesti geslo za dostop do SSL VPN prehoda.
    - **SSL VPN (tunel):** je alternativna verzija SSL VPN, ki omogoča spletnemu brskalniku zaščiten dostop do mnogih omrežnih storitev, tudi če te niso del spleta s pomočjo tunela, ki deluje na podlagi SSL. SSL tunel zahteva brskalnik, s katerim je sposoben komunicirati in na podlagi katerega bo prikazoval aktivno vsebino (npr. JavaScript, Flash, ActiveX aplikacije ali vtičniki). S tem se povečuje funkcionalnost kot pri klasičnem SSL Portal VPN.

- **IPsec VPN:** IPsec protokol med dvema točkama poteka na omrežni plasti OSI modela in potrebuje določeno strojno opremo, da lahko deluje. Upravljanje tega protokola poteka skozi omrežno kodo operacijskega sistema in ne skozi programsko aplikacijo, kot je to pri SSL VPN. Zaradi potrebe po strojni opremi to otežuje napadalcem, da bi lahko izvršili uspešen napad na omrežje. Strojna oprema in z njo povezana programska oprema povečujeta začetne stroške pri vzpostavitvi takšne VPN povezave in predstavljata dodatno delo za IT oddelek v podjetju, ki skrbi za pridobitev licenc in posodabljanje programske opreme.

  (Barracuda, 2022)

4.2 SESTAVA VPN POVEZAVE

VPN uporablja več različnih metod, s katerimi se zagotavlja varna povezava:

- Zaupnost podatkov: zaupnost podatkov je bistvo, zakaj se ljudje odločajo za VPN povezave. Prenos ali pošiljanje podatkov preko javnega interneta ni varno, saj javni internet ni bil ustvarjen kot varno omrežje, ampak kot način prostega dostopa do podatkov. Zaupnost podatkov dosežemo z digitalnim šifriranjem, ki ga lahko dešifrira le točno določen uporabnik. Zaupnost podatkov se doseže v večini primerov VPN povezav z naslednjimi protokoli: IPsec (56-bitno ali 168 bitno šifriranje), PPTP/MPPE (40-bitno in 128-bitno šifriranje) in L2TP/IPsec (128-bitno ali 256-bitno šifriranje).
- Celovitost podatkov: preverjanje, da se podatki med prenosom niso spremenili oz. v primeru VPN: da se šifriran del paketa ali glava z informacijami nista spremenila. Ob spremembi se paket oz. datagram[3] ne prenese.
- Overjanje izvora podatkov: korak, s katerim se ugotovi, kdo je poslal podatek oz. podatke, kar varuje prejemnika pred napadom, ki bi spremenil identiteto pošiljatelja.
- Preprečevanje ponovitev komunikacije: ponovitev komunikacije je dogodek, s katerim tretja oseba prisluškuje komunikaciji med pošiljateljem in prejemnikom in lahko v vmesnem koraku (preden prejemnik prejme sporočilo) prestreže sporočilo, ga zadrži, prebere njegovo vsebino ali jo spremeni in ga pošlje naprej do prejemnika. To se lahko prepreči na način, da se za vsako izmenjavo podatkov uporabi enkratno geslo, ki velja le za to izmenjavo in se ne more ponovno uporabiti (angl. OTP ali one-time password).

[3] Paket ali datagram je neodvisno, samostojno sporočilo, ki je poslano preko interneta, katerega prihod, čas prihoda in vsebina nista zajamčena. (Oracle, 2022)

- Tuneliranje podatkov: s procesom tuneliranja podatkov se paket oz. datagram, ki ga želi pošiljatelj poslati, vstavi v nov paket (t.i. enkapsulacija) in se ga pošlje preko interneta. S tem procesom se doseže anonimnost naprave, iz katere izvira promet, kam potuje, dolžina sporočila ali frekvenca komuniciranja. Pomembno je razumeti, da samo tuneliranje ne zagotavlja varnosti podatkov, ker je primarni paket z enkapsulacijo mogoče s pomočjo naprav za lovljenje paketov (angl. packet-capture device) prestreči in prebrati. Če želimo doseči omenjeno varnost, potrebuje tuneliranje tri različne protokole:
    - Nosilni protokol: nosilni protokol ima funkcijo usmerjanja paketov od pošiljatelja do naslovnika po omrežju z enkapsulacijo. Usmerjanje paketov preko interneta poteka z uporabo protokola IP.
    - Protokol za enkapsulacijo: s tem protokolom se doseže enkapsulacija primarnega paketa, ustvarjanje, vzdrževanje in zapiranje tunela (protokoli GRE, IPsec, L2F, PPTP in L2TP).
    - Transportni protokol: protokol, ki ga uporablja omrežje, preko katerega potujejo informacije (protokola SLIP in PPP).
- AAO (avtentikacija, avtorizacija in odgovornost): AAO ali AAA (angl. Authentication, authorization, and accounting) ugotavlja, kdo je oseba, ki opravlja komunikacijo (avtentikacija, ki se opravi z vpisom uporabniškega imena in gesla), kakšna dovoljenja ima ta oseba (avtorizacija) in kaj ta oseba počne (odgovornost, ki je potrebna zaradi revizijske sledi v podjetju).
- Preprečevanje tajenja: s to metodo se zagotovi, da udeleženi osebi pri prenosu podatkov ne moreta trditi, da podatkov nista poslali ali da podatkov nista prejeli (to se doseže npr. z uporabo metode kot je tehnika podpisa).

  (Menezes, Oorschot, & Vanstone, 2001)

5 ŠIFRIRANJE PODATKOV IN ZGOŠČEVALNE FUNKCIJE

5.1 Šifriranje podatkov

Šifriranje oz. zakrivanje sporočil (kriptografija) se izvaja po postopku (algoritmu), s pomočjo katerega osnovno sporočilo, ki ga imenujemo tudi čistopis (angl. plaintext), spremenimo v šifropis (angl. ciphertext). V algoritmu se uporabijo določene vrednosti za parametre, ki se imenujejo ključ. Pošiljatelj in prejemnik sporočila se morata dogovoriti o algoritmu in ključu, če si želita pošiljati šifrirana sporočila (daljši kot je ključ težje ga je dešifrirati).

Simetrično šifriranje podatkov temelji na simetričnih šifrirnih algoritmih, pri katerem sta ključ za šifriranje podatkov in ključ za dešifriranje podatkov enaka. Prednost takšnega ključa je v preprostosti šifriranja in dešifriranja podatkov (še posebej pri šifriranju velikih količin podatkov je simetrično šifriranje hitrejše), težava nastane v njegovi izmenjavi, ki ne sme potekati preko nezaščitene povezave in v številu ključev, saj mora vsak uporabnik imeti svoj ključ za vsakega dopisovalca posebej. Primeri simetričnih šifrirnih algoritmov so: AES (angl. Advanced Encryption Standard, DES (angl. Data Encryption Standard) algoritem, RC2 (vgrajen v e-pošto) RC4 (vgrajen v brskalnike) RC5, IDEA. MARS, Blowfish in Serpent.

Asimetrično šifriranje podatkov se je razvilo prvič leta 1975 kot t.i. The Diffie-Hellman key agreement protocol zaradi težav pri simetričnem šifriranju in temelji na šifriranju z javnim-zasebnim ključem (tak koncept sta razvila Whitfield Diffie in Martin Hellman). Uporabnik pri asimetričnem šifriranju ustvari dva ključa, ki sta med seboj povezana in enega izmed njiju objavi (javni ključ). Vsak pošiljatelj sporočila bo uporabil javni ključ za šifriranje sporočila, ampak le omenjen uporabnik oz. prejemnik sporočila bo lahko sporočilo dešifriral s svojim zasebnim ključem. Prednost asimetričnih algoritmov pred simetričnimi je v zaščiti pri izmenjavi skupnih ključev. Njihova uporaba je na področju digitalnega podpisovanja. Danes se v večini pri asimetričnem šifriranju uporablja algoritem RSA, ki je bil razvit leta 1977 na univerzi MIT. (Thomas, 2000)

Poznamo pa tudi algoritme ECC (angl. Elliptic Curve Cryptosystems), ki temeljijo na eliptičnih krivuljah. Pri ECC zadoščajo krajši ključi kot pri RSA, zato se jih uporablja v manj zmogljivih napravah (za isto stopnjo varnosti dolžine ključa RSA v velikosti 512 bitov zadošča dolžina ključa ECC v velikosti 106 bitov).

Tako kot pri varni povezavi tudi tukaj ni dovolj, da se šifrirano sporočilo pošlje po javnih vodih, saj lahko npr. tretja oseba sporočilo spremeni ali pa se začne nekdo drug izdajati za izdajatelja javnega ključa z namenom seznanitve s sporočili. Zaradi tega so tudi tukaj pomembni: zaupnost, celovitost, overjanje izvora, preprečevanje ponovitev komunikacije in preprečevanje tajenja.

(Schneier, 1996)

5.2 Zgoščevalne funkcije

Zgoščevalne funkcije tvorijo skupaj s šifriranjem podatkov celoto. Zgoščevalne funkcije omogočajo spremembo poljubno dolgega teksta v število fiksne dolžine (število je izraženo v bitih). V praksi se zgoščevalne funkcije uporabljajo pri digitalnih podpisih, saj se tam izračuna z zgoščevalno funkcijo t.i. »fiksni povzetek« sporočila, ki je zašifriran z zasebnim ključem. Prejemnik potem z javnim ključem dešifrira podpis in izračuna prej omenjeni fiksni povzetek ter ga primerja s tistim v podpisu.

Najbolj znani zgoščevalni funkciji sta MD5 in SHA.

6 OBVLADOVANJE TVEGANJ S POMOČJO ISO STANDARDA 31000

Podjetja imajo za obvladovanje tveganj uveden standard ISO. Najnovejši standard ISO je ISO 31000.

Mednarodna organizacija za standardizacijo angl. International Organization for Standardization (ISO) je mednarodno telo, ki določa industrijske, lastniške in komercialne standarde po svetu.

Standard ISO 31000 je osnovni standard, ki je z načeli in smernicami namenjen obvladovanju tveganj. Standard je primeren za katerokoli podjetje ne glede ne njegovo dejavnost ali velikost. Njegovi temelji so, da vsako podjetje ali organizacija obstaja z namenom doseganja ciljev, da na doseganje ciljev vplivajo notranji in zunanji dejavniki, kar povzroči negotovost pri doseganju ciljev in posledično je zaradi negotovosti s tem povezano tudi tveganje. Posebej ISO standard obravnava tri pojme: načela, okvir in proces.

6.1 Načela

Delijo se na:

- **Načelo integracije** (obvladovanje tveganj je del celotne organizacije in vseh njenih aktivnosti).
- **Načelo strukture in popolnosti** (za konsistentne in primerljive rezultate je potrebno obvladovati tveganja s strukturiranim in popolnim pristopom).
- **Načelo prilagojenosti** (pojma okvirja in procesa sta prilagojena vsaki organizaciji glede na njihove cilje in organizacijo).
- **Načelo vseobsežnosti** (obvladovanje tveganj je možno s vključevanjem interesnih skupin v podjetju, saj s svojimi pogledi in znanjem prispevajo k obvladovanju).
- **Načelo dinamičnosti** (ne glede na spremembo strukture organizacije, ki je lahko tako zunanja kot notranja in se na podlagi tega tveganja spremenijo, jih je potrebno predvideti, odkriti in se na njih odzvati).

- **Načelo najboljše informiranosti** (vsako negotovost in nejasnost na podlagi preteklih, sedanjih in prihodnjih pričakovanih informacij je potrebno vzeti v obzir pri obvladovanju tveganj).
- **Načelo človeškega in kulturnega faktorja** (na vseh področjih obvladovanja tveganj je prisoten človeški in kulturni faktor).
- **Načelo nenehnega izboljševanja** (na podlagi preteklih, sedanjih in prihodnjih pričakovanih informacij se obvladovanje tveganj izboljšuje).

  (ISO, 2018)

6.2 Okvir in proces

V okvirju je opisano, kako razumeti poslovanje podjetja in njegovega okolja, kako določiti odgovornosti in pristojnosti, kako vzpostaviti politiko upravljanja tveganj, kako po načelu integracije obvladovanje tveganj vključiti v vse organizacijske procese in kako vzpostaviti način zunanjega in notranjega poročanja.

V procesu je predstavljena analiza parametrov zunanjih in notranjih dejavnikov, ki lahko ali ki vplivajo na doseganje ciljev, vključuje opis zunanjih in notranjih interesnih skupin, njihovo podrobno analizo in določa cilje za obvladovanje tveganj.

(Stanič, Blanc, & Sambolec, 2012)

7 PRAKTIČNI DEL

V praktičnem delu bom uporabil požarni zid naslednje generacije Sophos SG UTM 9, ki ga uporabljajo poslovni uporabniki v poslovnem okolju.

Požarni zid Sophos UTM je individualno prilagodljiv za različne uporabnike, njim se dodelijo različne pravice in različni dostopi iz enega centra, imenovanega Web Admin. Zaposleni se za vzpostavitev VPN povezave poveže preko separatnega portala, imenovanega User Portal. V nadaljevanju je seznam vseh funkcij požarnega zidu in pod vsakim podpoglavjem tudi opis možnosti.

