KAUNO KOLEGIJA

TECHNOLOGIJŲ FAKULTETAS
INFORMATIKOS IR MEDIJŲ TECHNOLOGIJŲ KATEDRA

Julius Skuolevičius

VĖJO JĖGAINIŲ VALDYMO SISTEMOS SAUGAUS TINKLO PROJEKTAS

Baigiamasis darbas

Kibernetinių sistemų ir saugos studijų programos
valstybinis kodas 6531BX024
Informatikos inžinerijos studijų krypties

Vadovas dr. Dangis Rimkus

Kaunas, 2024

TURINYS

LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS

LENTELĖS

PAVEIKSLAI

SĄVOKŲ SĄRAŠAS

Sąvoka	Aprašymas	Nuoroda į šaltinį
openwrt	„OpenWrt“ yra operacinė sistema, paremta „*linux*“ operacine sistema, skirta įterptiesiems įrenginiams.	(openwrt.org, n.d)
DHCP	DHCP (angl. *Dynamic host configuration protocol*) yra protokolas, skirtas automatizuotam IP adresų paskirstymui kompiuterinio tinklo įrenginiams.	(coursera.com, 2023)
DNS	DNS (angl. *Domain name system*) išverčia svetainių pavadinimus, kurie sudaryti iš raidžių ir yra lengvai įsimenami žmonėm, į IP adresus, kuriuos kompiuteriai naudoja bendraudami tarpusavyje.	(gcore.com,2023)
TCP	TCP (angl. *Transmission control protocol*) yra duomenų perdavimo protokolas. Šis protokolas yra į ryšį orientuotas komunikacijos protokolas, padedantis keistis pranešimais tarp skirtingų įrenginių tinkle, užtikrinant, kad duomenys siunčiami laikantys tam tikrų taisyklių.	(geeksforgeeks.org, 2024)
UDP	UDP (angl. *User datagram protocol*) yra standartizuotas duomenų perdavimo tarp dviejų kompiuterių tinkle metodas. UDP šį procesą atlieka paprastai, nesilaikant gausybes taisyklių: siunčia paketus tiesiai į tikslinį IP adresą, prieš tai neužmegzdamas ryšio, nenurodydamas paketų sekos ir netikrindamas, ar jie atkeliavo taip, kaip numatyta.	(cloudflare.com, n.d)
HTTP	HTTP (angl. *Hypertext Transfer Protocol*) yra taisyklių rinkinys, apibrėžiantis, kaip duomenys perduodami tarp kliento ir serverio internete.	(Bello, 2023)
HTTPS	Saugus hiperteksto perdavimo protokolas (angl. *Hypertext transfer protocol secure*) yra šifruota HTTP versija	(Pol, 2024)
ISAKMP	Interneto saugos asociacija ir raktų valdymo protokolas (angl. *Internet Security Association and Key Management Protocol*) skirtas sukurti saugumo asociacijas ir saugiai keistis raktais.	(Kumar, 2023)
IP adresas	Interneto protokolo (angl. *Internet protocol*) adresas yra unikalus identifikavimo numeris, priskirtas kiekvienam įrenginiui, prijungtam prie kompiuterinio tinklo.	(fortinet.com,2024)
SIM	SIM kortelė yra maža plastikinė kortelė su kompiuterio lustu, įdedama į įrenginį, palaikantį mobilųjį ryšį. SIM kortelėje yra daugybė informacijos, įskaitant telefono numerį ir kitą informaciją su kuri naudojama leidžiant prisijungti prie išorinio tinklo. SIM reiškia abonento tapatybės modulį (angl. *Subscriber Identity Module*).	(vodafone.co.uk, n.d)
RS232	RS-232 yra duomenų perdavimo protokolas, siunčiantis po vieną bitą serijiniu būdu. RS-232 kabelis yra tai, kas leidžia užmegzti tokio tipo ryšį, perduodant duomenis iš vieno įrenginio į kitą.	(uk.rs-online.com,2023)
RS485	RS-485 yra pramoninė specifikacija, apibrėžianti elektrinę sąsają ir fizinį sluoksnį, skirtą elektros prietaisų ryšiui perduoti iš taško į tašką. RS-485 standartas leidžia nutiesti kabelius dideliu atstumu elektros triukšmingoje aplinkoje ir gali palaikyti kelis įrenginius toje pačioje magistralėje.	(Kelly, 2024)
LTE	LTE (angl. *Long-Term Evolution*) yra ketvirtos kartos belaidžio ryšio standartas, užtikrinantis didesnį tinklo pajėgumą ir greitį mobiliesiems telefonams ir kitiems mobilųjį ryšį palaikantiems įrenginiams.	(Gillis, 2023)

Sąvoka	Aprašymas	Nuoroda į šaltinį
VDC	VDC (angl. *Volts Direct Current*) yra nuolatinės srovės grandinės įtampa.	(French, 2023)
SSH	SSH (angl. *Secure Shell*) yra tinklo protokolas, per kurį vartotojai gali užmegzti saugius nuotolinius ryšius norint pasiekti išteklius neapsaugotame išoriniame arba vietiniame tinkle. Administratoriai dažniausiai naudoja SSH protokolą norėdami prisijungti nuotoliniu būdu ir pasiekti savo tinklo įrenginius, atlikti failų perkėlimą, vykdyti komandas ir valdyti įrenginius.	(manageengine.com, 2024)
Wi-Fi	Wi-Fi yra belaidė technologija, leidžianti mobiliesiems telefonams, kompiuteriams, planšetiniams kompiuteriams ir kitiems elektroniniams įrenginiams prisijungti prie kompiuterinio tinklo.	(usnews.com, 2023)
SSL	SSL (angl. *Secure Sockets Layer*) yra standartinė technologija, skirta užtikrinti interneto ryšį šifruojant duomenis, siunčiamus tarp svetainės ir naršyklės (arba tarp dviejų ir daugiau tinklo įrenginių, serverių, naršyklių).	(digicert.com, n.d)
TLS	TLS (angl. *Transport Layer Security*) yra atnaujinta, saugesnė SSL versija.	(digicert.com, n.d)

SANTRAUKA

Autorius Julius Skuolevičius. *Vėjo jėgainių valdymo sistemos saugaus tinklo projektas*. Baigiamasis darbas. Vadovas dr. Dangis Rimkus. Kauno kolegija, Technologijų fakultetas, Informatikos ir medijų technologijų katedra. Kaunas, 2024, 56 psl.

Reikšminiai žodžiai: VPN, sauga, vėjo jėgainės.

Baigiamajame darbe analizuojamas vėjo jėgainių valdymo sistemos kompiuterinis tinklas, įvertinamas tinklo kibernetinės saugos pažeidžiamumo lygis, taip pat, analizuojamas tinklo įrenginių kibernetinio saugumo lygis ir perkuriamas esamas tinklas į saugų tinklą. Išanalizavus esamą tinklą, pateikiami sprendimų būdai, kaip padidinti saugumo lygį visai infrastruktūrai. Kompiuterių tinklų infrastruktūra pakeičiama panaudojant VPN galimybes, tinklo įrenginiai apsaugomi naujais slaptažodžiais, sudarytais pagal naujai nustatytą slaptažodžių politiką. Įgyvendinamos atakų prevencijos funkcijos, prieigos blokavimo funkcijos. Rezultatas pasiektas toks, kad pritaikant visas siūlomas saugias technologijas, tinklo kibernetinio pažeidžiamumo balas sumažėja daugiau nei 2 kartais.

SUMMARY

Author Julius Skuolevičius. *Secure Network Project for the Wind Turbin Control System*. Graduation Thesis. Supervisor PhD Dangis Rimkus. Kauno kolegija HEI, Faculty of Technologies, Department of Informatics and Media Technologies. Kaunas, 2024, 56 pages.

Keywords: VPN, security, wind turbines.

In the thesis, the computer network of the wind turbine control system is analyzed, the network cyber security vulnerability level is assessed, the cyber security level of the network devices is also analyzed and the existing network is rebuit into a secure network. After analyzing the existing network, solutions are provided to increase the level of security for the entire infrastructure. The infrastructure of computer network is changed using VPN capabilities, network devices are protected with new passwords created according to the newly established password policy. Attack prevention functions, access blocking functions are implemented. The result is that when applying all the proposed safe technologies, the cyber vulnerability score of the network descreases more than 2 times.

ĮVADAS

Darbo aktualumas. Šiuolaikiniame pasaulyje, įmonių saugus kompiuterinis tinklas yra tapęs esminiu veiksniu, kuris nulemia ne tik operatyvų, nepertraukiamą įmonės darbo vykdymą, bet ir pačio verslo sėkmę. Įmonė, administruojanti nutolusio vėjo jėgainių parko kompiuterinio tinklo įrangą, privalo užtikrinti galimybę saugiai pasiekti tinko įrangą iš nuotolio, kad būtų galima stebėti jos darbą, atlikti konfigūracijų pakeitimus, be įsilaužimo ar duomenų pažeidimų rizikos. Taip pat, įmonė privalo užtikrinti tinklo prieinamumą, nes bet koks tinklo sutrikimas, neveikimas turi didelės įtakos įmonės pelningumui. Kibernetiniai išpuoliai prieš tinklo įrenginius gali sutrukdyti sklandų vėjo jėgainių parko darbą, galimi sistemos sutrikimai įmonei reiškia piniginius nuostolius. Saugus tinklas privalo užtikrinti nepertraukiamą duomenų siuntimą, įrenginiai privalo būti atsparūs įvairioms kibernetinėms atakoms, tokių būdų surinkti reikalingi duomenys bus siunčiami nepertraukiamai, įmonė nepatirs finansinių nuostolių.

Darbo problema. Įmonė, kuri administruoja nutolusį vėjo jėgainių kompiuterinį tinklą naudojama nesaugias technologijas, kurios kelią didelį pavojų nepertraukiamam kompiuterinio tinklo darbui. Tinklas diegtas nesilaikant kibernetinio saugumo reikalavimų, nebuvo vadovautasi gerąją kibernetinės saugos praktika. Norint išvengti galimų sėkmingų atakų prieš tinklo įranga, privaloma tinklą rekonstruoti nuo pagrindų, apimant nuotolinės įrangos pasiekiamumo technologijas bei pačio įrenginio vidines konfigūracijas.

Darbo objektas. Nutolusio vėjo jėgainių parko valdymo sistemos tinklo bei tinklo įrenginių sauga.

Darbo tikslas – sukurti vėjo jėgainių valdymo sistemos saugaus tinklo projektą, panaudojant industrinius bevielio ryšio 4G technologijos maršrutizatorius, kurie užtikrins didžiausią įmanomą tinklo apsaugą nuo kibernetinio saugumo grėsmių.

Darbo uždaviniai:

1. Išanalizuoti esamą įmonės administruojamą kompiuterinį tinklą bei šiuo metu naudojamas technologijas, pasiekti tinklo įrangą iš nuotolio.
2. Išanalizuoti tinklo įrenginių vidinius nustatymus, nustatyti tinklo kibernetinio pažeidžiamumo riziką.
3. Suprojektuoti naują tinklą įvertinant tinkamas technologijas bei įrankius, skirtus užtikrinti administruojamo tinklo saugumą, atsižvelgiant į specifinius vėjo jėgainių parko kompiuterinio tinklo įrenginių valdymo reikalavimus.
4. Suprojektuoti atitinkamus tinklo įrenginių vidinių nustatymų pakeitimus, kurie sumažins įrangos kibernetinio pažeidžiamumo riziką.