Funkcije, ki jih požarni zid ponuja so:

- Dashboard,
- Management,
- Definitions & Users,
- Interfaces & Routing,
- Network Services,
- Network Protection,
- Web Protection,
- Email Protection,
- Advanced Protection,
- Endpoint Protection,
- Wireless Protection,
- Webserver Protection,
- RED Management,
- Site-to-site VPN,
- Remote Access,
- Logging & Reporting,
- Support.

7.1 Dashboard

Dashboard predstavlja grafični prikaz trenutnega delovanja požarnega zidu:

- General Information (prikazani podatki o imenu gostitelja, modelu, licenci in času delovanja).
- Version Information (podatki o strojni opremi in podatki o razpoložljivih posodobitvah).
- Resource Usage (prikaz v odstotku koliko procesorja, RAM, trdega diska in UPS je v uporabi).
- Today's Threat Status (zaznane nevarnosti v tekočem dnevu: virusi, nezaželena sporočila, blokirani napadi na server, vohunska programska oprema itd.).
- Interfaces (status in poimenovanje vmesniških kartic in posodobljen prikaz za prihodni in odhodni promet omrežja).
- Advanced Threat Protection (prikaz števila okuženih gostiteljev, pri katerih se opozorilo izbriše po 72 urah).
- Current System Configuration (prikaz omogočenih in onemogočenih varnostnih funkcij kot so: požarni zid, STMP strežnik, POP3 strežnik, VPN povezava site-to-site, oddaljen dostop, RED, Sophos UTM upravljalec, Sophos nadzor mobilnih naprav, brezžična varnost, pregled omrežja, protivirusna zaščita, zaščita proti nezaželeni pošti in zaščita proti vohunski programski opremi).

7.2 Management

Management funkcija se deli na:

- System Settings (uporabnik oz. skrbnik lahko v tej funkciji upravlja ime gostitelja, datum in čas, ime organizacije, mesto, državo in skrbnikovo e-pošto, pregleda nastavitve, ponastavi konfiguracijo in gesla).
- WebAdmin Settings (nastavitev jezika v modulu WebAdmin in osnovnih nastavitev, kot so dovoljeni administratorji, dovoljena omrežja, dnevnik vstopnega prometa, TCP vrata, HTTPS certifikate in uporabniške nastavitve).
- Licensing (namestitev licence in pregled aktivnih IP naslovov).
- Up2Date (pregled posodobitev strojne opreme in posodobitev vzorcev, s katerimi se posodablja protivirusna zaščita, zaščita proti nezaželeni pošti in zaščita proti vohunski programski opremi).
- Backup/Restore (shranjevanje nastavitev Sophos UTM v datoteko na trdem disku, saj se s tem lahko ponastavi sistem, ki ne deluje ali ima težave na prejšnjo delujočo različico. Varnostne kopije lahko uporabnik oz. skrbnik napravi ročno ali pa za to poskrbi sistem s samodejnimi varnostnimi kopijami).
- User Portal (v tej spletni aplikaciji se nahajajo e-poštna sporočila v karanteni, nezaželena sporočila, seznam dovoljenih pošiljateljev in blokiranih pošiljateljev, avtentikacija uporabnika, oddaljen dostop, HTML5 VPN portal, sprememba gesla, enkratno geslo oz. OTP in HTTPS strežnik).
- Notifications (je namenjen obvestilom uporabnika oz. skrbnika omrežja glede dogodkov, ki se nanašajo na nevarnost. Obvestila so lahko različna in vključujejo napake, opozorila in informacije).
- Customization (s to funkcijo je možno urejati in lokalizirati e-poštna obvestila in jih s tem prilagoditi politiki podjetja).
- SNMP (SNMP je okrajšava za angl. Simple Network Management Protocol. S tem se spremlja stanje naprav, ki so povezane na omrežje, kot so to routerji, serverji in usmerjevalniki).

- Central Management (namenjen prilagoditvi vmesnika orodij za upravljanje).
- Sophos Mobile Control (omogoča skrbniku, da na mobilnih napravah in tabličnih računalnikih upravlja, nadzoruje, posodablja, locira naprave, zavaruje zaupne informacije podjetja ne glede na operacijski sistem, ki je lahko iOS, Android ali Windows Phone).
- High Availability (funkcija omogoča nadaljnje izvajanje storitev tudi ob napaki na strojni opremi).
- Shutdown/Restart (ročni zagon ali ustavitev Sophos UTM).

7.3 Definitions & Users

Funkcijo sestavljajo:

- Networks and Definitions (namenjeno ustvarjanju omrežja, omrežnih skupin, kdo so osebe, ki se v omrežje povezujejo in določitev MAC naslovov).
- Service Definitions (tip prometa, ki je sprejet oz. zavrnjen, TCP in UDP protokoli in številke vrat).
- Time Period Definitions (ustvarjanje ponavljajočih dogodkov ali osamljenih dogodkov, s katerimi lahko avtomatiziramo proces).
- Users & Groups (VPN povezava za oddaljen dostop, uporaba e-pošte in ustvarjanje uporabnikov ter skupin za spletno aplikacijo WebAdmin).
- Client Authentication (avtentikacija uporabnikov za vstop v Sophos UTM z dodeljenimi pravicami pri uporabi omrežja).
- AWS Profiles (dodeljena možnost komunikacije z oblačnimi storitvami, kot so to Amazon CloudWatch, Amazon Virtual Private Cloud itd.).
- Authentication Services (preverjanje in potrditev uporabnikov, ki se želijo povezati v omrežje z zbirko podatkov o uporabnikih).

7.4 Interfaces & Routing

Pomožne funkcije so:

- Interfaces (upravljanje mrežnih kartic, kot je njihovo ime, naslov in strojna oprema).
- Quality of Service (nadzor nad mehanizmi z namenom zagotavljanja pasovne širine točno določenemu omrežnemu prometu).
- Uplink Monitoring (spremljanje povezave in določitev dejanj ob spremembi povezave).
- IPv6 (zaradi nadgradnje IPv4 v IPv6 je možnost prilagoditi Sophos UTM na IPv6).
- Static Routing (s static routing je možno natančno določiti pot, po kateri potujejo mrežni paketi do naslovnika).
- Dynamic Routing (z drugimi besedami tudi OSPF angl. Open Shortest Path First je hierarhični protokol, ki se uporablja v večjih avtonomnih sistemskih omrežjih).
- Border Gateway Protocol (protokol, ki ga uporabljajo v večini ponudniki internetnih storitev za komunikacijo z drugimi ponudniki internetnih storitev).
- Multicast Routing (tehnika, s katero več prejemnikov prejme omrežne pakete z nizko uporabo omrežnega prometa).

7.5 Network Services

Vključuje možnosti nastavitve omrežja preko DNS, DHCP in NTP:

- Pri DNS se določi omrežja, ki bodo uporabljala požarni zid kot DNS resolver.
- DHCP (avtomatično določi naslove iz definiranega t.i. IP pool priključenim računalnikom za poenostavitev omrežnih nastavitev v velikih podjetjih, ki imajo velika omrežja).
- NTP (omogoča nastavitev NTP serverja na povezanih omrežjih z NTP protokolom).

7.6 Network Protection

Funkcija omogoča varovanje omrežja na način, da lahko določimo parametre za:

- Firewall (omogoča nastavitev protokolov in pravil za požarni zid).
- NAT (omogoča nastavitev protokolov in pravil za NAT).
- Intrusion Prevention (namenjen zaznavanju napadov na omrežje z določitvijo IPS pravil).
- Server Load Balancing (distribucija prihodnega prometa SMTP ali HTTP na več serverjev za njihovimi vrati angl. gateway).
- VoIP (namenjen pošiljanju zvočnih sporočil po omrežju).
- Advanced Settings (določitev dodatnih nastavitev, kot so generični proxy, SOCKS proxy in IDENT reverse proxy).

7.7 Web Protection

Možnost zaščite pri brskanju po spletu se deli na:

- Web Filtering (možnost preverjanja odhodnega in dohodnega prometa s protivirusnim programom, kar preprečuje vohunsko programsko opremo in blokira škodljive spletne strani in hkrati nastavitev filtriranja, da na določene spletne strani v določenih kategorijah zaposleni ne morejo dostopati npr. igre na srečo).
- Web Filtering Profiles (namenjen ustvarjanju različnih profilov filtriranja za različna omrežja v podjetju, s tem se lahko določeni skupini ljudi v podjetju omeji dostop do interneta do določenih kategorij. To se doseže s prijavo v sistem, na podlagi katere se določijo pravice uporabniku).
- Filtering Options (konfiguracija izjem od pravil filtriranja).
- Policy Test (testiranje URL ali ustrezajo pravilom filtriranja).
- Application Control (ta funkcija omogoča uporabniku, da oblikuje in blokira omrežni promet glede na vrsto prometa, vendar na drugačen način kot prej omenjeni Web Filtering. Pri Application Control se omrežni promet ne preverja le po protokolu ali URL, ampak s pomočjo klasifikacije omrežnega prometa).

- FTP (omogoča nastavitev FTP proxy oz. FTP protokola, ki se uporablja za izmenjavo datotek po spletu. S tem se lahko blokirajo določeni tipi datotek, ki bi bili preneseni s pomočjo FTP protokola).

7.8 Email Protection

E-pošto je možno zaščititi na naslednje načine:

- SMTP (SMTP angl. Simple Mail Transfer Protocol se uporablja za prenos e-pošte na strežnik in v opciji SMTP v Sophos UTM lahko skrbnik zaščiti notranji server za e-pošto pred zlonamerno programsko opremo).
- POP3 (konfiguracija POP3 protokola angl. Post Office Protocol 3, ki se uporablja za dohodno e-pošto. V tej konfiguraciji je priporočljivo nastaviti časovno omejitev strežnika na več kot 1 minuto za pridobivanje večje dohodne e-pošte).
- Encryption (šifriranje e-pošte je asimetrično v Sophos UTM).
- SPX Encryption (šifriranje, ki nešifrirana e-poštna sporočila in priponke spremeni v PDF dokument ter jih zaklene z geslom).
- Quarantine Report (karantena, v katero se preusmerijo sumljiva e-poštna sporočila, ki so lahko: nezaželena e-pošta, vsebujejo sumljive priponke, so okužena z virusom ali vsebujejo nezaželeno izrazoslovje).
- Mail Manager (namenjen organizaciji e-pošte, preden ta prispe do prejemnika, da se lahko že v tej fazi izbriše, sprosti ali preusmeri v karanteno).

7.9 Advanced Protection

Se deli na:

- Sophos Sandstorm (oblačna storitev, namenjena analiziranju sumljivih prenosov datotek z nalaganjem datotek v oblak, imenovan Sandstorm, kjer jih oblačna storitev lahko analizira).
- Advanced Threat Protection (modul, ki spremlja omrežni promet in je ustvarjen za premagovanje vsakodnevnih ovir v omrežjih podjetij še posebej s politiko BYOD, ki v omrežje podjetja prinaša različne mobilne telefone zaposlenih z naraščajočim številom zlonamernih programskih oprem. V tem modulu se spremlja omrežni promet, kot so to npr. IP paketi, HTTP zahteve in DNS zahteve).

7.10 Endpoint Protection

Skrbnik lahko v Endpoint Protection upravlja z varnostjo prenosnih računalnikov, mobilnih telefonov in serverjev t.i. končnih naprav angl. endpoint devices.

Možnosti, ki jih Sophos UTM ponuja v tej funkciji, so:

- Computer Management (vklop ali izklop zaščite na posameznih računalnikih, ki so povezani v omrežje in so del podjetja. Možno je tudi posamezne računalnike povezovati v skupine z različnimi zaščitami).
- Antivirus (kot opisano zgoraj pri Computer Management je tudi tukaj možno posamezne računalnike povezovati v skupine z različnimi protivirusnimi zaščitami in dodajati izjeme k protivirusnim zaščitam).
- Device Control (možnost definiranja, katere naprave, ki so priklopljene na računalnik, se lahko uporabljajo in katere ne. Vsakič, ko se naprava priklopi na računalnik, se preveri nastavljena politika uporabe za posamezno skupino).
- Endpoint Web Control (zaščita naprav, ki niso v omrežju npr. pri delu od doma, so naprave pod enako politiko zaščite kot tiste v podjetju, tudi če ta računalnik ni povezan v omrežje pod nadzorom Sophos UTM. To se doseže s pomočjo oblačne storitve LiveConnect).

7.11 Wireless Protection

Služi za upravljanje in nastavljanje brezžičnih omrežij in uporabnikov, ki uporabljajo brezžična omrežja. Možnost je tudi pregledovati povezane naprave, brezžična omrežja v podjetju, njihov status in mesh omrežja (ne deluje na tehnologiji ojačevalcev signala, ampak vsaka mesh točka deluje kot samostojna enota in ni povezana le z glavnim usmerjevalnikom, ampak še s preostalimi enotami v skupno omrežje).

- Global Settings (brezžična varnost in WPA/WPA2 avtentikacija).
- Access Points (pregled nad dostopnimi točkami, kot so mesh omrežja, brezžična omrežja in mobilne dostopne točke, angl. hotspots).

7.12 Webserver Protection

Webserver Protection je namenjen konfiguraciji spletne aplikacije, da lahko ta zaščiti server pred zlonamerno programsko opremo in napadi na server.