5. Įgyvendinti sprendimus, kurie užtikrins projektuojamojo tinklo bei tinklo įrangos didžiausią įmanomą kibernetinę apsaugą.
6. Atlikti ekonominių skaičiavimų įvertinimus.

Rezultatai. Išanalizavus tinklą, nesaugios technologijos, skirtos pasiekti nutolusią tinklo įrangą, pakeičiamos saugiomis, įrenginiuose pritaikomi saugumo sprendimai, taip apsaugant ne tik patį tinklą, bet ir tinklo įrenginius. Pritaikius saugias priemones bei technologijas, sukuriant atitinkamas saugumo politikas, sumažinama kompiuterinio tinklo kibernetinio pažeidžiamumo rizika.

1. ANALITINĖ DALIS

Šiuo metu internetinės galimybės pasaulyje yra išnaudojamos labai plačiai – nuo kasdienio naršymo socialiniuose tinkluose, iki surinktų duomenų, iš nutolusių ir lengvai nepasiekiamų objektų, perdavimo į atitinkamus duomenų centrus tolesnei jų analizei. Tiek naršant socialiniuose tinkluose, tiek valdant tinklo įrangą, privalu užtikrinti gerą kibernetinio saugumo profilaktiką, norint, kad darbas būtų nepertraukiamas ir sklandus. Siekiant užtikrinti kuo didesnį įmonės administruojamą nutolusio vėjo jėgainių parko kompiuterinio tinklo saugumą, reikia atsižvelgti į esamą situaciją ir išanalizuoti dabar naudojamas technologijas bei pačią tinklo įrangą, taip pat galimas grėsmes.

Įmonės administruojamą vėjo jėgainių parką sudaro 5 vėjo jėgainės, prie kurių yra prijungta po vieną maršrutizatorių. Prie maršrutizatoriaus lokaliai yra prijungtas sensorius, kuris kaupia bei perduoda duomenis apie vėjo malūno darbą. Duomenys yra įvairių tipų, tokie kaip, vėjo greitis, vėjo kryptis, temperatūra ir slėgis, vėjo greičio pokyčiai, elektros generavimo duomenys. Šie duomenys vėliau panaudojami priimant tinkamus sprendimus dėl vėjo jėgainės veiklos optimizavimo, priežiūros bei efektyvumo. Vienas įmonės kompiuterinių tinklo inžinierius administruoja 5 vėjo jėgainėse esančius kompiuterinio tinklo įrenginius. Tinklo inžinierius privalo stebėti tinklo įrangos darbą, esant poreikiui, atlikti tinklo įrangos konfigūracinius pakeitimus.

Šiuo metu įmonė „X“ administruoja vieną vėjo jėgainių parką, sudarytą iš penkių vėjo jėgainių, tačiau ateityje, administruojamų objektų skaičius didės. Įmonės politika diktuoja, kad tinklo inžinieriai privalo dirbti iš ofiso, todėl prie vėjo jėgainių tinklo įrangos, tinklų inžinierius privalo jungtis tik iš darbo vietos.

Analizuojant šią situaciją, būtina atkreipti dėmesį į tai, kad tinklo elementai, esantys objektuose, yra sunkiai prieinami fiziškai ir jų priežiūra, monitoringas, privalo būti atliekamas prisijungiant iš nuotolio, o ne lokaliai. Lokaliai įrenginiai yra pasiekiami tik tada, kai būna pristatytas užsakymas. Juos galima sukonfigūruoti bei įmontuoti į objektus jau su pilnai įgyvendintomis konfigūracijomis. Įkėlus įrenginį į objektą, jį pasiekti lokaliai galima tik keliais atvejais. Pirmasis atvejis būtų, kai yra atliekami iš anksto suplanuoti vėjo jėgainės priežiūros bei tvarkymo darbai. Antrasis atvejis yra kai tinklo įrenginys tampa visiškai nebepasiekiamas bei surinkti duomenys nebesiunčiami – tokiu atveju yra iškarto statomas naujas tinklo įrenginys ir analizuojama kas nutiko senajam. Pastarojo atvejo rekomenduojama stipriai vengti, nes tai reiškia įmonei nenumatytas išlaidas, todėl tinklo įranga turi būti patikima.

Galiausiai, svarbu atsižvelgti į faktą, kad tinklo įrenginiai turi būti pasiekiami visada, todėl negalima pasikliauti vienu būdu pasiekianti įrenginius iš nuotolio. Privaloma pasiruošti scenarijams kaip tinklo įrenginiai bus pasiekiami iš nuotolio, jei pagrindinė naudojama technologija nustos veikti.

1.1. Technologijų ir technikos apžvalga

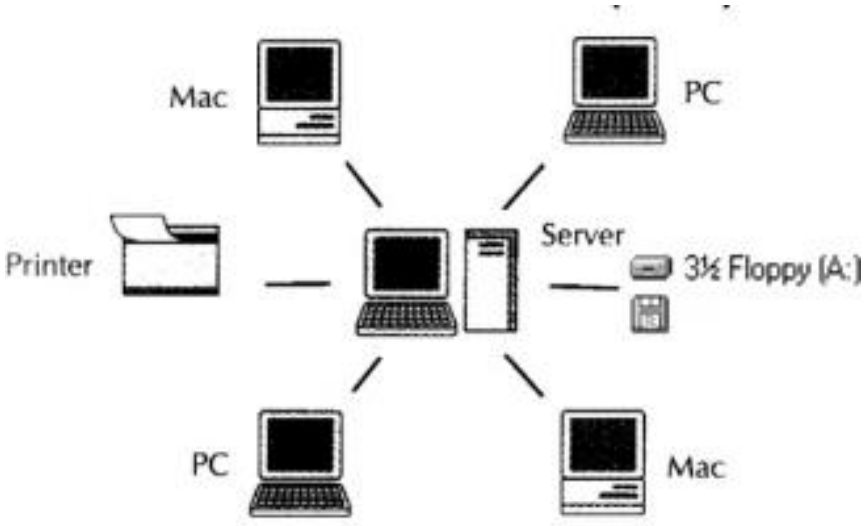
Prieš pradedant pačio objekto analizę, būtina apžvelgti esamas bei galimas technologijas.

Kompiuterinis tinklas – komunikacijų tinklas, leidžiantis įrenginiams keistis duomenimis, pagal tam tikras taisykles, vadinamas protokolais. Duomenims perduoti, pirmiausia turi būti atitinkamos techninės įrangos sąlygos. Duomenys gali būti perduodami laidinėmis priemonėmis, optinėmis priemonės ar radijo ryšio linijomis. Žinomiausias kompiuterinis tinklas yra internetas. Tinklo įrenginiai, kurie sukuria, nukreipia ir priima duomenis yra vadinami tinklo mazgais. Kompiuteriniai tinklai vieni nuo kitų skiriasi duomenų perdavimui naudojamoms technologijoms bei protokolais (Ahlawat, Anand, 2014).

Dažniausiai kompiuteriniai tinklai skirstomi į:

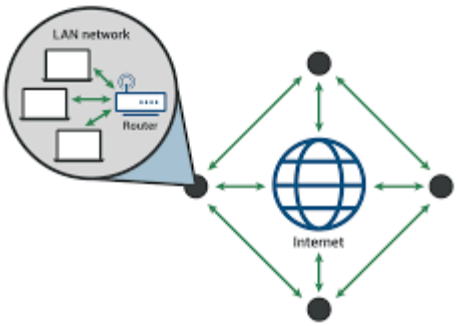
- Vietinis tinklas (LAN – angl. *local area network*);
- Globalusis tinklas (WAN – angl. *wide are network*).

Vietinis tinklas (LAN) apima nedidelį plotą žiūrint iš geografinės pusės, tokią kaip kambario, namo ar ofiso aukšto teritorija. Vietiniam tinkle yra bendrinami ištekiai ir informacija tarp skirtingų įrenginių, tokių kaip kompiuteriai, serveriai, spausdintuvai ir panašiai, tai leidžia tinklo vartotojams dalintis failais, spausdinti dokumentus, bei apskritai komunikuoti su kitais įrenginiais, esančiais tame pačiame vietiniame tinkle. Vietinis tinklas dažniausiai būna sujungtas panaudojant laidus, tokius kaip eterneto (angl. *Ethernet)* kabelius, kurie jungia įrenginius į centrinį maršrutizatorių, tiesiogiai arba per vieną ar kelis komutatorius. LAN tinklo schema atvaizduojama 1.1 paveiksle.



1.1 pav. LAN tinklas (router-switch.com, 2018)

Globalusis tinklas (WAN) apima didelį plotą žiūrinti iš geografinės pusės. Globalusis tinklas sujungia skirtingus vietinius tinklus ar įmones, ar organizacijas, ar net ištisas šalis tarpusavyje. WAN naudojamas duomenims perduoti ir gauti su kitais vartotojais, neatsižvelgiant į jų geografinę buvimo vietą, jei tik jie turi prieigą prie tam tikro WAN tinklo. Prieiga gali būti suteikta per virtualius privačius tinklus (VPN), belaidžius tinklus ir kitus tinklų tipus. Šis tinklas yra labai svarbus ne tik tarptautiniam verslui, bet ir kasdieniam naudojimui, nes internetas yra laikomas didžiausiu WAN tinklu pasaulyje (Comptia.org, n.d). WAN tinklo schema pavaizduojama 1.2 paveiksle.



1.2 pav. WAN tinklas (cloudflare.com, n.d**)**

Tinklo įrenginiai tarpusavyje komunikuoja naudodami IP adresus, per skirtingus protokolus, priklausomai nuo panaudojimo srities. IP adresas yra unikalus adresas, skirtas konkrečiam prietaisui, kuris yra prijungtas tinkle. IP adresai skirstomi į viešuosius IP adresus bei privačiuosius IP adresus.

Viešieji IP adresai yra unikalūs adresai, kuriais įrenginys yra identifikuojamas internete. Šie adresai yra pasiekiami iš išorinio tinklo ir naudojami komunikacijai tarp įrenginių internete. Šie adresai yra pasiekiami iš bet kurio įrenginio, turinčio interneto prieigą.

Privatūs IP adresai naudojami privačiuose tinkluose ir nėra tiesiogiai pasiekiami iš interneto. Šie adresai naudojami lokaliuose tinkluose, taip pat, siekiant apsaugo tinklo įrenginius nuo tiesioginės prieigos iš išorinio tinklo vartotojų.

1.2. Kibernetinių atakų prieš tinklo įrenginius analizė

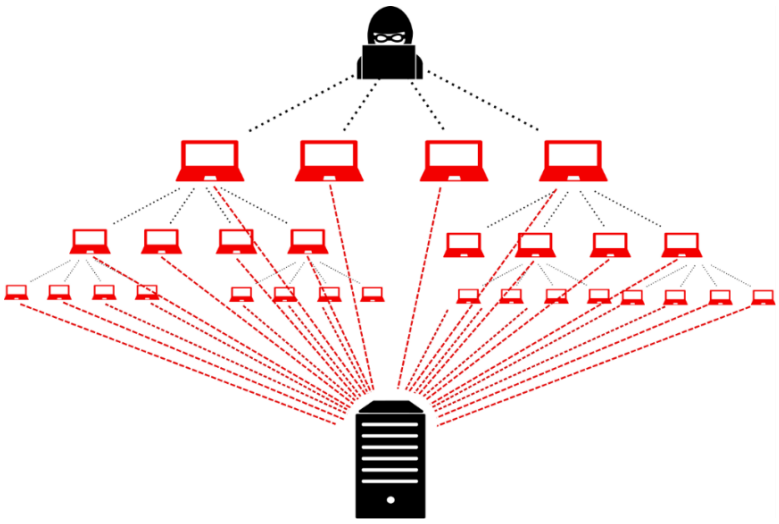
Kibernetinės atakos prieš tinklo įrenginius gali sužlugdyti įmonės veiklą. Pavojingiausios ir daugiausiai žalos sukeliančios kibernetinės atakos šiai įmonei, kuri administruoja nutolusią vėjo jėgainių tinklo įranga, yra šios:

- Neteisėta prieiga prie tinklo įrenginių vykdant slaptažodžių atakas;
- DDoS atakos;
- MitM atakos.

Neteisėta prieiga prie tinklo įrenginių vykdant slaptažodžių atakas gali sukelti negrįžtama žalą kompiuterinių tinklų įrenginiams. Pasak Tasevski (2015), atakos prieš slaptažodžius yra vienas iš lengviausių ir paprasčiausių atakų vektorių. Sėkmingai įvykdžius šią ataką, užpuolikas gali prisijungti prie informacinės sistemos neteisėtai. Yra žinoma skirtingų metodų, kuriais bandoma atspėti slaptažodžius. Dažniausiai šie metodai būna automatizuoti, pasitelkiant jau sukurtas ir viešai prieinamas programas arba įsilaužėliai patys susikurią programą, pagal specifinį objektą, kurį bandomą nulaužti. Yra pasitelkiami tokie atakų metodai, kaip žodyno atakos, hibridinės žodyno atakos ar brutalios jėgos (angl. *brute force*) atakos. Jei šios atakos įvykdomos sėkmingai, įsilaužėlis gauna prieiga prie tinklo įrenginio ir gali atlikti veiksmus, įrenginyje, pagal nulaužto vartotojo teises.

DDoS atakos metu būna pažeistas duomenų prieinamumas. DDoS atakos metu kibernetinis nusikaltėlis bando užkrauti auką (pvz. serverį ar kito tinklo įrangą) siunčiamomis užklausomis ir jeigu auka neatlaiko gaunamų užklausų kiekio, ji tampa neveiksni (Bendovschi, 2015).

Sėkmingai įvykdžius šią ataką prieš tinklo įrenginius, jie taptų nebepasiekiami iš nuotolio ir tai sukeltų didelių finansinių nuostolių, nes nebūtų įmanoma užtikrinti reikalingų duomenų siuntimo iš objektų. DDoS atakos atvaizdavimas matomas 1.3 paveiksle.



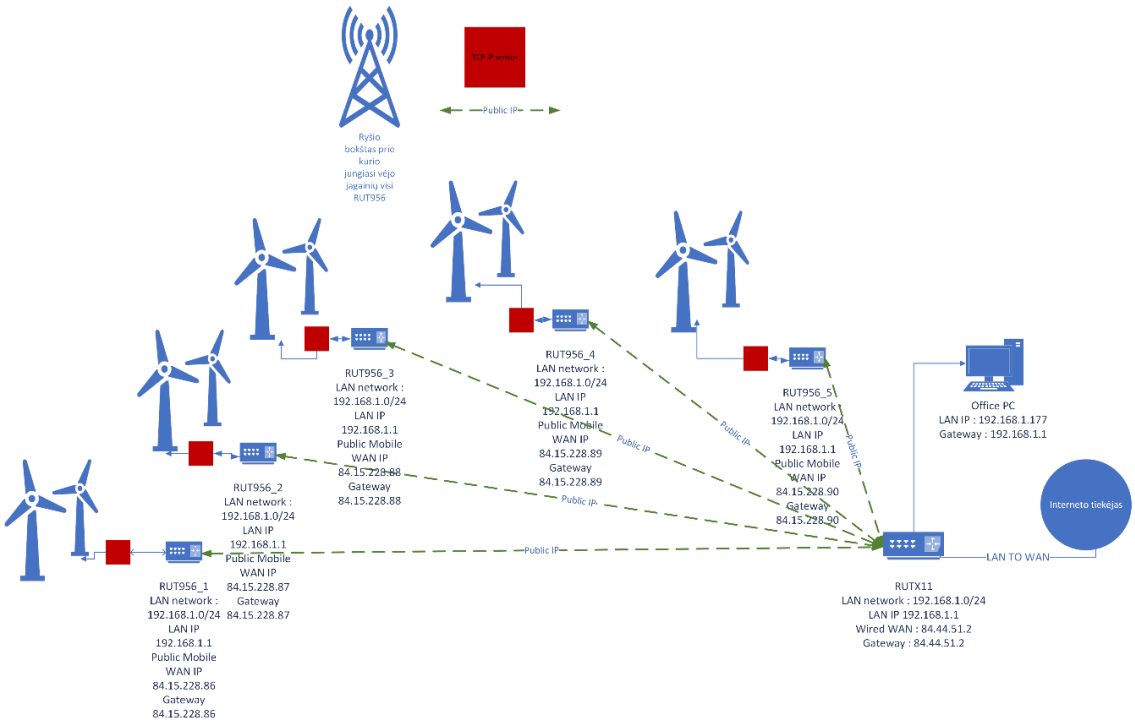
1.3 pav. DDoS atakos atvaizdavimas (ruggedtooling.com, 2018)

MitM ataka įvyksta, kai kibernetinis nusikaltėlis įsiterpia tarp dviejų įrenginių komunikacijos galų, rezultate visi duomenys siunčiami iš taško A į tašką B, pasiekia pirmiausią užpuoliką, o ne paskirties vietą. Šią ataką sėkmingai įvykdžius, užpuolikas gauna neleistiną prieigą prie neskelbtinos informacijos arba užpuolikui atsiranda galimybė modifikuoti ar sunaikinti siunčiamus duomenis (Bendovschi, 2015).

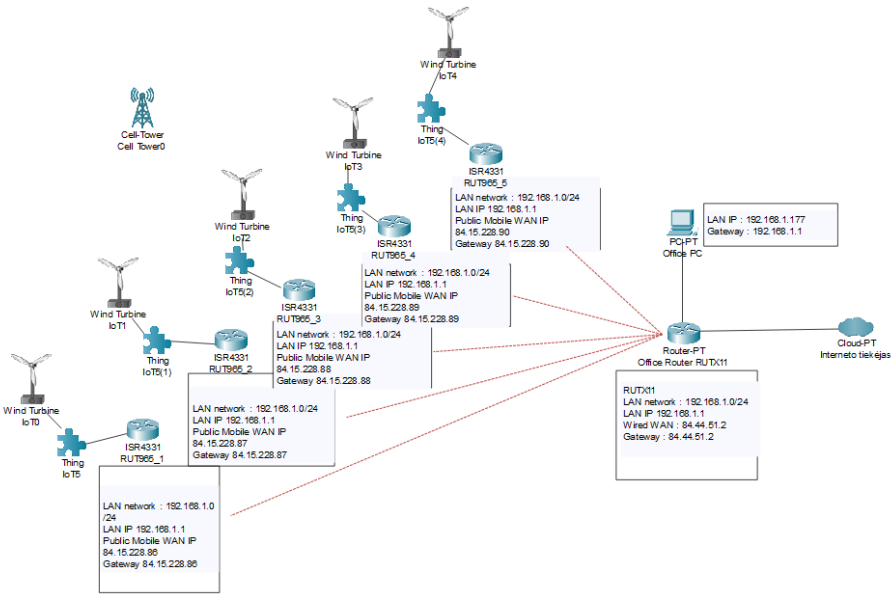
Surinktų ir siunčiamų duomenų teisingumas bei konfidencialumas yra svarbūs kriterijai, kad įmonė galėtų teisingai apdoroti gaunamus duomenis ir pagal juos priimti tolimesnius strateginius sprendimus.

1.3. Esamo administruojamo objekto tinklo įrangos analizė

Tinklų inžinierius, nutolusią tinklo įrangą, pasiekia atvykęs į savo darbą, iš savo darbinio kompiuterio. Prie darbinio kompiuterio, yra prijungtas maršrutizatorius, kuris teikia internetą. Nutolę įrenginiai yra pasiekiami per jų viešuosius IP adresus. Taip tinklo inžinierius pasiekia visus 5 nutolusius įrenginius ir gali prisijungti prie jų grafinės sąsajos ar komandinės eilutės sąsajos. Esamo tinklo topologija atvaizduojama 1.4 ir 1.5 paveiksluose.



1.4 pav. Esama administruojama vėjo jėgainių tinklo topologija „Microsoft Visio“ programoje



1.5 pav. Esamos tinklo topologijos atvaizdavimas „Packet Tracer“ programoje

Prie darbinio kompiuterio yra prijungtas Teltonika „RUTX11“ maršrutizatorius, o į vėjo jėgaines yra įkelti Teltonika „RUT956“ maršrutizatoriai. Prie kiekvieno maršrutizatoriaus yra prijungtas sensorius, kuris kaupia įvairius duomenis apie vėjo jėgainės darbą, bei siunčia šiuos duomenis į atitinkamą galinį tašką. Abiejų maršrutizatorių gamintojų tinklo įranga yra pritaikyta specialiai tokioms vietoms, kur neįmanoma panaudoti verslo ar namų klasės tinklo įrangos. Būtina paminėti, kad tinklo įranga, kuri yra sumontuota vėjo jėgainėse, negali gauti prieigos į išorinį tinklą per WAN iš interneto paslaugų operatorių jungiant fiziškai laidu, todėl ši tinklo įranga veikia su SIM kortelėmis ir taip ji gali siųsti bei gauti duomenis iš išorinio tinklo. Naudojama įranga yra tinkama, nes darbinė temperatūrą atlaiko tiek žemą temperatūrą, tiek labai aukštą temperatūrą, taip pat kitus aplinkos faktorius, kaip drėgmė, dulkės, prie kurios dauguma verslo bei namų klasės tinklo įrangos nustotų veikti. Įrangos aparatūrinės specifikacijos pateikiamos 1 lentelėje.