- Web Application Firewall (nastavitev zaščite serverja pred zlonamerno programsko opremo in napadom na server, kot npr. SQL injection).
- Firewall Profiles (nastavitev stopnje zaščite spletnega serverja z WAF profili. Stopnje se razlikujejo glede na filtriranje in pregledovanje spletnega serverja).
- Reverse Authentication (ustvarjanje avtentikacijskih profilov, s katerimi je možno uporabnike identificirati neposredno in ne s pomočjo spletnih serverjev).
- Customization (urejanje pojavnih oken z opozorili, ko uporabnik ne more dostopati do določene spletne strani).
- Certificate Management (urejanje certifikatov, ki so povezani s Sophos UTM npr. X.5089 certifikat in nalaganje CRL - Certificate Revocation Lists).

7.13 RED Management

RED oz. Remote Ethernet Device je funkcija, ki omogoča povezavo manjših poslovalnic oz. povezanih enot podjetja z matično enoto (kot če bi ostale enote bile del lokalnega omrežja matičnega podjetja).

7.14 Site-to-site VPN

Konfiguracija site-to-site VPN povezave.

- Amazon VPC (povezava Amazon Virtual Private Cloud v Sophos UTM. To omogoča uporabnikov ustvarjanje virtualnih zasebnih oblakov, le če ima Sophos UTM statični javni naslov IP).
- IPsec (Standard, s šifriranjem in/ali avtentikacijo IP paketov ščiti IP komunikacijo).
- SSL (opisano v poglavju 4.1).
- Certificate Management (urejanje certifikatov, ki so povezani s Sophos UTM npr. X.5089 certifikat in nalaganje CRL - Certificate Revocation Lists).

7.15 Remote Access

Konfiguracija oddaljenega dostopa do omrežja s pomočjo Sophos UTM na podlagi VPN povezav.

- SSL (SSL VPN s pomočjo Open VPN ustvari šifriran tunel med zaposlenimi, ki se povezujejo od zunaj, in podjetjem. Vsak zaposleni lahko dostopa do podatkov podjetja s svojim uporabniškim imenom in geslom).
- PPTP (angl. Point-to-Point Tunneling Protocol je starejši in pogost VPN protokol, ki ga je lažje vzpostaviti in je vključen v vseh verzijah Microsoft Windows od Windows 95 naprej. Protokol PPTP je nadomestil protokol PPP angl. Point-to-Point Protocol. PPTP protokol je priporočljivo vzpostaviti le, kjer zaščita podatkov ni tako nujna, saj ima protokol varnostne pomanjkljivosti).
- L2TP over IPsec (L2TP je protokol, ki skupaj z IPsec protokolom tvori celoto in zagotavlja zasebnost, avtentikacijo in celovitost podatkov. L2TP potrebuje IPsec, saj drugače ni mogoče zagotavljati zasebnosti podatkov. S pomočjo IPsec se ustvari šifriran tunel).

- IPsec (Standard, ki s šifriranjem in/ali avtentikacijo IP paketov ščiti IP komunikacijo).
- HTML5 VPN Portal (opisano v poglavju 4.1).
- Cisco VPN Client (oddaljen dostop do omrežja podjetja s pomočjo IPsec protokola preko Cisco VPN klienta).
- Certificate management (opisano v poglavju 7.14).

7.16 Logging & Reporting

Funkcija Logging & Reporting je namenjena beleženju predhodnih in trenutnih sistemskih in tudi omrežnih varnostnih dogodkov. S pomočjo beleženja je možno odkriti varnostne pomanjkljivosti ali odpraviti težave (oboje je prikazano v obliki diagramov ali grafov).

7.17 Support

Funkcija, namenjena podpori uporabnikov Sophos UTM, ki se deli na:

- Documentation (spletni priročnik v PDF formatu je na voljo v različnih jezikih).
- Printable Configuration (poročilo o trenutnih nastavitvah WebAdmin spletne aplikacije).
- Contact Support (pomoč uporabnikom podjetja Sophos).
- Support Access (povezava na spletno aplikacijo WebAdmin uslužbencev podpore Sophos UTM, ki imajo korenski dostop do Sophos UTM).
- Tools (orodja za preverjanje: ping, traceroute in DNS Lookup).
- Advanced (podrobnejši prikaz trenutnih procesov in informacij glede Sophos UTM).

V poslovnem okolju so za zaposlene pri opravljanju dela uporabne naslednje 4 funkcije v Sophos UTM:

- Sophos Sandstorm (Sophos Sandstrom s pomočjo sandbox tehnologije in strojnega učenja, imenovanega deep learning, zazna različne vrste groženj, kot so to ciljni napadi ali izsiljevalski virusi, preden ti pridejo v omrežje).
- Flexi Port (razširitveni modul, s katerim se lahko razširi priključna mesta glede na potrebe podjetja).
- Sophos RED (uporabnost pri podjetju s podružnicami ali pri delu od doma, saj omogoča 256 bitno šifriranje).
- UTM Manager in iView (omogoča spremljanje naprav, stanje naprav, dodajanje ali odvzemanje varnostih pravil in ustvarjanje varnostnih kopij iz UTM Manager konzole. S pomočjo iView je z vdelanimi podrobnimi poročili o stanju naprav možno hitreje prepoznati morebitne napade na omrežje podjetja).

(Sophos, 2019)

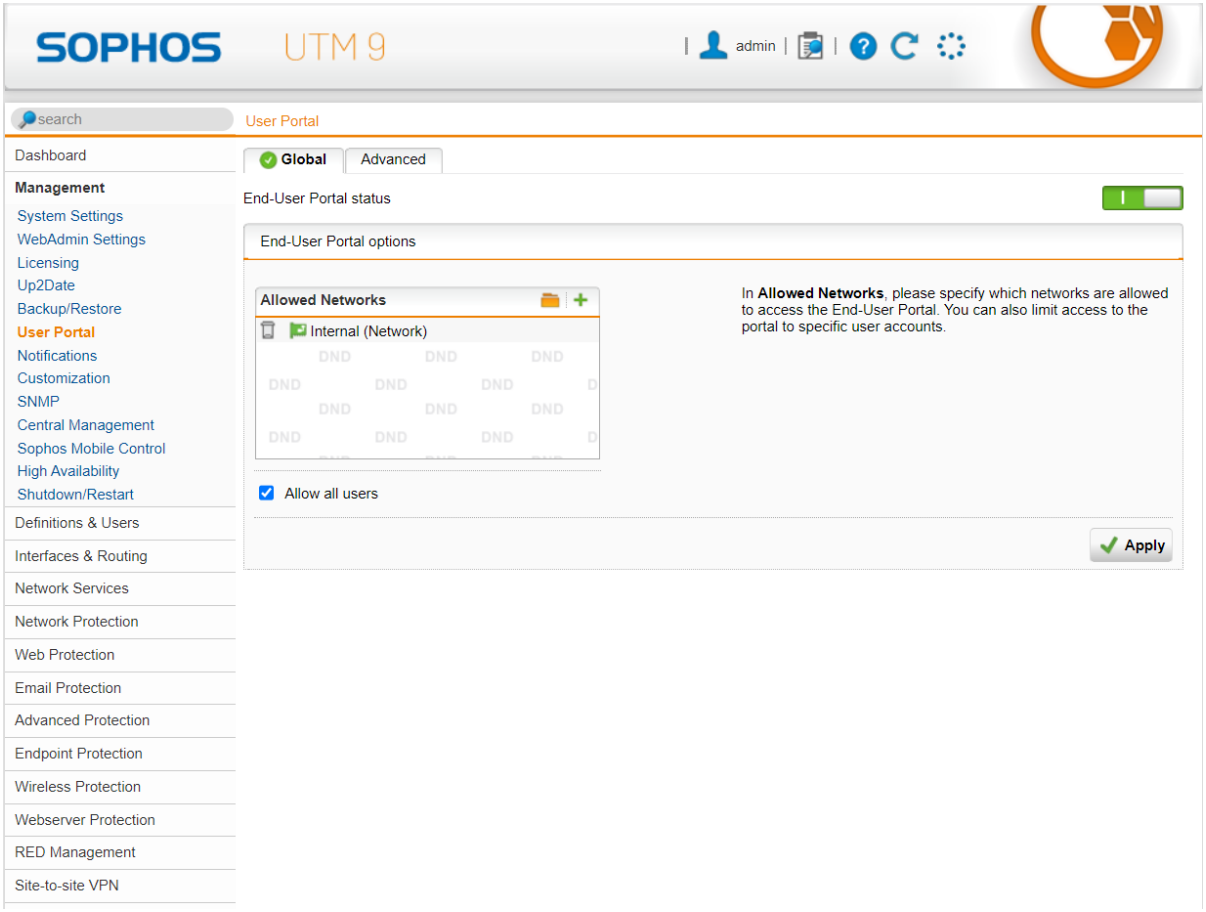
7.18 Hipoteze

7.18.1 Z ustrezno VPN tehnologijo dosegamo več kot 99,9% zaščite omrežja pred vdori v omrežje

Hipoteza je potrjena, saj z ustreznim protokolom in šifriranjem dosežemo 99,9% zaščito pred vdori v omrežje. Šifriranje je lahko simetrično ali asimetrično in protokoli so IPsec, PPTP/MPPE in L2TP/IPsec (natančneje opisano v poglavju 4 in 5).

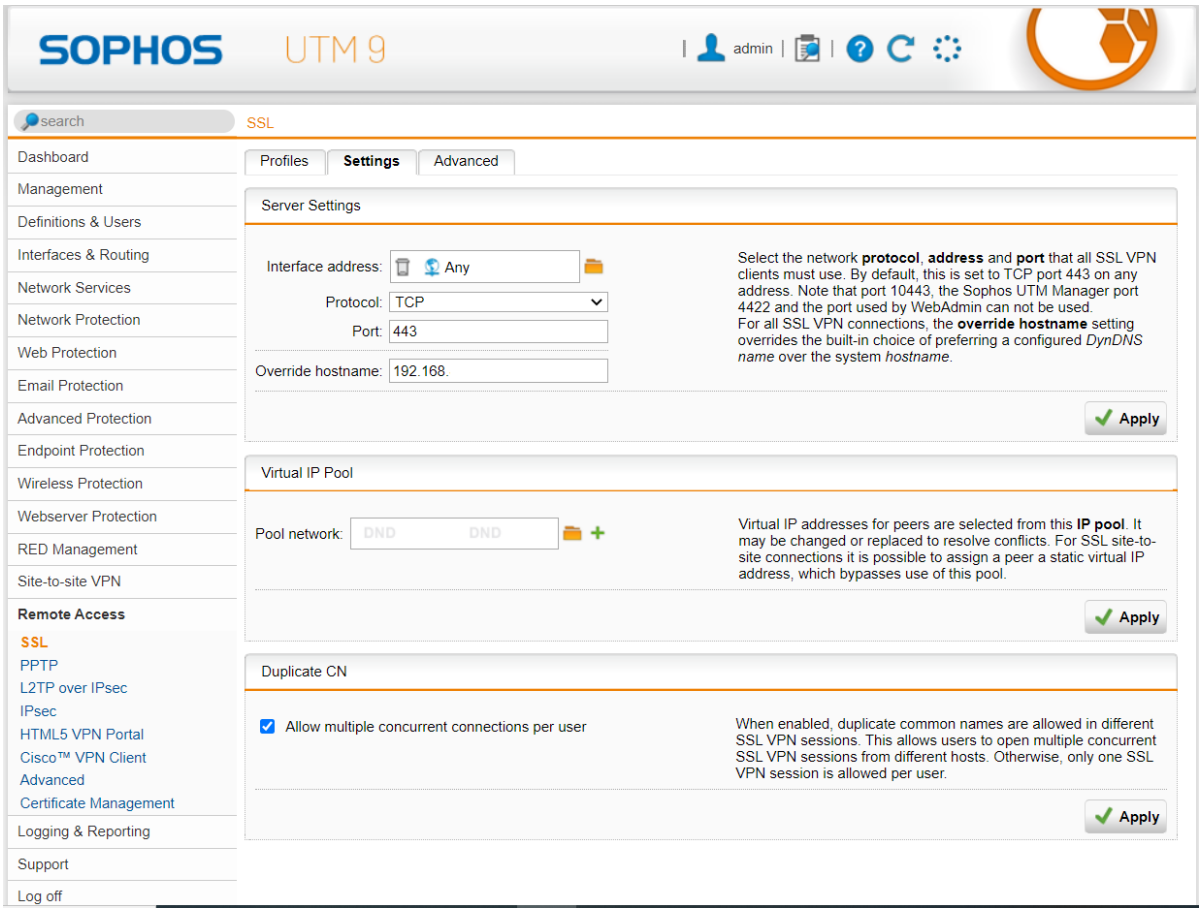
7.18.2 Za vzpostavitev VPN povezave in omrežja ni potrebno dodatno poznavanje omrežja in njegove varnosti

Hipoteza je zavrnjena, saj je za uspešno vzpostavitev omrežja in VPN povezave, dodelitev uporabnika in njegovih pravic potrebno znanje o omrežjih in njihovem delovanju. Izbira dovoljenega omrežja za končnega uporabnika oz. na katera omrežja se lahko končni uporabnik poveže in na katera ne. Tak pristop je pomemben, da se zaposleni iz enega oddelka ne more povezati na omrežje drugega oddelka, če to ni zahtevano in da ne dostopa do podatkov, ki so zaupne narave (prikazano na sliki 3).