1 lentelė. Įrangos aparatūrinės specifikacijos (Sudaryta autoriaus pagal Teltonika-Networks.com pateikiama informaciją, 2024)

Įranga / **Specifikacijos**	**Teltonika „RUTX11“**	**Teltonika „RUT956“**
LAN prievadai	3x10/100/1000 Mbps, RJ-45	3x10/100 Mbps, RJ-45
WAN prievadai	1x x10/100/1000 Mbps, RJ-45	1x10/100 Mbps, RJ-45
SIM kortelių skaičius	2x	2x
RS232 jungtis	0	1x
RS485 jungtis	0	1x
Mobiliojo ryšio technologijos	Palaiko 4G (LTE CAT6), 3G, 2G ryšio standartus	Palaiko 4G (LTE CAT4), 3G, 2G ryšio standartus
Palaikomos darbinės temperatūros rėžiai	-40 °C iki 75 °C	-40 °C iki 75 °C
Užmaitinimo įėjimo įtampos diapazonas	9 iki 50 VDC	9 iki 30 VDC
Įrangos nuotrauka		

1.4. Esamo administruojamo objekto tinklo įrenginių konfigūracijos analizė

Visi RUT956 įrangos nustatymai yra palikti numatytieji, tai reiškia, kad LAN adresai nutolusioje įrangoje yra visi po tuo pačiu potinkliu – 192.168.1.0/24. Tai reiškia, kad yra 254 galimų IP adresų, įrenginiams prijungtiems į objekto LAN tinklą. Taip pat, RUTX11 maršrutizatoriaus, prie kurio šiuo metu yra prijungtas tik vienas kompiuteris, LAN potinklis yra 192.168.1.0/24. Visi tinklo įrenginių numatytieji tinklo parametrai pateikiami 2 lentelėje.

2 lentelė. Tinklo įrenginių numatytieji tinklo parametrai

	LAN potinklis bei kaukė	LAN IP	WAN IP	Išėjimo į išorinį tinklą IP
RUT956_1	192.168.1.0/24	192.168.1.1	84.15.228.86	84.15.228.86
RUT956_2	192.168.1.0/24	192.168.1.1	84.15.228.87	84.15.228.87
RUT956_3	192.168.1.0/24	192.168.1.1	84.15.228.88	84.15.228.88
RUT956_4	192.168.1.0/24	192.168.1.1	84.15.228.89	84.15.228.89
RUT956_5	192.168.1.0/24	192.168.1.1	84.15.228.90	84.15.228.90
RUTX11	192.168.1.0/24	192.168.1.1	84.44.51.2	84.44.51.2

Prisijungę prie vieno iš įrenginių grafinės sąsajos įsitikiname, kad jo LAN ir WAN IP adresai yra teisingi. Prie RUT956_1 įrenginio prisijungiame per jo viešąjį IP adresą ir grafinėje sąsajoje susirandame tinklo LAN bei WAN tinklo nustatymus (žr. 1 priedą).

Šiuo metu, prie kiekvieno RUT956 maršrutizatoriaus objekte yra prijungtas tik vienas LAN įrenginys, o prie RUTX11 prijungtas taip pat tik vienas kompiuteris į LAN tinklą, tai reiškia, kad kiekviename maršrutizatoriuje yra 254 galimų IP adresų LAN įrenginiams. Palikti tokios didelės apimties potinklius, kai jungiama labai mažai įrenginių į lokalų tinklą, nėra gera mintis, nes tai sukuria papildomą saugumo spragą. Kai dauguma IP adresų potinklyje yra nenaudojami, naudojami adresai tampa potencialiai pažeidžiami. Įsilaužėliams gali tapti lengviau sužinoti tinklo struktūrą ir surasti vienintelį prijungtą tinklo įrenginį. Geroji kibernetinio saugumo praktika diktuoja, kad geriausia būtų naudoti potinklio kaukę tokią, kuri apribotų prijungtų įrenginių kiekį iki lengvai valdomo skaičiaus (FasterCapital, 2024).

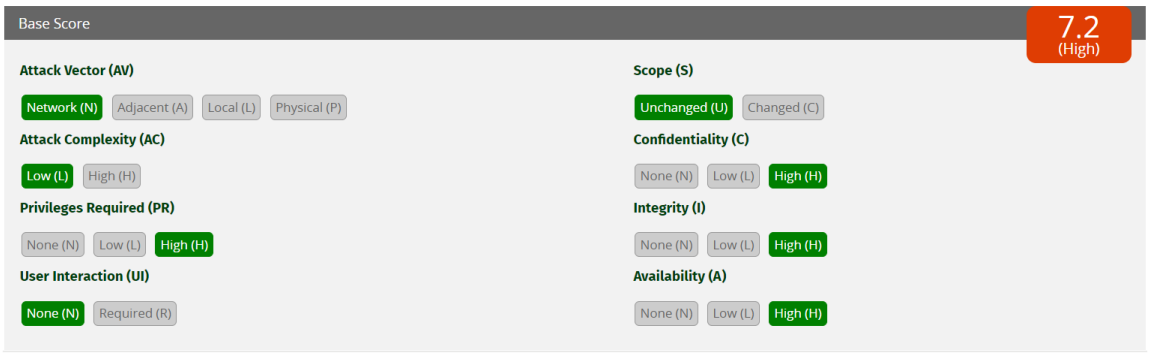
Taip pat, kadangi naudojama įranga yra su numatytomis konfigūracijomis, jos ugniasienė taip pat nėra pritaikyta atitinkamai pagal įrenginių panaudojimo sritį, tai taip pat palieka vietos kibernetinės grėsmėms. Galiausiai, dėl tos pačios priežasties, įrenginių prisijungimo slaptažodžiai taip pat naudojami nesaugūs, tai sukuria idealią terpę įvykdyti sėkmingas kibernetines atakas prieš tinklo įrenginius. Įrenginio RUT956 ugniasienės nustatymai bei naudojamas slaptažodis matomas 2 priede.

Kaip ir minėta ankščiau, tinklo įranga pasiekiama per viešuosius statinius IP adresus, kurie yra priskiriami interneto tiekėjo, per įdėtą SIM kortelę į tinklo įrangą. Tai reiškia, kad tinklo įrangą gali pasiekti bet kas, turintys prieigą prie išorinio interneto, o ne tik tinklų inžinierius, kuris privalo

administruoti nutolusius tinklo įrenginius. Kadangi įrenginiai dirba su numatytosiomis konfigūracijomis ir yra pasiekiami iš išorinio tinklo kiekvieną dieną, visą parą nepertraukiamai, įrangą tampa lengvas taikinys kibernetiniams nusikaltėliams. Nusikaltėliai gali pasiekti įrangą per viešąjį IP adresą ir bandyti atspėti slaptažodžius, pasinaudojant tam tikru slaptažodžių atspėjimo būdų, taip pat, nusikaltėliai gali užkrauti įrangą vykdant DDoS atakas ir perrimti informaciją vykdant MitM atakas (Kaspersky LAB, 2018; pgitl.com, 2023).

1.5. Tinklo pažeidžiamumo įvertinimas *CVSS* sistemoje

Bendroji pažeidžiamumo vertinimo sistema (angl. *CVSS*) yra viešai prieinama platforma, kurioje galima sužinoti apie aparatūrinės bei programinės įrangos pažeidžiamumus, taip pat, galima nustatyti pažeidžiamumo svarbą, pagal gautą įvertinimo balą (first.org, n.d). Įvertinus bei nustačius esamo tinklo pažeidžiamumo vektorių reikšmes, gautas įvertinimas lygus 7,2 balo. Nustatomas vektorius bei galutinis balas atvaizduojamas 1.6 paveiksle.



1.6 pav. Nustatytas vektorius bei galutinis balas

Gautas aukštas vektoriaus balas, nurodantis, kad sistema yra nesaugi bei pažeidžiama. Detalūs vektorių pasirinkimo paaiškinimai pateikiami 4 priede.

1.6. Kibernetinės saugos technologijų bei įrankių analizė

Norint užtikrinti, kad tinklas būtų saugus nuo anksčiau išvardintų atakų, reikalinga apžvelgti kokios technologijos bei įrankiai padėtų tai įgyvendinti. VPN technologija, saugių slaptažodžių politika bei atitinkamas ugniasienės konfigūravimas, galėtų padėti užkirsti kelią minėtoms atakoms.

VPN technologija yra esminis įrankis, galintis užtikrinti saugumą internete bei atstoti šiuo metu naudojamus viešuosius IP adresus. VPN yra virtualus privatus tinklas, kurį galima sukonfigūruoti, kad veiktų tiek lokaliam tinkle, tiek išoriniam tinkle – internete, siekiant apsaugoti

konfidencialius duomenis, kurie yra siunčiami tinkle. Naudodami VPN, galime sukurti apsaugotą komunikacijos terpę tarp tam tikrų įrenginių, kuriuos patys pridedame į virtualų privatų tinklą (Kaur, Sharma, 2020).

Taip pat, VPN gali atstoti viešuosius IP adresus, tokiu būdu, ne bet kas galėtų pasiekti tinklo įrenginius iš išorinio tinklo. VPN veikia kaip tarpininkas, užmaskuodamas įrenginių IP adresus ir peradresuodamas visą duomenų srautą. Taip pat, VPN užšifruoja duomenų srautą, kuris eina per VPN tunelį, todėl galima teigti, kad toks VPN serverio ir šifruoto tunelio derinys neleidžia interneto paslaugų tiekėjui, įsilaužėliams ar kitiems asmenims šnipinėti bei bandyti nulaužti įmonės įrenginių iš išorinio tinklo.

Slaptažodžių politika – taisyklių rinkiniai, kurie nurodomi naudotojui, siekiant, kad jų būtų laikomasi, kuriant bei naudojant slaptažodžius. Slaptažodžių politika nustato, kokie simboliai turėtų būti naudojami, kokio ilgo slaptažodis turėtų būti, taip pat, tipą ir formatą slaptažodžio. Šios politikos taikomos siekiant padidinti bei užtikrinti įrenginių ar paskyrų saugumą, naudojant sudėtingus slaptažodžius (Hussain, 2022). Rekomendaciniai patarimai, kuriant saugų slaptažodį (microsoft.com, n.d):

- Naudoti mažiausiai 12 simbolių;
- Kombinacijos didžiųjų bei mažųjų raidžių, skaičių ir specialiųjų simbolių;
- Slaptažodyje neminėti žodžių, kurie randami žodynuose, vardų, vietovių, organizacijų pavadinimų, žaidimų ar filmų personažų.

Rekomendaciniai patarimai saugant slaptažodžius :

- Nesidalinti slaptažodžiais su niekuo;
- Nesiųsti slaptažodžių žinutėmis ar elektroniniu paštu, naudojant nepatikimas bei nesaugias platformas;
- Nenaudoti tų slaptažodžių, kurie buvo naudojami seniau, kituose įrenginiuose ar platformose.

Kaip ankščiau išanalizuota, visi įmonės tinklo įrenginiai naudoja vieną ir tą patį slaptažodį – *Admin123*. Patikrinus slaptažodį su viešai prieinama slaptažodžių tikrinimo programa, paaiškėjo, kad tokį slaptažodį įmanoma nulaužti per 0,34 sekundes dalį. Rezultatas matomas P3.1 paveiksle (žr. 3 priedą).

1.7. Apibendrinimas

Išanalizavus technologijas, naudojamas pasiekti tinklo įrenginius iš nuotolio, taip pat peržvelgus įrenginių nustatymus, įvertinus CVSS pažeidžiamumo balą, galime apibendrinti, kad

naudojamos technologijos bei palikti numatytieji įrenginių parametrai neatitinka kibernetinės saugos gerosios praktikos ir yra paliekama palanki terpė įvykdyti kibernetines atakas. Įrenginius gali pasiekti kas tik nori iš išorinio tinklo, įrenginiai apsaugoti nesaugiais slaptažodžiais.

2. SPECIFIKACIJA

Norinti užtikrinti, kad sukurtas kompiuterinis tinklas atitiks visus specifiškus reikalavimus, reikia išsiaiškinti projektuojamo objekto paskirtį, apibūdinimą, kokius parametrus tinklo įranga privalo atitikti.

Projektuojamo objekto apibūdinimas. Projektuojamas objektas yra vėjo jėgainių valdymo sistemos kompiuterinis tinklas. Kompiuterinį tinklą sudaro 5 nutolę tinklo įrenginiai ir 1 ofiso tinklo įrenginys.

Projektuojamo objekto paskirtis. Vėjo jėgainėse yra kaupiami duomenys apie pačios vėjo jėgainės darbą, efektyvumą. Taip pat yra matuojami aplinkos veiksniai, tokie kaip vėjo greitis, jo kryptis, intensyvumas, atmosferos slėgis, kritulių kiekis. Kaupiami duomenys ir apie techninę būkle. Šie duomenys apima informaciją apie patiriamą vibraciją, vėjo turbinos būklę, veikimo temperatūrą. Visi duomenys yra svarbūs siekiant užtikrinti efektyvų vėjo jėgainės darbą, infrastruktūrinio vieneto saugumą. Šie sukaupti duomenys siunčiami į nutolusį serverį, tolesniam duomenų apdorojimui bei interpretavimui. Duomenims siųsti, reikalinga kompiuterinių tinklų įranga ir interneto prieiga.

Reikalavimai projektuojamo objekto tinklo įrangai. Į vėjo jėgainės įkeliami maršrutizatoriai privalo turėti mažiausiai 3 LAN prievadus, nes numatoma, kad ateityje išvis bus prijungti 3 įrenginiai per LAN prievadus, 2 SIM kortelių vietas, palaikyti 4G mobilųjį ryšį, RS232 ir RS485 jungtis, užmaitinami 9-30 VDC srove bei darbinė temperatūra turi atitikti -20°C iki 70°C rėžį.

Kompiuterinio tinklo įranga privalo būti apsaugoti stipriais slaptažodžiais, vadovaujantys gerąją slaptažodžių naudojimo praktika.

Nutolusius įrenginius pasiekti privalo tik autorizuotas darbuotojas ir tik iš darbinio kompiuterio, prijungto į RUTX11 maršrutizatorių. Daugiau niekas negali turėti prieigos prie įrenginio. Prie RUTX11 įrenginio bus minimaliai prijungti du darbuotojų kompiuteriai.

Įrenginiai privalo palaikyti VPN funkcijas, ugniasienės nustatymų pakeitimų galimybes, integruotas atakų prevencijos funkcijas, numatytojo slaptažodžio pakeitimo galimybę. Turi būti galimybė prisijungti prie įrenginio per komandinę eilutę panaudojant SSH protokolą bei per grafinę sąsają. Įrenginių kaina privalo būti iki 350 eurų už vienetą.

3. PROJEKTINĖ DALIS

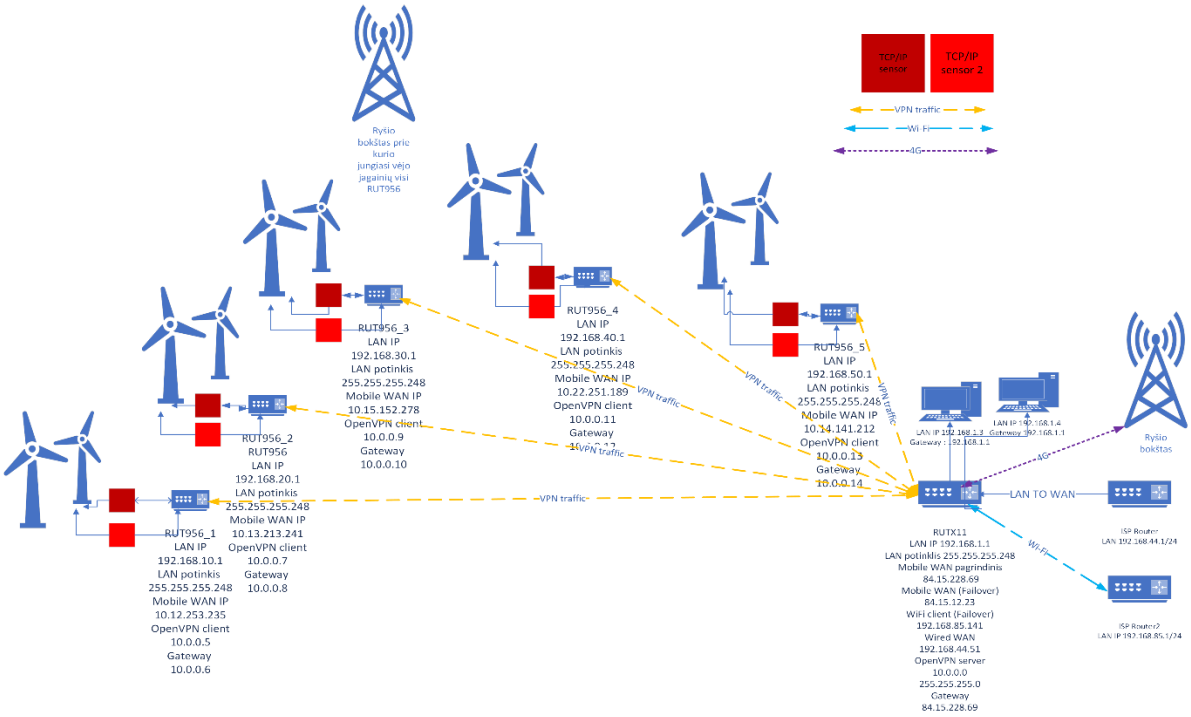
Naujai projektuojamo tinklo nutolę įrenginiai yra pasiekiami per sukonfigūruoto VPN tunelio galinių taškų IP adresus, įrenginių LAN potinkliai pakeičiami į tokius, kurie atitinka planuojamų prijungti įrenginių skaičių, nutolusių įrenginių WAN IP adresas pakeičiamas iš viešojo į privatų, tokiu būdu įrenginių niekas nebegalės pasiekti iš išorinio tinklo. Taip pat, atliekami papildomai konfigūraciniai žingsniai, kurių dėka, nutrūkus interneto ryšiui iš pagrindinės SIM kortelės, įrenginys automatiškai perjungs kitą SIM kortelę, kuri įdėta į maršrutizatorių. Atsarginė SIM kortelė yra su viešuoju IP adresu, tokiu būdu, nebepasiekiamą įrenginį per VPN, būtų galima iš naujo pasiekti per viešąjį IP adresą ir atlikti atitinkamus laikinus konfigūracinius pakeitimus, iki kol bus atstatytas pagrindinės SIM kortelės interneto ryšis.

RUTX11 maršrutizatorius, kuris naudojamas ofiso patalpose suteikti interneto prieigą darbiniui kompiuteriui, sukonfigūruojamas kaip VPN serveris, iš kurio yra pasiekiami VPN klientai, kurie yra nutolę įrenginiai. Taip pat, RUTX11 LAN potinklis pakeičiamas taip, kad galėtų prisijungti tik reikiamas skaičius kompiuterių, WAN IP adresas paliekamas su viešuoju IP adresu, nes VPN serveris visada privalo turėti viešąjį IP adresą, tačiau sukonfigūruojant atitinkamą ugniasienės taisyklę, nustatome, kad niekas negalėtų pasiekti įrenginio, per jo viešąjį IP adresą. Taip pat, kad užtikrinti nenutrūkstama interneto prieigą, sukonfigūruojamos atsarginės WAN sąsajos, kurios persijungs tik nutrūkus interneto ryšiui iš pagrindinės WAN sąsajos.

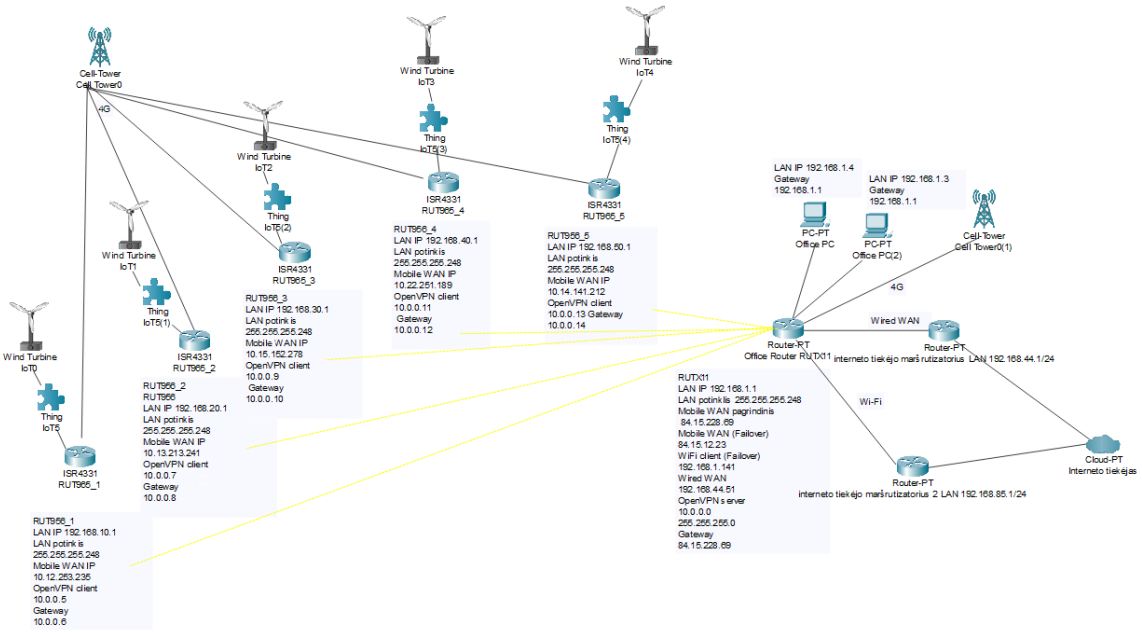
3.1. Projektuojamo objekto rekonstruotas tinklo modelis

Projektuojamo objekto tinklas visiškai restruktūrizuotas, pradedant LAN potinklių keitimu, WAN IP adresų pakeitimų iš viešųjų į privačius ir sukonfigūruojant VPN sąsajas. Nutolusios įrangos viešieji WAN IP adresai buvo pakeisti privačiais IP adresais, tokiu būdų niekas nebegalės pasiekti tinklo įrangos iš išorinio tinklo. Vietoj viešųjų IP adresų, yra pasitelkiama VPN technologija. Ofiso maršrutizatorius RUTX11, sukonfigūruotas kaip *OpenVPN* serveris, o nutolę tinklo įrenginiai RUT956 sukonfigūruoti kaip *OpenVPN* klientai. Tokiu būdu, yra padaromas visiškai naujas privatus virtualus tinklas. Kiekvienas tinklo įrenginys įgauna VPN adresus ir per tuos VPN adresus kiekvienas tinklo įrenginys yra pasiekiamas iš darbinio kompiuterio, kuris prijungtas į *OpenVPN* serverį, RUTX11 maršrutizatorių. Nutolę tinklo įrenginiai yra nebepasiekiami neautorizuotiems asmenims, iš išorinio tinklo, juos gali pasiekti tik autorizuotas tinklo inžinierius, iš savo darbo vietos, darbinio kompiuterio. Tai stipriai pagerina nutolusių įrenginių saugumą, užtikrina, kad tinklo įrenginiai yra nepažeidžiami iš išorės. Tik ofiso patalpose esantis maršrutizatorius paliktas su viešuoju IP adresu, nes to reikalaujama konfigūruojant *OpenVPN* serverį, tačiau buvo imtasi papildomų veiksmų,

leidžiančių taip pat užkardyti prieiga prie šio įrenginio neautorizuotiems asmenims iš išorinio tinklo. Projektuojamojo objekto topologija atvaizduojama 3.1 ir 3.2 paveiksluose.