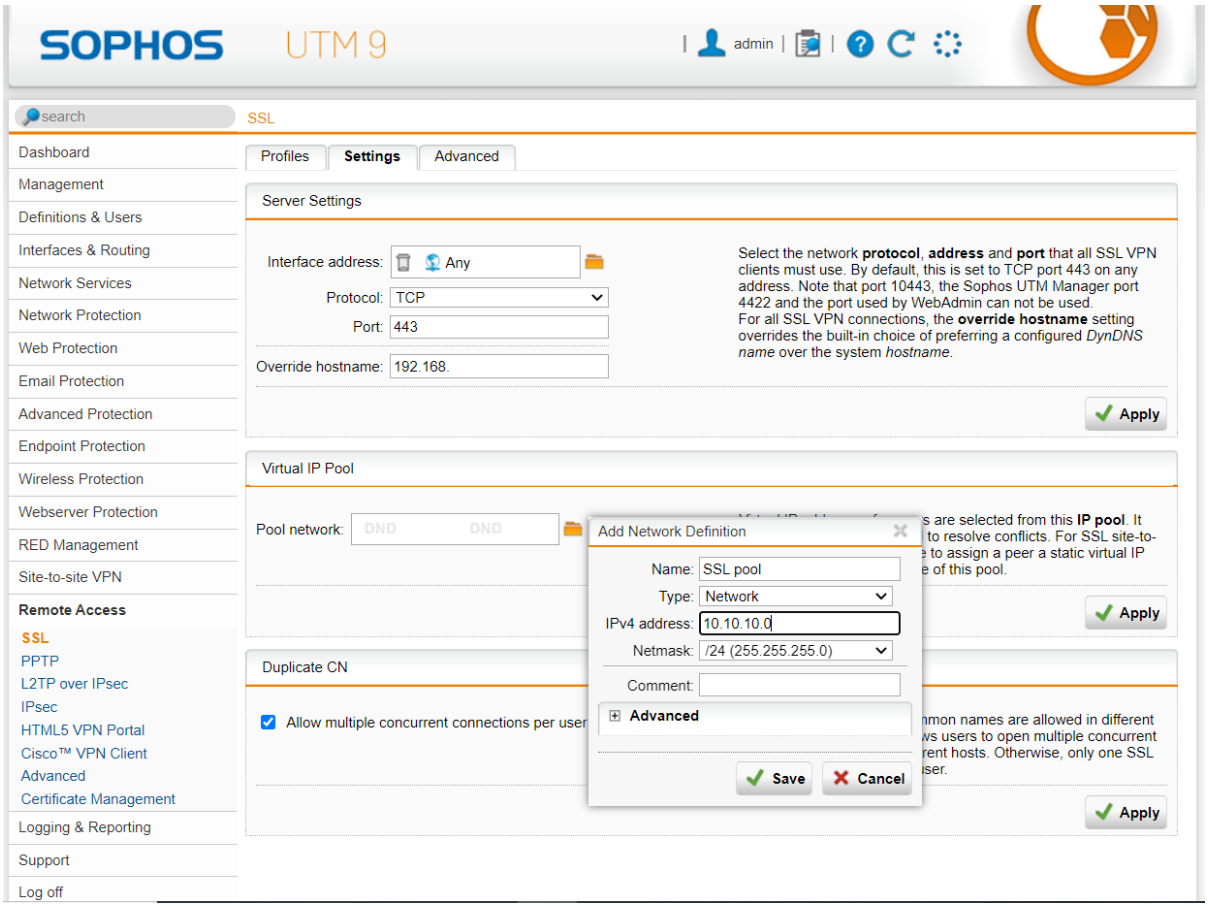
Slika 3: izbira dovoljenega omrežja za končnega uporabnika

Vir: lastni



Slika 4: izbira naslova, protokola, vrat, IP naslova in dodelitev možnosti več istočasnih povezav istega posameznika na omrežje (npr. računalnik, telefon in tablični računalnik)

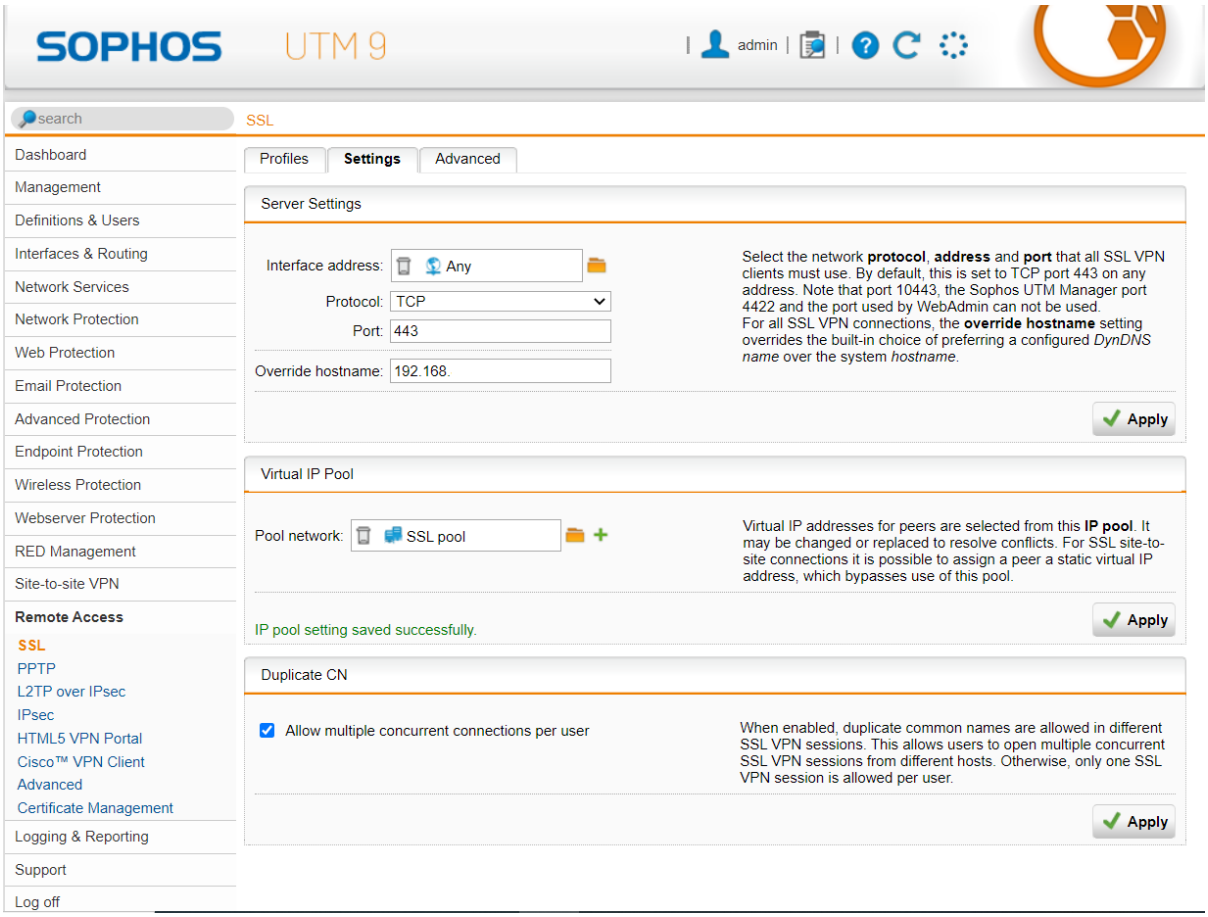
Vir: lastni



Slika 5: konfiguracija zaloge naslova (IP Pool)

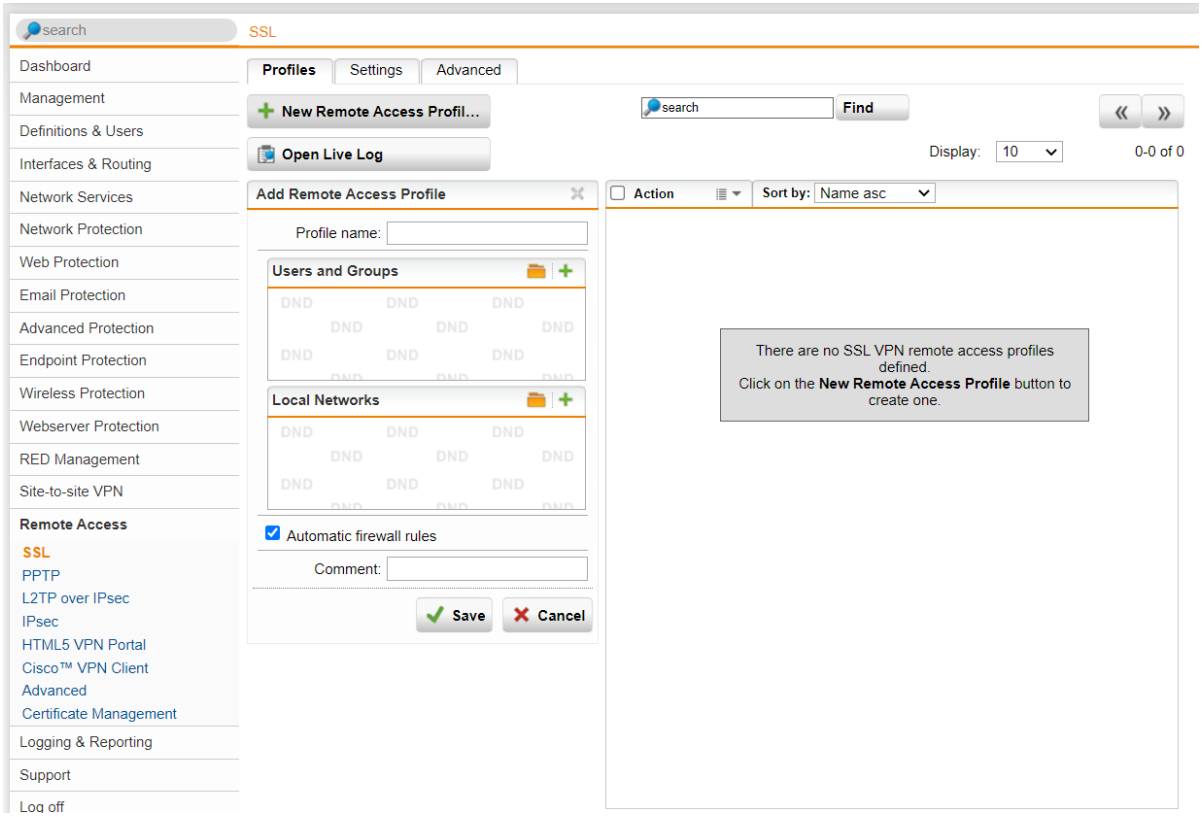
Vir: lastni

Prikaz konfiguracije zaloge naslova IP Pool, ki določi IP naslove SSL uporabnikom iz določenega IP obsega.



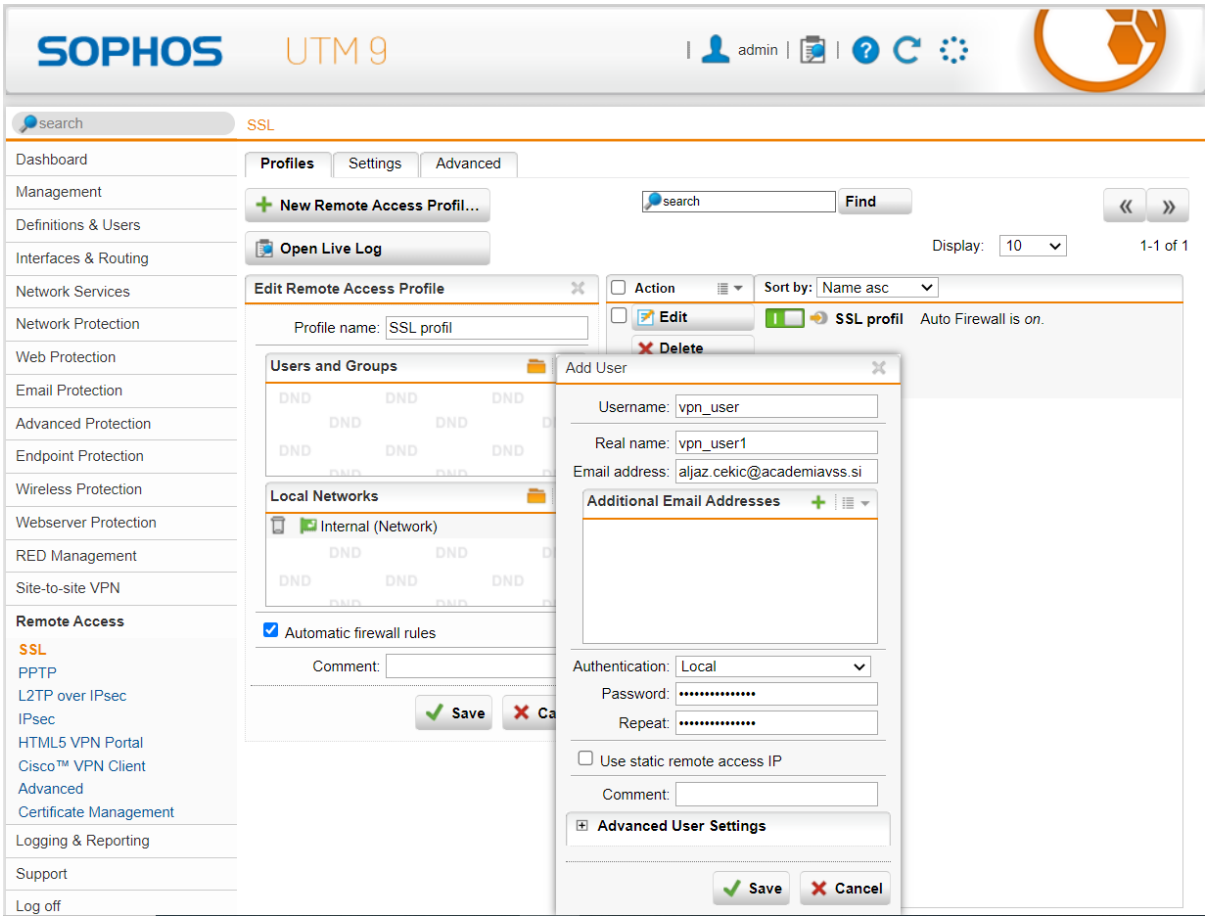
Slika 6: potrditev vseh nastavitev z gumbom »Apply«

Vir: lastni



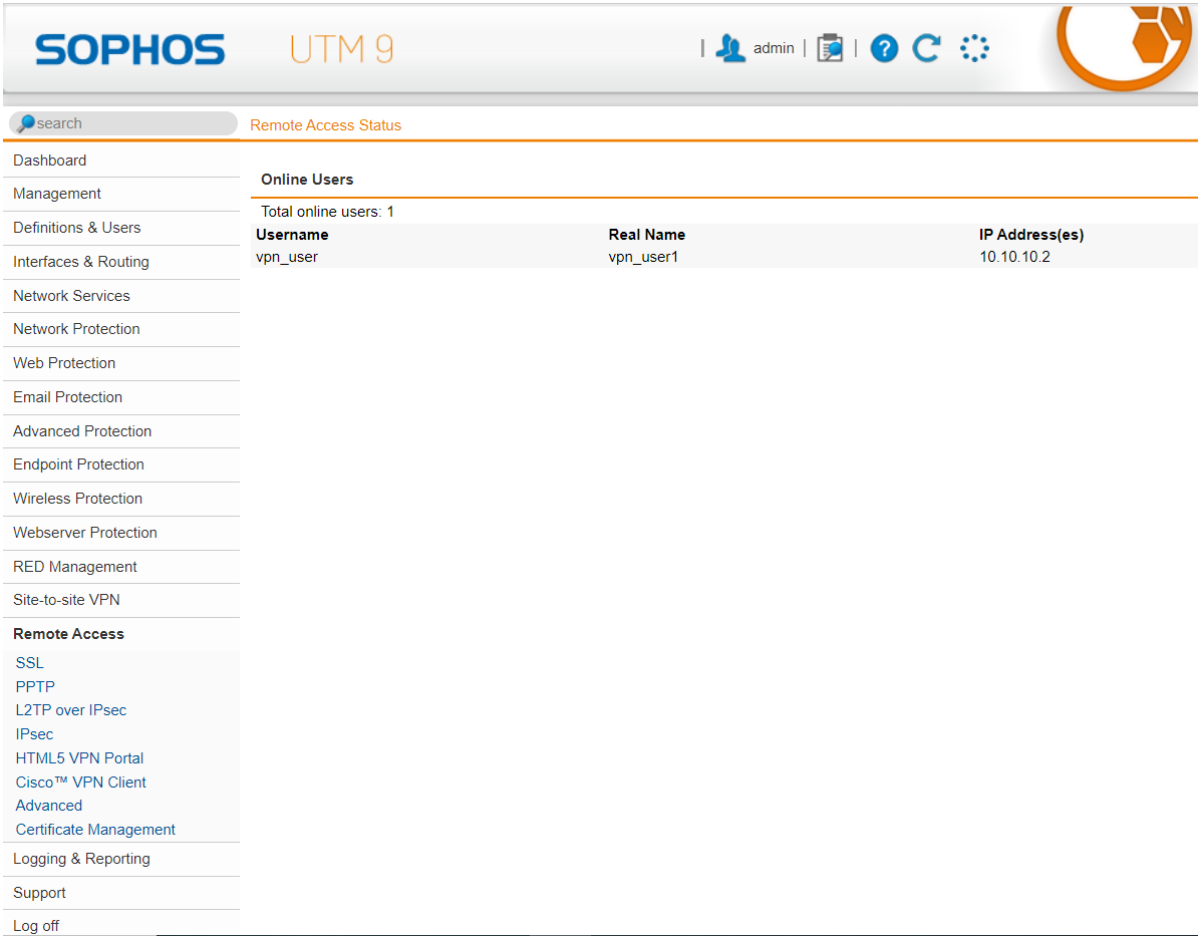
Slika 7: vnos uporabnika ali skupine in lokalnega omrežja

Vir: lastni



Slika 8: določitev uporabniškega imena, elektronskega naslova uporabnika in gesla (povezava s sliko 15)

Vir: lastni



Slika 9: pregled vseh povezanih uporabnikov na omrežje

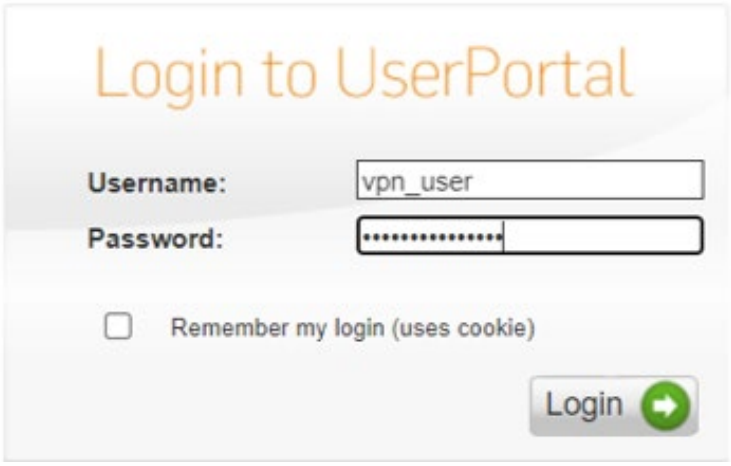
Vir: lastni

Ob povezavi uporabnika oz. uporabnikov na omrežje je tudi to mogoče pregledovati. Prikazano je njihovo uporabniško ime, pravo ime in IP naslov.

7.18.3 Uporaba VPN povezave ne zahteva dobrega poznavanja VPN tehnologije

Hipoteza drži, saj je uporaba VPN povezave za končnega uporabnika enostavna. Prve 3 korake in dodelitev uporabniškega imena in gesla v podjetju opravi podjetje samo oz. skrbnik IT, ki naloži vse potrebno za učinkovito delovanje VPN povezave.

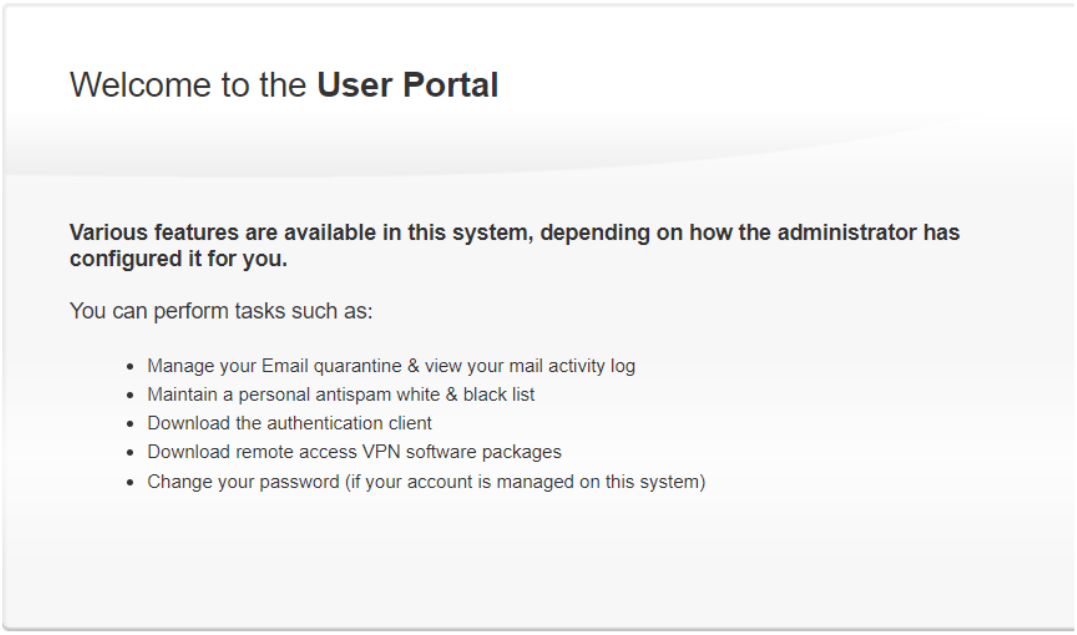
Korak 4 in 5 pa izvede končni uporabnik oz. zaposleni (pritisne na gumb »connect«, vpiše uporabniško ime in geslo ter pritisne na gumb »ok«).



Slika 10: vpis v User Portal z uporabniškim imenom in geslom

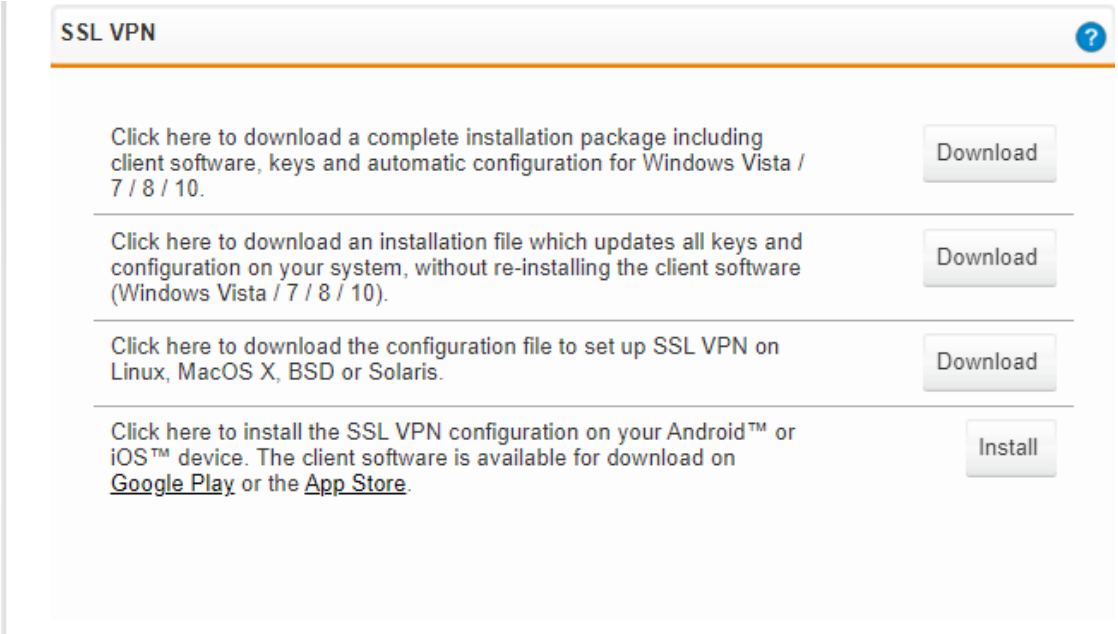
Vir: lastni

Korak 1 je vpis dodeljenega uporabniškega imena (Username) in gesla (Password) v UserPortal.