3.1 pav. Projektuojamo objekto topologija „Microsoft Visio“ aplinkoje



3.2 pav. Projektuojamo objekto topologija „Packet Tracer“ programoje

Taip pat, iš tinklo konfigūracinės pusės, pakeisti LAN potinkliai iš prieš tai buvusių, tiek nutolusiems įrenginiams, tiek ofiso tinklo įrenginiui. Uždėti specifinius reikalavimus atitinkantys

LAN potinkliai, tokiu būdų mažinama kibernetinės grėsmės rizika ir didinimas geresnis įrenginių monitoringo bei atpažinimo procesas.

Galiausiai, ofise buvo pridėti du papildomi interneto paslaugų tiekėjo maršrutizatoriai, kurie suteikia atsarginę interneto prieigą RUTX11 maršrutizatoriui. To reikia tam, kad jei nutrūktų pagrindinis interneto ryšis, darbuotojų kompiuteriai neprarastų prieigos prie interneto. Įmonė, kuri administruoja nutolusius tinklo įrenginius, neturi jokios prieigos prie interneto tiekėjo maršrutizatorių, išskyrus prijungimo į ofiso maršrutizatorių veiksmų. Į RUTX11 internetą tiekia laidu prijungtas vienas interneto tiekėjo maršrutizatorius. Kitas interneto tiekėjo maršrutizatorius veikia kaip bevielės interneto prieigos taškas ir į jį yra jungiamasi per Wi-Fi. Interneto paslaugų tiekėjas nustatęs maršrutizatorių potinklius, tokius, kad potinkliai nekonfliktuotų su RUTX11 įrenginio potinkliais, tokiu būdu, IP nekonfliktuos ir duomenų srautas nebus paveiktas ar nutraukiamas. Visų įrenginių LAN, WAN IP adresai pateikiami 3 lentelėje.

Visi LAN potinkliai nustatyti taip, kad atitiktų kriterijus, nurodytus specifikacijos dalyje. Tai reiškia, kad prie kiekvieno nutolusio RUT956 įrenginio bus prijungti trys įrenginiai, fiziškai jungiant kabelį iš įrenginio į RUT956 LAN prievadą. Tai reiškia, kad LAN potinklio kaukė turi būti nustatyta būtent tokia, kad prijungtiems įrenginiams, būtų paskirtas vietinio tinklo IP adresas.

Prie RUTX11 bus jungiami minimaliai du darbuotojų kompiuteriai, todėl potinklis pasirinktas taip pat toks, kad būtų teisingai paskirstyti IP adresai ir neatsitiktų taip, kad neužteks IP adresų prijungtiems darbuotojų kompiuteriams. Visa informacija apie reikiamą IP adresų skaičių, bei diapazonas, pagal kurį galime matyti kiek IP adresų įrenginys gali priskirti į vietinį tinklą jungiamiems įrengiam pateikiami 4 lentelėje.

Svarbu pabrėžti, kad potinkliai turi būti atsakingai parenkami. Jeigu potinklis bus parinktas neteisingas, įrenginiai, kurie bandys jungtis prie maršrutizatoriaus patirs įvairių problemų. Jungiamas įrenginys gali neprisijungti prie tinklo, nes paprasčiausiai negaus IP adreso, to rezultate, įrenginys negaus interneto prieigos bei negalės naudotis kitais tinklo ištekliais. Taip pat, gali pasitaikyti IP konfliktų scenarijus. Tai atsitinka, kai įrenginiui bandoma priskirti IP adresą kurį jau kitas įrenginys tame pačiame tinkle turi. Tai sukelia tinklo sutrikimus ir netinkamą veikimą abiejų įrenginių atžvilgiu. Svarbu akcentuoti ir tai, kad jungiami įrenginiai privalo palaikyti IPv4 protokolą, nes įrenginys palaikantis tik IPv6 protokolą, gali sukelti tinklo nesuderinamumo problemų ir įrenginys neprisijungs. Taip pat, jungiamų įrenginių apsaugos nustatymai turi būti nustatyti taip, kad įrenginiai galėtų priimti IP adresų paskyrimą. Visada yra tikimybė, kad jungiamo įrenginio konfigūracijose yra klaidų, dėl kurių jis gali negauti IP adreso iš maršrutizatoriaus, net jeigu maršrutizatorius sukonfigūruotas ir veikia teisingai. Tokiu atveju, reikėtų tvarkyti jungiamą įrenginį, o ne maršrutizatorių. Nepaskirtų IP adresų problemų metu reikia atidžiai išnagrinėti kiekvieną galimą priežastį, kad būtų galima nustatyti iš kur problema atsiranda bei surasti jos sprendimo būdą.

3 lentelė. Administruojamo objekto tinklo įrenginių LAN bei WAN IP adresai bei potinkliai

	RUT956_1	RUT956_2	RUT956_3	RUT956_4	RUT956_5	RUTX11
LAN IP adresas	192.168.10.1	192.168.20.1	192.168.30.1	192.168.40.1	192.168.50.1	192.168.1.1
LAN potinklio kaukė	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248
WAN IP adresas	10.12.253.235	10.13.213.241	10.15.152.278	10.22.251.189	10.14.141.212	84.15.228.69
Laidinio WAN IP adresas	Nėra	Nėra	Nėra	Nėra	Nėra	192.168.44.51
Wi-Fi WAN IP adresas	Nėra	Nėra	Nėra	Nėra	Nėra	192.168.85.141
Išėjimo į išorinį tinklą IP adresas	10.0.0.6	10.0.0.8	10.0.0.10	10.0.0.12	10.0.0.14	84.15.228.69

Trečioje lentelėje matoma, kad LAN IP adresai, kiekvienam nutolusiam įrenginiui padaryti skirtingi. Toks sprendimas buvo priimtas, nes *OpenVPN* klientai, esantys tam pačiam VPN tinkle, privalo turėti skirtingus LAN IP adresus.

4 lentelė. Galimi įrangos LAN IP adresai

	RUT951_1	RUT956_2	RUT956_3	RUT956_4	RUT956_5	RUTX11
Potinklis	192.168.10.0	192.168.20.0	192.168.20.0	192.168.20.0	192.168.20.0	192.168.1.0
Tinklo kaukė	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248	255.255.255.248
Rezervuotas IP adresas tinklo įrenginiui	192.168.10.1	192.168.20.1	192.168.30.1	192.168.40.1	192.168.50.1	192.168.1.1
Galimi IP adresai	5	5	5	5	5	5
Reikiamų IP adresų skaičius	3	3	3	3	3	2
IP adresų diapazonas	192.168.10.2- 6	192.168.20.2- 6	192.168.30.2- 6	192.168.40.2- 6	192.168.50.2- 6	192.168.1.2- 6

Ketvirtoje lentelėje matoma, kad parinktos tinklo kaukės atitinka nurodytus specifinių įrenginių skaičius ir dar lieka vietos rezerviniam įrenginiui, todėl galima teigti, kad potinkliai parinkti teisingi. Svarbu pastebėti, kad vienas IP adresas visada yra užrezervuotas pačiam tinklo įrenginiui. Tas IP adresas yra diapazono pradžios adresas, taigi, iš visų galimų IP adresų, reikia atimti vieną rezervuotą IP adresą ir gauname realų galimų IP adresų skaičių.

3.1.1. Tinklo įrenginių atviri prievadai

Norinti užtikrinti, kad įrenginys būtų saugus, privalome žinoti, kurie atviri prievadai įrenginyje yra palikti, kokia jų funkciją ir ar jų reikia. Visų RUT956 įrenginių konfigūracijos yra beveik identiškos, todėl ir atviri prievadai yra tie patys. Konfigūruojant RUTX11 įrenginį laikytasi tų pačių reikalavimų, kad nepalikti nereikalingų prievadų atvirų. RUTX11 atviri prievadai yra tokie patys, kaip ir RUT956 įrenginiuose. 5 lentelėje pateikiama, kokie prievadai yra atviri bei, ar jie yra reikalingi.

5 lentelė. RUT956 ir RUTX11 įrenginių atviri prievadai

Prievado numeris	Tipas	Protokolas	Reikalingas/Nereikalingas
53	UDP/TCP	DNS	Reikalingas
22	TCP	SSH	Reikalingas
80	TCP	HTTP	Reikalingas
443	TCP	HTTPS	Reikalingas
1194	TCP/UDP	OpenVPN	Reikalingas
67	UDP	DHCP	Reikalingas
500	UDP	ISAKMP	Reikalingas

Kaip matyti, visi atviri prievadai yra žinomi bei reikalingi, todėl galima teigti, kad įrenginiai sukonfigūruoti teisingai.

3.1.2. Atnaujinto tinklo VPN konfigūracijos apžvalga ir sąlygos

Pasirinktos VPN technologijos apžvalga. Svarbiausia dalis, pertvarkant kompiuterinį tinklą, pakeisti nesaugią viešųjų IP adresų technologiją, nutolusių įrenginių pasiekiamumui. Tam buvo panaudotos VPN galimybės, konkrečiai, *OpenVPN* viešai prieinamas protokolas.

Įrenginiai paskirstyti į dvi grupes – *OpenVPN* serveris bei *OpenVPN* klientai. Visi nutolę RUT956 tinklo įrenginiai yra padaryti, kad atliktų *OpenVPN* kliento funkcijas, o ofise esantis RUTX11 įrenginys, padarytas, kad veiktų kaip *OpenVPN* serveris.

OpenVPN yra atvirojo kodo, visiems prieinama programinė įranga, kuria naudojantis, sukuriamas virtualus privatus tinklas. *OpenVPN* yra populiarus bei plačiai naudojamas tiek verslo, tiek asmeninėje aplinkoje. Ši programinė įranga palaiko įvairius šifravimo bei autentifikavimo

metodus, užtikrinant platų konfigūracijų pasirinkimą bei saugumą. Prieš pradedant konfigūracijas, būtina apibrėžti kaip veikia pasirinktas VPN protokolas, kokie galimi konfigūraciniai veiksmai, kas jais pasiekiama, taip pat būtina apžvelgti kokios yra sąlygos, sėkmingam *OpenVPN* tunelio veikimui.