Slika 11: pozdravno okno z opisom možnosti

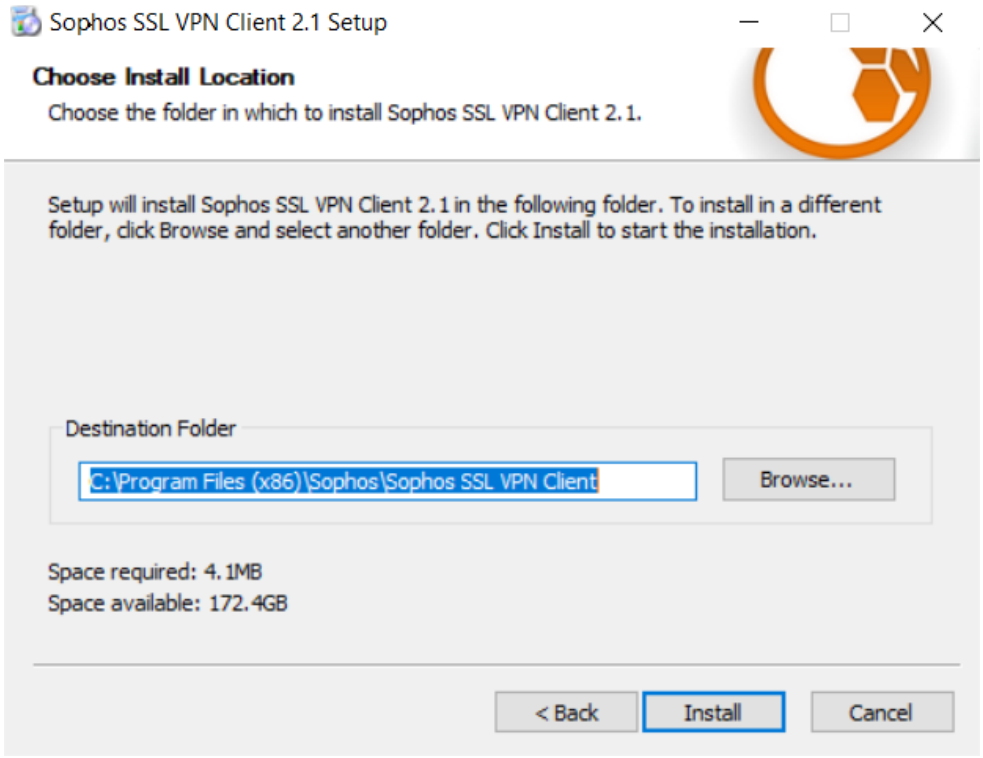
Vir: lastni



Slika 12: izbira namestitve

Vir: lastni

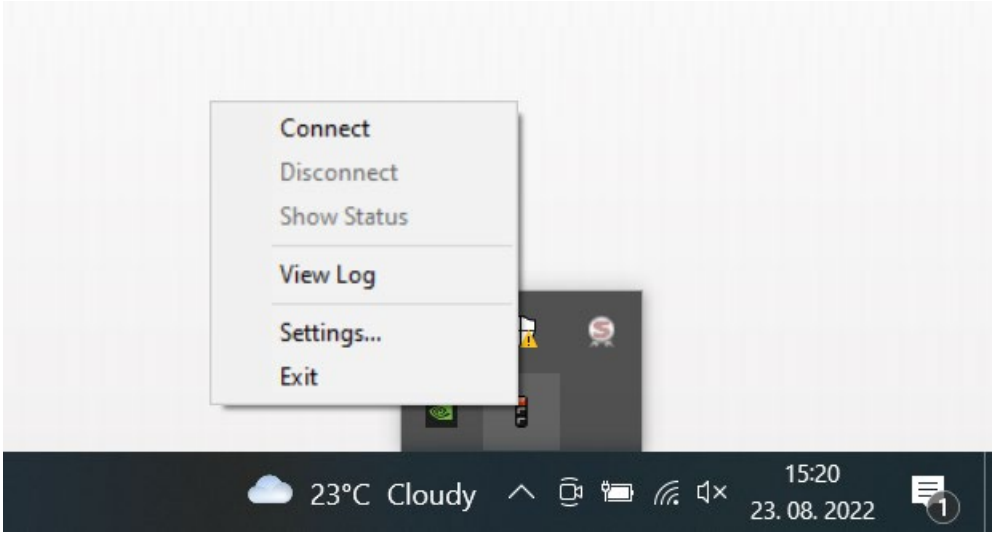
- Korak 2 na sliki 12 je izbira namestitve: pri izbiri prve možnosti (od zgoraj navzdol) Sophos UTM namesti na računalnik vse potrebno za delovanje VPN povezave za operacijski sistem Windows Vista, 7, 8 ali 10.
- Druga možnost je namenjena posodobitvi ključev in konfiguracije na sistemu, ne da bi uporabnik moral ponovno namestiti programsko opremo VPN. Druga možnost je prav tako za operacijski sistem Windows Vista, 7, 8 ali 10.
- Tretja možnost je namenjena namestitvi in vzpostavitvi VPN povezave na operacijskih sistemih Linux, MacOS X, BSD ali Solaris.
- Četrta možnost je namenjena namestitvi in vzpostavitvi VPN povezave na operacijskih sistemih za mobilne telefone Android ali iOS. Programska oprema je na voljo tudi na Google Play in App Store.



Slika 13: izbira mape na lokalnem disku za namestitev VPN povezave

Vir: lastni

V tretjem koraku je na voljo izbira mape na lokalnem disku za namestitev VPN povezave. S klikom na gumb »Install« se namestitev izvede.



Slika 14: povezava na VPN

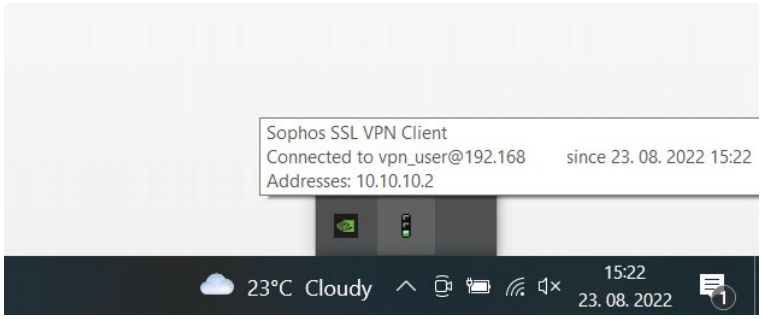
Vir: lastni

V 4. koraku se izvede povezava na VPN s pritiskom na gumb »Connect« (slika 14).

Slika 15: vpis uporabniškega imena in gesla

Vir: lastni

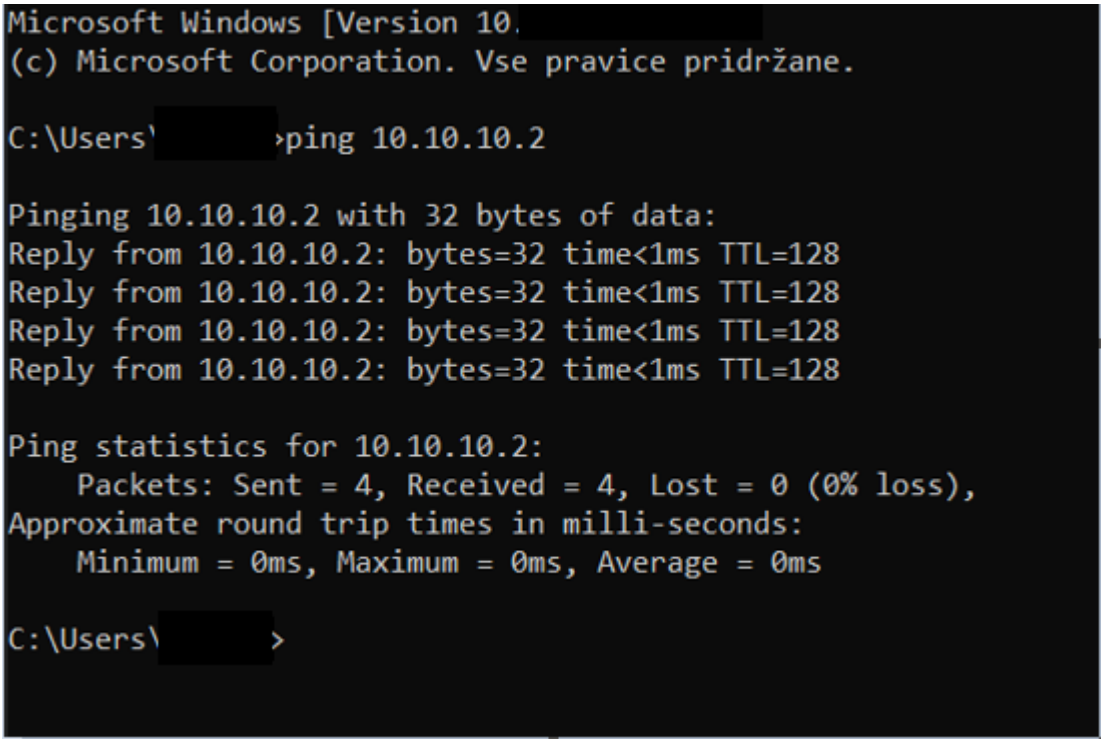
Korak 5 na sliki 15 je vpis uporabniškega imena in gesla, ki ga skrbnik dodeli posamezniku skupaj z vsemi pravicami in omejitvami (se navezuje na sliko 7).



Slika 16: prikaz uspešno vzpostavljene povezave

Vir: lastni

Prikaz uspešno vzpostavljene povezave: prikazana je ikona zelene barve in beseda »Connected to« (slika 16).



Slika 17: zakasnitev (ping) naslova 10.10.10.2

Vir: lastni

7.18.4 Vzpostavitev VPN povezave je zadosten ukrep pri varovanju zaupnih podatkov podjetja brez dodatnih varnostnih mehanizmov (požarni zidovi, protivirusni programi itd.)

Hipoteza je zavrnjena, saj kot je opisano v poglavjih 7.1, 7.7 in 7.10, tudi požarni zid potrebuje protivirusno zaščito, da preprečuje namestitev vohunske programske opreme in blokira škodljive spletne strani. VPN povezava in šifriranje podatkov je brez učinka, če je na računalniku nameščena vohunska programska oprema, ki se je že seznanila s podatki. Požarni zid je namenjen določitvi, kaj bo dostopalo v omrežje in na računalnik. VPN pa je namenjen varnemu prenosu podatkov preko interneta in ohranjanju anonimnosti. Zaradi tega je pomembno za učinkovito in celovito zaščito uporabljati tako požarni zid kot tudi protivirusni program in VPN povezavo.

7.18.5 Vzpostavitev VPN povezave je cenejša rešitev v primerjavi s SD-WAN

Site-to-site VPN povezava ponudnika Amazon se obračuna 0,05$ na vsako uro (za najbližjo izbrano regijo Frankfurt). Amazon za primer uporabi povezavo, ki je aktivna 30 dni, 24 ur na dan in če se skozi povezavo prenese 1000 GB podatkov na računalnik oz. računalnike in če se 500GB podatkov pošlje preko interneta. Za site-to-site povezavo je cena 36$ na mesec, za pošiljanje podatkov preko interneta s pomočjo VPN povezave pa je cena 0.09$ za vsak GB oz. 36$ na mesec. Skupni stroški tako nanesejo na 72,00$ na mesec za site-to-site VPN povezavo.

(Amazon, 2022)

SD-WAN ponudnika Amazon vključuje več storitev, kot site-to-site VPN povezava: Core Network Edge ali CNE predstavljajo dostopne točke v AWS regiji, ki je vključena v omrežje: cena je 0,50$ na uro ali 365,00$ na mesec. Data processing: za data processing se šteje vsak poslan podatek s pomočjo Amazon VPC (Amazon Virtual Private Clouds) ali VPN do core network edge: cena je 0,02$ za vsak GB, ki je poslan preko Amazon VPC oz. za 100GB poslanih podatkov je znesek 2$ na mesec. Core Network Edge attachments so za VPN in SD-WAN povezave, kot tudi Amazon VPC: cena je 0,080$ za vsako uro ali 94,90 $ na mesec. Amazon VPC je kompatibilen s Sophos UTM (opisano v poglavju 7.14).

Skupni strošek SD-WAN je 461,90$.

(Amazon, 2022)

7.18.6 Uporaba rešitev različnih ponudnikov storitev lahko privede do nezdružljivosti in tehničnih težav (večji stroški vzpostavitve VPN povezave)

Hipoteza je potrjena, saj VPN povezava s procesom tuneliranja podatkov paket oz. datagram, ki ga želi pošiljatelj poslati, vstavi v nov paket (t.i. enkapsulacija) in ga pošlje preko interneta.

Zaradi enkapsulacije lahko paket presega maksimalno dovoljeno velikost za prenos in se paketi oz. datagrami razdelijo na manjše pakete (t.i. fragmentacija). Fragmentacija, ki se pojavlja v opisanem primeru, se pojavi tudi ob napadu na omrežje. To je pogosta težava in povzroča nezdružljivost med VPN povezavo in požarnim zidom.

(Wack, Cutler, & Pole, 2022)

Zaradi tega je priporočljivo za podjetja, da uporabljajo enotno rešitev, kot to zagotavlja Sophos UTM.

7.18.7 Prenosna hitrost je pri vzpostavljeni VPN povezavi počasnejša kot brez vzpostavljene VPN povezave

Hipoteza je delno potrjena:

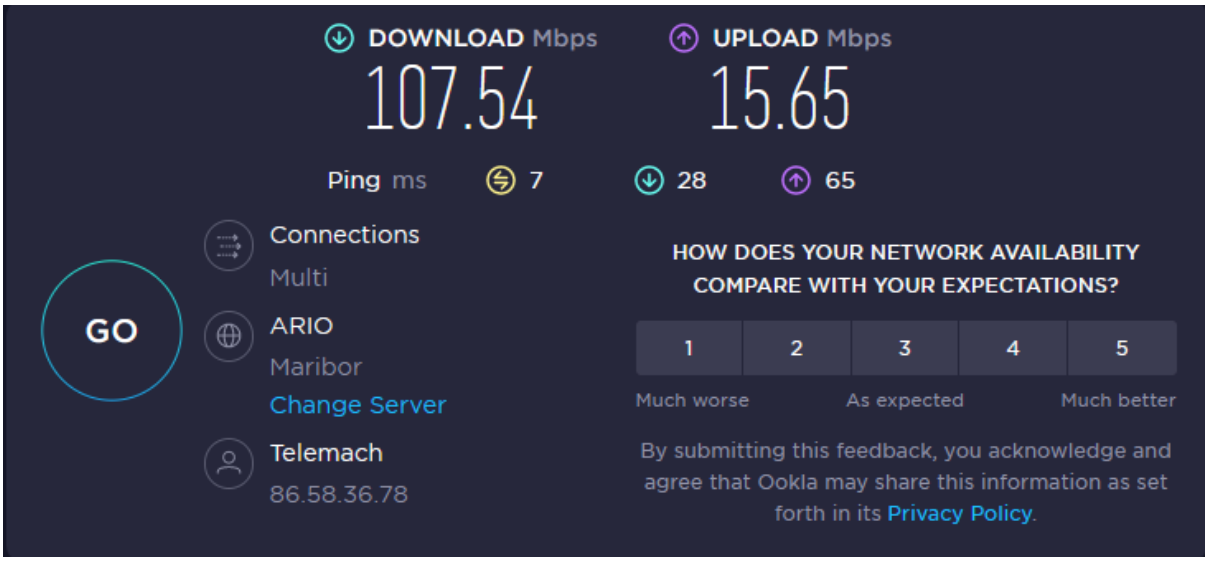
Potrjena je v delu, da se vsi podatki prenašajo skozi šifriran tunel in to predstavlja dodaten korak. Z dobro VPN povezavo je padec v hitrosti internetne povezave nizek. Šifriranje podatkov s standardom AES (angl. Advanced Encryption Standard), ki je lahko 128-bitno, 192-bitno ali 256-bitno šifriranje nam z vsako višjo stopnjo šifriranja ponuja večjo varnost in zanesljivost pri varnosti podatkov, kar po drugi strani zmanjšuje prenosno hitrost. Razmerje med hitrostjo in stopnjo zaščite je obratno sorazmerno oz. večja kot je stopnja zaščite, manjša je prenosna hitrost in obratno: nižja kot je stopnja zaščite, višja je prenosna hitrost.