OpenVPN serveris yra atsakingas už visą VPN infrastruktūra. Jis klausos bei priima prisijungimus iš *OpenVPN* klientų, juos autentifikuoja ir sukuria saugų komunikacijos tunelį. *OpenVPN* serveris paskirto IP adresus klientams, nurodo VPN srautą bei pačio tunelio šifravimo metodus. Serveris privalo turėti viešąjį WAN IP adresą, kad klientai galėtų sėkmingai inicijuoti jungimąsi prie VPN serverio.

OpenVPN kliento pagrindinė užduotis yra sėkmingai inicijuoti prisijungimą prie VPN serverio. Kai klientas sėkmingai prisijungia prie VPN serverio, serveris jam suteikia IP adresą, nurodo atitinkamas duomenų srauto reguliavimo taisykles. *OpenVPN* klientas gali turėti tiek viešąjį, tiek privatų WAN IP adresą, jungimuisi prie serverio tai neturi jokios įtakos (openvpn.net, 2024).

Kadangi *OpenVPN* klientai ir *OpenVPN* serveriai atlieka visiškai skirtingas funkcijas virtualiame privačiame tinkle, įrenginiai yra konfigūruojami irgi skirtingai. Tiek nutolę įrenginiai RUT956, tiek ofiso RUTX11, turi *OpenVPN* konfigūracijų grafinę sąsają, tai palengvina darbą konfigūruojant.

Sąlygos naudojant *OpenVPN*. Visų pirma, pagrindinė sąlyga yra tai, kad įrenginiai aplamai palaikytų *OpenVPN* serverio ar *OpenVPN* kliento konfigūracijas. Taip pat, kaip ir minėta ankščiau, *OpenVPN* serveris privalo turėti viešąjį WAN IP adresą, o klientas gali turėti arba viešąjį, arba privatų IP adresą. Trečioji sąlyga yra, kad įrenginiai turėtų prieigą prie interneto, nes tai yra svarbu, inicijuojant VPN tunelį. Šiuo atveju, visos šios privalomos sąlygos projektuojamame objekte atitinka, nes RUTX11 turi viešąjį, o visi RUT956 privačius IP adresus, taip pat, abu šie modeliai palaiko tiek *OpenVPN* serverio, tiek *OpenVPN* kliento konfigūracijas. Taip pat įrenginiuose nėra blokuojama interneto prieiga, ji pilnai pasiekiama.

Prieš pradedant konfigūruoti, privalome išsiaiškinti kokie yra galimi konfigūracijų pasirinkimai, ką jie reiškia, bei kuris labiausiai tinkamas šio darbo atveju. Tai svarbu suprasti bei atsirinkti, nes pasirinkus neteisingą konfigūracijų opciją, galime sukurti nesaugų ar nestabilų VPN tunelį. Išsiaiškinus ką galime konfigūruoti, bei pasirinkus specifines opcijas, dėl kurių VPN tunelis taps saugus, pasieksime savo norimą rezultatą. Pagrindiniai kriterijai, į kuriuos privaloma atsižvelgti yra ryšio tipas, duomenų perdavimo protokolas bei autentifikavimo tipas. Šie kriterijai išskirti kaip pagrindiniai, nes jie yra laikomi VPN tunelio pamatu. Jei šiuos kriterijus atsirinksime neteisingus, nesaugius, visi kiti taikomi saugumo kriterijai praras esmę, nes be saugaus protokolo, atitinkamo ryšio tipo ar saugaus autentifikavimo tipo negalime užtikrinti saugaus tunelio. Visi šie kriterijai yra apžvelgiami 6-8 lentelėse.

6 lentelė. *OpenVPN* ryšio tipo pasirinkimas

Ryšio tipas	Apibūdinimas	Pasirinkimas	Pasirinkimo pagrįstumas
TUN (tunelinis)	TUN naudojamas, kai yra daugiau nei keli klientai VPN tinkle, veikia su 3 OSI lygio paketais.	Taip	Objekte yra daugiau nei vienas įrenginys, kuris turės dirbti kaip VPN klientas, komunikacija vyks 3 OSI lygmenyje.
TAP (tiltinis)	TAP naudojamas tinkle tik tarp dviejų tinklo įrenginių, veikia su 2 OSI lygio paketais – eterneto rėmeliais (angl. ethernet frames).	Ne	-

7 lentelė. *OpenVPN* duomenų perdavimo protokolo pasirinkimas

Protokolas	Apibūdinimas	Pasirinkimas	Pasirinkimo pagrįstumas
UDP	Pagrinde naudojamas dėl greičio, pateikia greitesnį informacijos srautą, praleidžiant klaidų tikrinimo procesą.	Ne	-
TCP	Lėtesnis duomenų perdavimo protokolas nei UDP, tačiau pristato ir gauna patikrintą informacijos paketų srautą, nes nėra praleidžiamas klaidų tikrinimo procesas	Taip	Duomenų perdavimo sparta nėra svarbiausiais kriterijus. Svarbiausia yra užtikrinti informacijos patikimumą bei vientisumą.

8 lentelė. *OpenVPN* autentifikavimo tipo technologijų pasirinkimas

Autentifikavimo tipas	Apibūdinimas	Pasirinkimas	Pasirinkimo pagrįstumas
TLS	Autentifikavimui ir privačių raktų mainams naudojami SSL/TLS sertifikatai.	Taip	Didesnis saugumo lygis, lyginant su statinio rakto naudojimo.
Statinis raktas	Autentifikavimui naudojamas statinis raktas	Ne	

Ryšio tipas pasirinktas TUN (tunelinis), duomenų perdavimo protokolas TCP, bei autentifikavimo tipas TLS. Šie pasirinkimai atlikti, nes aukščiausias prioritetas yra kuo didesnis tinklo saugumas bei atsparumas nuo įsilaužėlių rengiamų kibernetinių atakų.

Svarbu atkreipti dėmesį į tai, kad naudosime TLS autentifikavimo tipą, o tai prideda dar kelias svarbias sąlygas bei pasiruošimo konfigūracijai žingsnius, kuriuos būtina atlikti. Naudojant TLS tipą, privaloma sugeneruoti kelis skirtingus sertifikatus bei raktus, kurie bus naudojami įrenginių autentifikavime.

OpenVPN serverio įrenginiui reikės šių sertifikatų bei raktų :

- *Root* sertifikato failo;
- Serverio sertifikato;
- Serverio rakto;

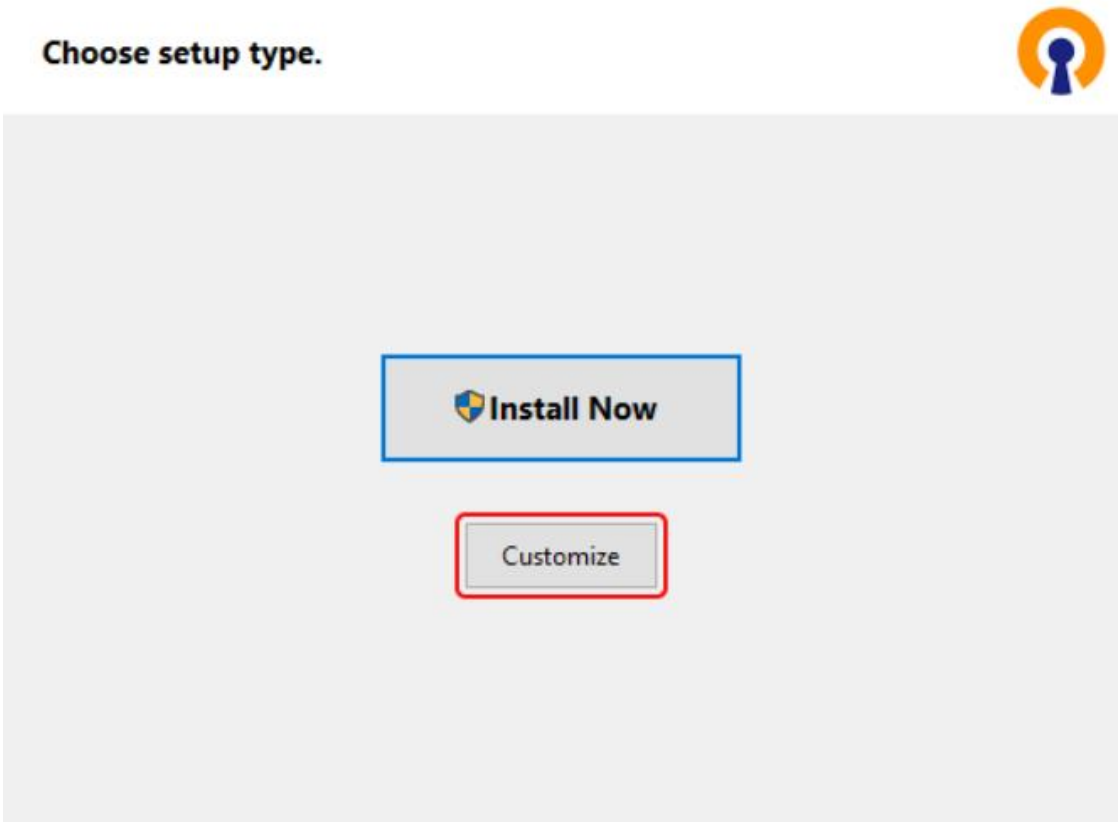
- *Diffie Hellman* parametrų failo.

OpenVPN kliento įrenginiui reikės šių sertifikatų bei raktų :

- *Root* sertifikato failo (to paties, kurį keliame ir į serverio įrenginį);
- Kliento sertifikato;
- Kliento rakto.