Na hitrost vpliva tudi obremenitev serverja oz. več kot je povezanih uporabnikov na serverju, večja je obremenitev in posledično je prenosna hitrost počasnejša.

Hipoteza je zavrnjena v delu, ko je internetna hitrost hitrejša z vzpostavljeno VPN povezavo, ker ponudnik internetnih storitev umetno upočasnjuje hitrost z namenom sprostitve obremenitve na širšem področju, npr. če želijo ob velikem številu gledalcev nogometne tekme preko interneta omejiti prenos za neko spletno stran.

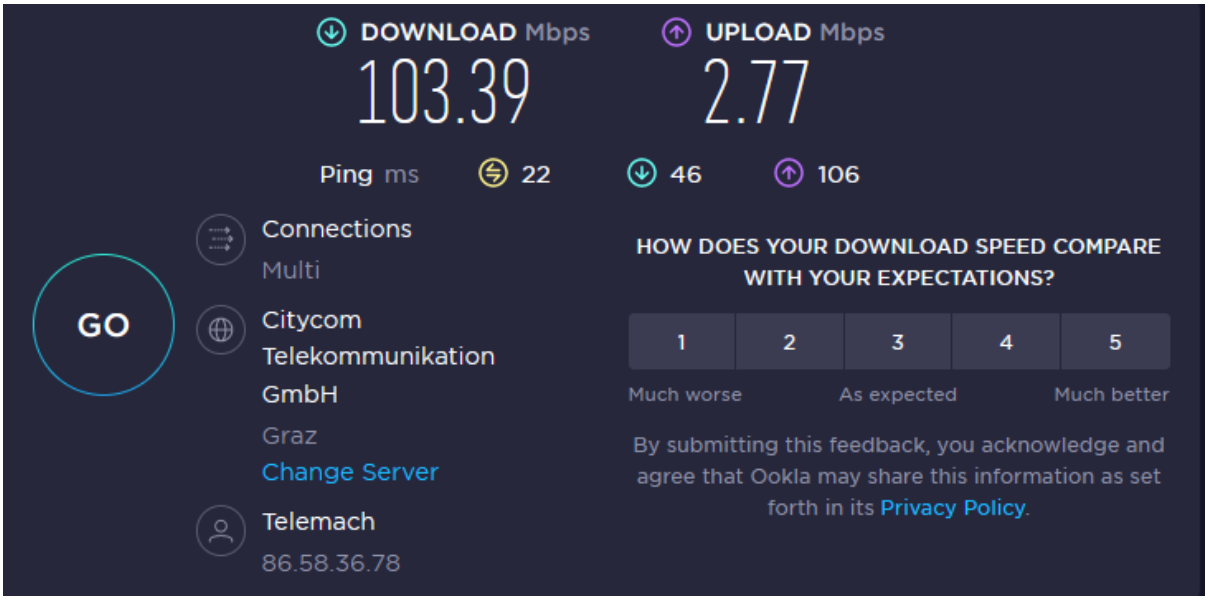
Ponudnik internetnih storitev ob vzpostavljeni VPN povezavi ne more postaviti takšnih omejitev, ker je prenos podatkov šifriran in s tem je blokiran vpogled v uporabnikovo dejavnost.

Praktična izvedba:



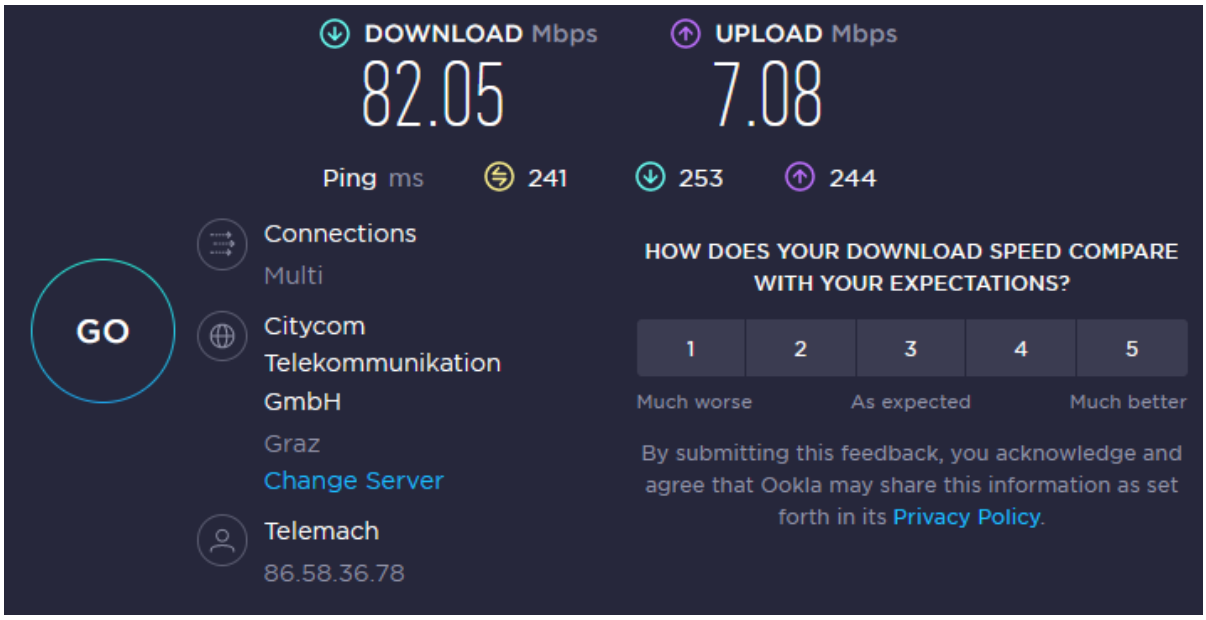
Slika 18: hitrost brez VPN povezave

Vir: lastni



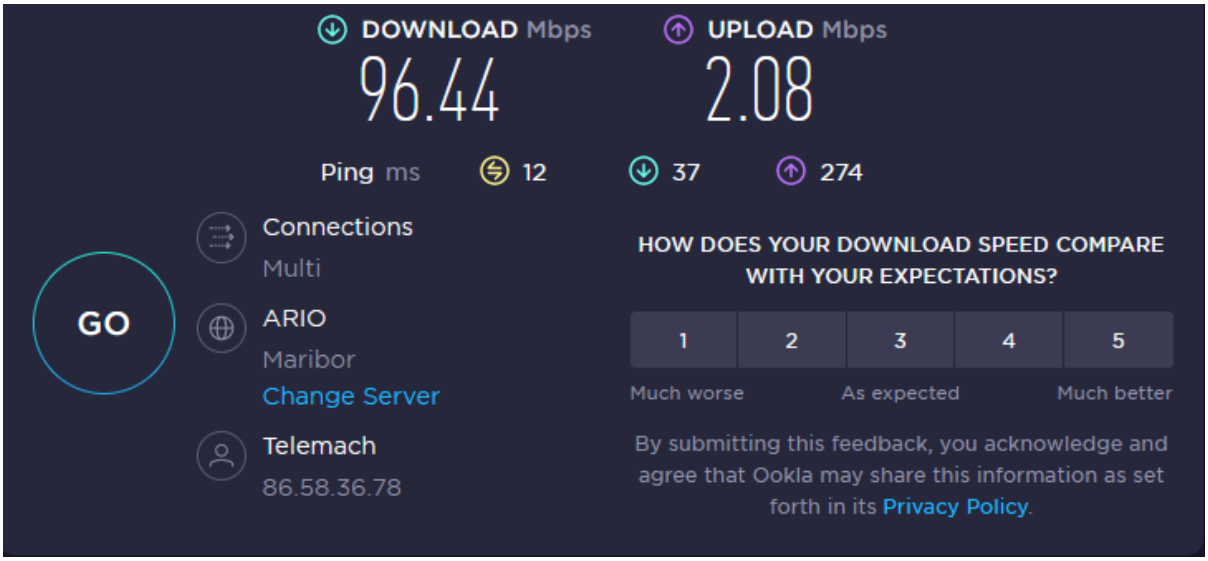
Slika 19: hitrost z vzpostavljeno VPN povezavo s serverjem v Avstriji z uporabo Surf Shark VPN

Vir: lastni



Slika 20: hitrost z vzpostavljeno VPN povezavo s serverjem v Indiji z uporabo Surf Shark VPN

Vir: lastni

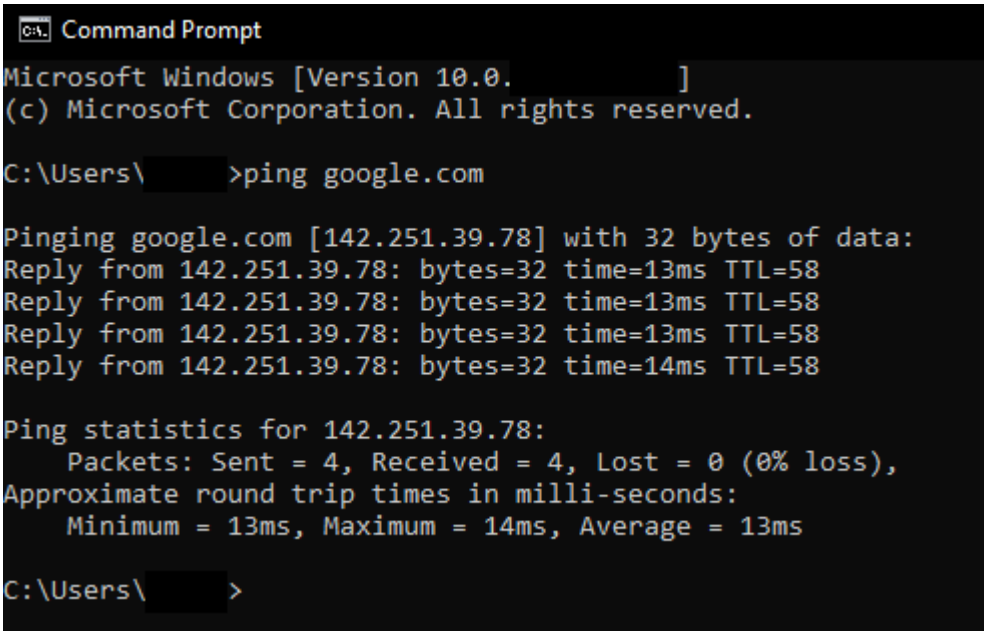


Slika 21: hitrost z vzpostavljeno VPN povezavo s serverjem v Sloveniji z uporabo Surf Shark VPN

Vir: lastni

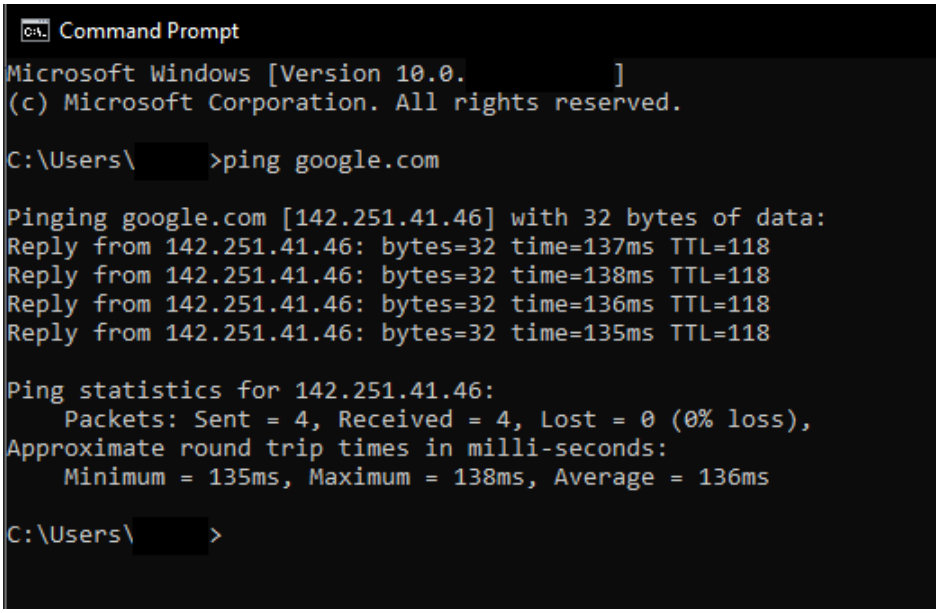
7.18.8 Obhodni čas (ping) se pri vzpostavljeni VPN povezavi podaljša v primerjavi, ko VPN povezava ni vzpostavljena

Hipoteza je potrjena, saj oddaljenost od serverja vpliva na prenosno hitrost, kar pomeni, da če se uporabnik iz Slovenije poveže na server v Avstraliji, bojo paketi potovali dlje časa, kot če bi izbrali server npr. v Indiji. Iz tega razloga je vedno priporočljivo izbrati server iz bližnje države ali izbrati lokalni VPN server.



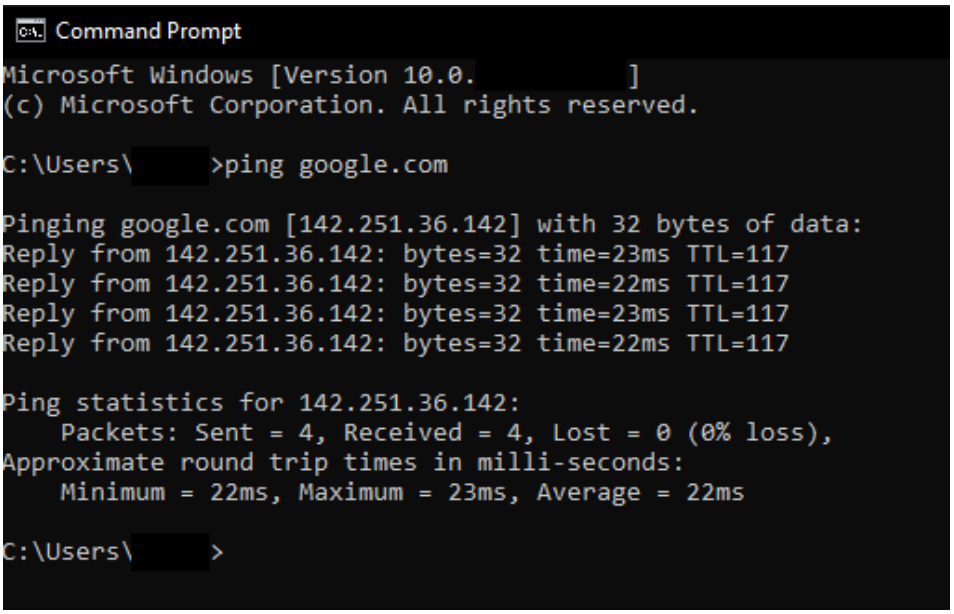
Slika 22: zakasnitev (ping) brez VPN povezave

Vir: lastni



Slika 23: prikaz zakasnitve (ping) z VPN povezavo s serverjem v Indiji

Vir: lastni



Slika 24: prikaz zakasnitve (ping) z VPN povezavo s serverjem v Avstriji

Vir: lastni

8 SKLEP

H1: Z ustrezno VPN tehnologijo dosegamo več kot 99,9% zaščite omrežja pred vdori v naše omrežje.

Hipoteza je potrjena, saj z ustreznim protokolom in šifriranjem dosežemo 99,9% zaščito pred vdori v naše omrežje. Šifriranje je lahko simetrično ali asimetrično in protokoli so IPsec, PPTP/MPPE in L2TP/IPsec (natančneje opisano v poglavju 4 in 5).

H2: Za vzpostavitev VPN povezave in omrežja ni potrebno dodatno poznavanje omrežja in njegove varnosti.

Hipoteza je zavrnjena, saj je za uspešno vzpostavitev omrežja in VPN povezave, dodelitev uporabnika in njegovih pravic potrebno znanje o omrežjih in njihovem delovanju. Izbira dovoljenega omrežja za končnega uporabnika oz. na katera omrežja se lahko končni uporabnik poveže in na katera ne. Tak pristop je pomemben, da se zaposleni iz enega oddelka ne more povezati na omrežje drugega oddelka, če to ni zahtevano in da ne dostopa do podatkov, ki so zaupne narave (prikazano na sliki 3).

H3: Uporaba VPN povezave ne zahteva dobrega poznavanja VPN tehnologije.

Hipoteza drži, saj je uporaba VPN povezave za končnega uporabnika enostavna. Prve 3 korake in dodelitev uporabniškega imena in gesla v podjetju opravi podjetje samo oz. skrbnik IT, ki naloži vse potrebno za učinkovito delovanje VPN povezave.

H4: Vzpostavitev VPN povezave je zadosten ukrep pri varovanju zaupnih podatkov podjetja brez dodatnih varnostnih mehanizmov (požarni zidovi, protivirusni programi itd.).

Hipoteza je zavrnjena, saj kot je opisano v poglavjih 7.1, 7.7 in 7.10, tudi požarni zid potrebuje protivirusno zaščito, da preprečuje namestitev vohunske programske opreme in da blokira škodljive spletne strani. VPN povezava in šifriranje podatkov je brez učinka, če je na računalniku nameščena vohunska programska oprema, ki se je že seznanila s podatki. Požarni zid je namenjen določitvi, kaj bo dostopalo v omrežje in na računalnik. VPN je namenjen varnemu prenosu podatkov preko interneta in ohranjanju anonimnosti. Zaradi tega je pomembno za učinkovito in celovito zaščito uporabljati tako požarni zid kot tudi protivirusni program in VPN povezavo.

H5: Vzpostavitev VPN povezave je cenejša rešitev v primerjavi s SD-WAN.

Site-to-site VPN povezava ponudnika Amazon se obračuna 0,05$ na vsako uro (za najbližjo izbrano regijo Frankfurt). Amazon za primer uporabi povezavo, ki je aktivna 30 dni, 24 ur na dan in če se skozi povezavo prenese 1000 GB podatkov na računalnik oz. računalnike in če se 500GB podatkov pošlje preko interneta. Za site-to-site povezavo je cena 36$ na mesec, za pošiljanje podatkov preko interneta s pomočjo VPN povezave pa je cena 0.09$ za vsak GB oz. 36$ na mesec. Skupni stroški tako nanesejo na 72,00$ na mesec za site-to-site VPN povezavo.

(Amazon, 2022)

SD-WAN ponudnika Amazon vključuje več storitev, kot site-to-site VPN povezava: Core Network Edge ali CNE predstavljajo dostopne točke v AWS regiji, ki je vključena v omrežje: cena je 0,50$ na uro ali 365,00$ na mesec. Data processing: za data processing se šteje vsak poslan podatek s pomočjo Amazon VPC (Amazon Virtual Private Clouds) ali VPN do core network edge: cena je 0,02$ za vsak GB, ki je poslan preko Amazon VPC oz. za 100GB poslanih podatkov je znesek 2$ na mesec. Core Network Edge attachments so za VPN in SD-WAN povezave, kot tudi Amazon VPC: cena je 0,080$ za vsako uro ali 94,90$ na mesec. Amazon VPC je kompatibilen s Sophos UTM (opisano v poglavju 7.14).

Skupni strošek SD-WAN je 461,90 $.

(Amazon, 2022)

H6: Uporaba rešitev različnih ponudnikov storitev lahko privede do nezdružljivosti in tehničnih težav (večji stroški vzpostavitve VPN povezave).

Hipoteza je potrjena, saj VPN povezava s procesom tuneliranja podatkov paket oz. datagram, ki ga želi pošiljatelj poslati, vstavi v nov paket (t.i. enkapsulacija) in ga pošlje preko interneta. Zaradi enkapsulacije lahko paket presega maksimalno dovoljeno velikost za prenos in se paketi oz. datagrami razdelijo na manjše pakete (t.i. fragmentacija). Fragmentacija, ki se pojavlja v opisanem primeru, se pojavi tudi v primerih napada na omrežje. To je pogosta težava in povzroča nezdružljivost med VPN povezavo in požarnim zidom, (Wack, Cutler, & Pole, 2022). Zaradi tega je priporočljivo za podjetja, da uporabljajo enotno rešitev, kot to zagotavlja Sophos UTM.

H7: Prenosna hitrost je pri vzpostavljeni VPN povezavi počasnejša kot brez vzpostavljene VPN povezave.

Hipoteza je delno potrjena.

Potrjena je v delu, da se vsi podatki prenašajo skozi šifriran tunel in to predstavlja dodaten korak. Z dobro VPN povezavo je padec v hitrosti internetne povezave nizek. Šifriranje podatkov s standardom AES (angl. Advanced Encryption Standard), ki je lahko 128-bitno, 192-bitno ali 256-bitno šifriranje, nam z vsako višjo stopnjo šifriranja ponuja večjo varnost in zanesljivost pri varnosti podatkov, kar po drugi strani zmanjšuje prenosno hitrost. Razmerje med hitrostjo in stopnjo zaščite je obratno sorazmerno oz. večja, kot je stopnja zaščite, manjša je prenosna hitrost in obratno: nižja, kot je stopnja zaščite, višja je prenosna hitrost.

Na hitrost vpliva tudi obremenitev serverja oz. več kot je povezanih uporabnikov na serverju, večja je obremenitev in posledično je prenosna hitrost počasnejša.

Hipoteza je zavrnjena v delu, ko je interneta hitrost hitrejša z vzpostavljeno VPN povezavo, ker ponudnik internetnih storitev umetno upočasnjuje hitrost z namenom sprostitve obremenitve na širšem področju: npr. če želijo ob velikem številu gledalcev nogometne tekme preko interneta omejiti prenos za neko spletno stran. Ponudnik internetnih storitev ob vzpostavljeni VPN povezavi ne more postaviti takšnih omejitev, ker je prenos podatkov šifriran in s tem je blokiran vpogled v uporabnikovo dejavnost.

H8: Obhodni čas (ping) se pri vzpostavljeni VPN povezavi podaljša v primerjavi, ko VPN povezava ni vzpostavljena.

Hipoteza je potrjena, saj oddaljenost od serverja vpliva na prenosno hitrost, kar pomeni, da če se uporabnik iz Slovenije poveže na server v Avstraliji, bojo paketi potovali dlje časa, kot če bi izbrali server npr. v Indiji. Iz tega razloga je vedno priporočljivo izbrati server iz bližnje države ali izbrati lokalni VPN server.

9 VIRI IN LITERATURA

Amazon. (2022). *AWS Cloud WAN.* Pridobljeno iz AWS Cloud WAN pricing: https://aws.amazon.com/cloud-wan/pricing/

Amazon. (2022). *AWS VPN.* Pridobljeno iz AWS VPN pricing: https://aws.amazon.com/vpn/pricing/

Barracuda. (1. november 2022). *Barracuda*. Pridobljeno iz SSL VPN: https://www.barracuda.com/glossary/ssl-vpn

Brglez, D. (4. november 2019). *eAcademia.* Pridobljeno iz Varnost naprav in delovanje omrežij - powerpoint predstavitev: https://student.academia.si/course/view.php?id=460

Cisco. (13. oktober 2008). *Cisco*. Pridobljeno iz How Virtual Private Networks Work: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Cisco. (4. maj 2009). *Cisco*. Pridobljeno iz Guest WLAN and Internal WLAN using WLCs Configuration Example: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/70937-guest-internal-wlan.html

ISO. (2018). *Online Browsing Platform (OBP).* Pridobljeno iz ISO 31000:2018(en) Risk management — Guidelines: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Menezes, J. A., Oorschot, P. C., & Vanstone, A. S. (1. avgust 2001). *Handbook of Applied Cryptography.* Pridobljeno iz Chapter 1: https://cacr.uwaterloo.ca/hac/

Nomasis. (1. november 2022). *Nomasis secures your mobility*. Pridobljeno iz Microsoft Intune: https://nomasis.ch/en/microsoft-intune/

Oracle. (1. november 2022). *The Java™ Tutorials*. Pridobljeno iz What Is a Datagram?: https://docs.oracle.com/javase/tutorial/networking/datagrams/definition.html

Schneier, B. (1. januar 1996). *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source.* Pridobljeno iz Applied Cryptography, Second Edition: Protocols, Algorthms, and Source: https://mrajacse.files.wordpress.com/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf

Sophos. (2019). *Sophos Support.* Pridobljeno iz Sophos UTM Administration Guide: https://docs.sophos.com/nsg/sophos-utm/utm/9.6/pdf/en-us/administration-guide-9.600.pdf

Stanič, A., Blanc, I., & Sambolec, Ž. (1. junij 2012). *Slovensko zavarovalno združenje.* Pridobljeno iz Sistem upravljanja tveganj: ISO 31000 ali COSO?: https://www.zav-zdruzenje.si/wp-content/uploads/2017/11/Stani%C4%8D-Sambolec.pdf

Thomas, A. S. (2000). *Higher intellect.* Pridobljeno iz SSL & TLS Essentials Securing the Web. New York: John Wiley & Sons, Inc.: https://cdn.preterhuman.net/texts/computing/security/SSL%20And%20TLS%20Essentials%20-%20Securing%20The%20Web%202000.pdf

Wack, J., Cutler, K., & Pole, J. (januar 2022). *University System of Maryland.* Pridobljeno iz Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology: https://www.usmd.edu/usm/adminfinance/itcc/firewallpolicynis.pdf