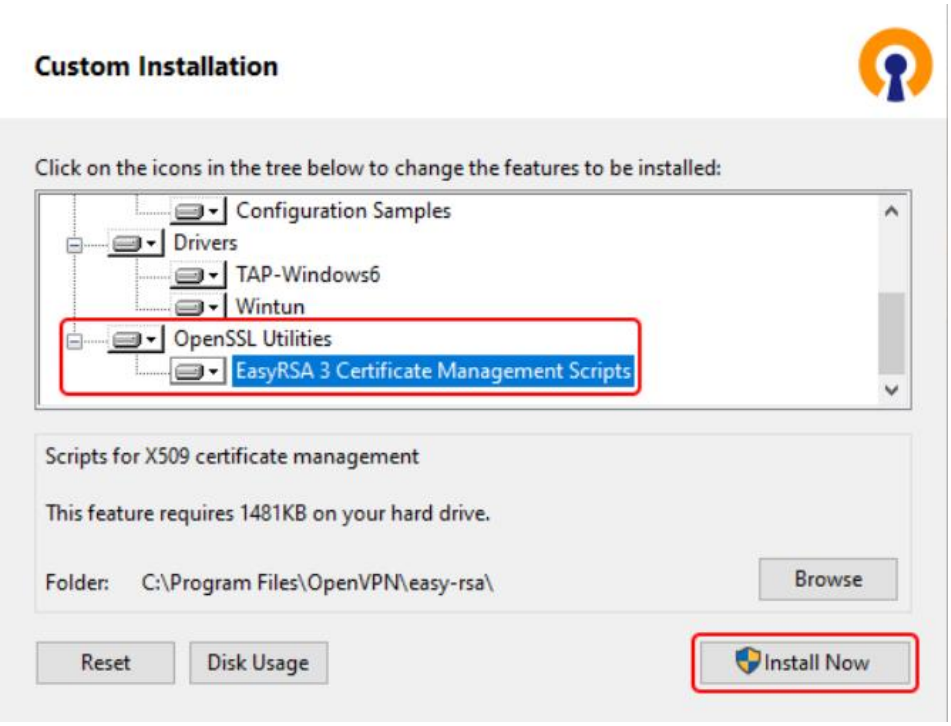
Žingsniai, kuriuos atlikus, būsime sugeneravę visus reikiamus sertifikatus bei raktus:

1. Pirmiausia privaloma parsisiųsti *OpenVPN* instaliacijos failą į kompiuterį bei jį paleisti. Paleidus, matysis du pasirinkimai, spaudžiame pritaikyti (angl. *Customize*) mygtuką, kaip pavaizduota paveiksle 3.3.



3.3 pav. *OpenVPN* instaliacija

2. Paspaudus nurodytą mygtuką, naujame lange turim pasirinkti „*Easy RSA3 Certificate Management Scripts*“ opciją, kaip nurodyta 3.4 paveiksle. „*Easy RSA3 Certificate Management Scripts*“ yra įrankių rinkinys, leidžiantis valdyti bei paskirstyti šifravimo sertifikatus. Tai yra ypač naudingas įrankių rinkinys, kuriant ir konfigūruojant virtualius privačius tinklus. Instaliuojantis bet kurią *OpenVPN* aplikaciją, šie papildomi įrankiai dažniausiai instaliuojami kartu, tai gali būti, kad kai kurie kompiuteriai jau juos turi ir nėra būtinybės juos siųstis papildomai.



3.4 pav. *EasyRSA3* opcija

3. Baigus instaliacijai, privaloma įsijungti komandinę eilutę, administratoriaus teisėmis.
4. Įsijungus komandinę eilutę, privaloma viena po kitos įvykdyti sekančias komandas:
   - *cd "C:\Program Files\OpenVPN\easy-rsa"*
   - *EasyRSA-Start.bat*
   - *./easyrsa init-pki*
   - *notepad vars.bat*

Po ketvirtosios komandos, bus atidarytas teksto redagavimo programa ir į atidarytą failą suvedame sekančias eilutes:

- *set KEY_COUNTRY=LT*
- *set KEY_PROVINCE=Kaunas*
- *set KEY_CITY=Kaunas*
- *set KEY_ORG=ImoneX*
- *set KEY_EMAIL=inzierius@ImoneX*
- *set DH_KEY_SIZE=2048*

Suvedus šias komandas, įsaugomas bei uždaromas redaguojamas failas. Galiausiai, liko įvesti dvi paskutines komandas ir galėsime pradėti generuoti sertifikatus bei raktus. Suvedamos komandos:

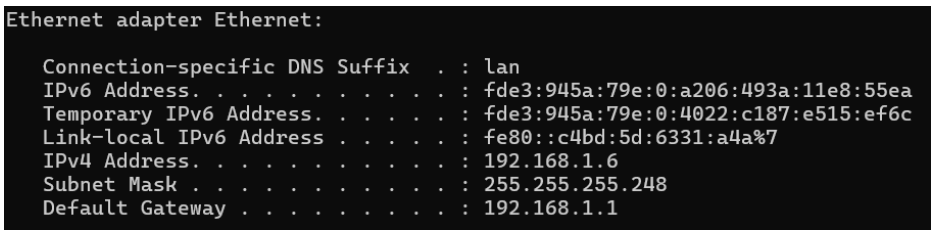
- *vars.bat*
- *./easyrsa clean-all*

Suvedus šias komandas, galima vesti kitas komandas, kurios jau sugeneruos reikiamus sertifikatus bei raktus. Komandos, jų paaiškinimai, sugeneruotas failas bei failo vieta, paaiškinami 9 lentelėje.

9 lentelė. Sertikatų bei raktų generavimo komandos ir paaiškinimai

Komanda	Paaiškinimas	Sukurto failo pavadinimas	Failo sukūrimo vieta
./easyrsa build-ca nopass	Sukuriamas „Root“ sertifikato failas	ca.crt	C:\Program Files\OpenVPN\easy-rsa\pki
./easyrsa build-server-full server nopass	Sukuriamas serverio sertifikatas bei serverio raktas	server.key server.crt	Serverio rakto sukūrimo vieta : C:\Program Files\OpenVPN\easy-rsa\pki\private Serverio sertfikato sukūrimo vieta : C:\Program Files\OpenVPN\easy-rsa\pki\issued
./easyrsa build-client-full Client1 nopass	Sukuriamas kliento sertifikatas bei kliento raktas	Client1.key Client1.crt	Kliento rakto sukūrimo vieta : C:\Program Files\OpenVPN\easy-rsa\pki\private Kliento sertifikato sukūrimo vieta : C:\Program Files\OpenVPN\easy-rsa\pki\issued
./easyrsa gen-dh	Sukuriamas „*Diffie Helman*“ paramterų failas	dh.pem	C:\Program Files\OpenVPN\easy-rsa\pki

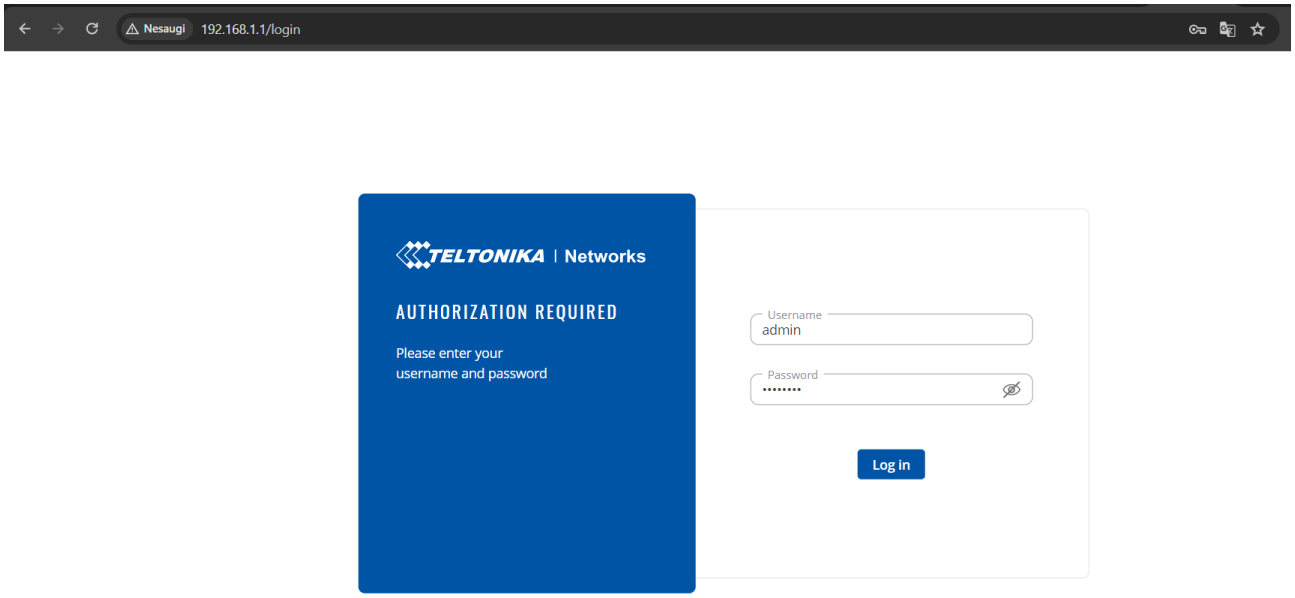
Įvykdžius visus šiuos žingsnius, sugeneruojami reikiami sertifikatai bei raktai, kurie bus naudojami konfigūruojant *OpenVPN* serverio įrenginį, bei *OpenVPN* kliento įrenginius. Tinklo įrenginių konfigūracija pradedama nuo serverio įrenginio, kuris yra RUTX11. Pirmiausia, prisijungiama į įrenginio grafinę sąsają. Prisijungti prie grafines sąsajos pirmiausia reikia kompiuterį prijungti prie įrenginio, fiziškai jungiant laidą iš RUTX11 LAN prievado, į kompiuterio LAN prievadą. Tokiu būdu, kompiuteris tampa RUTX11 suteikiamo tinklo įrenginys ir iš darbinio kompiuterio galime pasiekti RUTX11 įrenginį, taip pat ir jo vartotojo sąsają bei komandinę eilutę. Norint pasiekti RUTX11 įrenginį, reikia jo LAN IP adresą suvesti į pasirinktos naršyklės paieškos eilutę. Norint sužinoti koks yra paskirtas darbiniui kompiuteriui IP adresas, taip pat koks yra RUTX11 LAN IP adresas, reikia atsidaryti komandinę eilutę darbiniame kompiuteryje ir suvesti komandą *ipconfig*. Pastaroji komanda yra komandinės eilutės įrankis, veikiantis tik ant Windows operacinės sistemos. Komandos rezultato išvestis atvaizduojama 3.5 paveiksle.



3.5pav. *ipconfig* komandos rezultatas

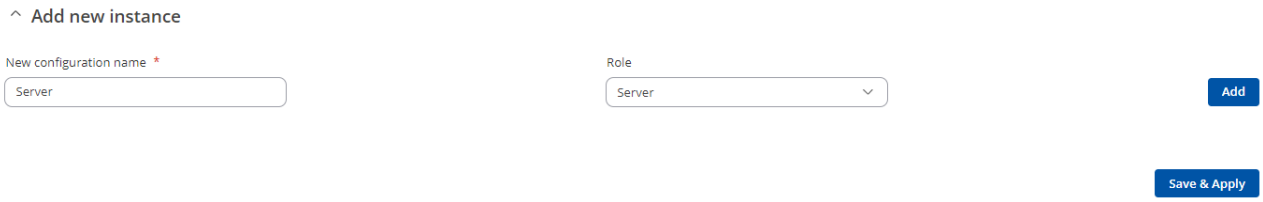
Ši komanda naudojama su kompiuteriniu tinklu susijusiai informacijai surasti bei valdyti. Įvesdami šią komandą matome paskirta IP adresą, bei pačio įrenginio IP adresą.

Žinodami IP adresą RUTX11 įrenginio, jį vedame į naršyklės paieškos lauką ir pasiekiame maršrutizatoriaus grafinės sąsajos prisijungimo langą, kuriame reikia suvesti prisijungimo duomenis. Maršrutizatoriaus grafinės sąsajos prisijungimo langas naršyklėje atvaizduojamas 3.6 paveiksle.



3.6 pav. Grafinės sąsajos prisijungimo langas

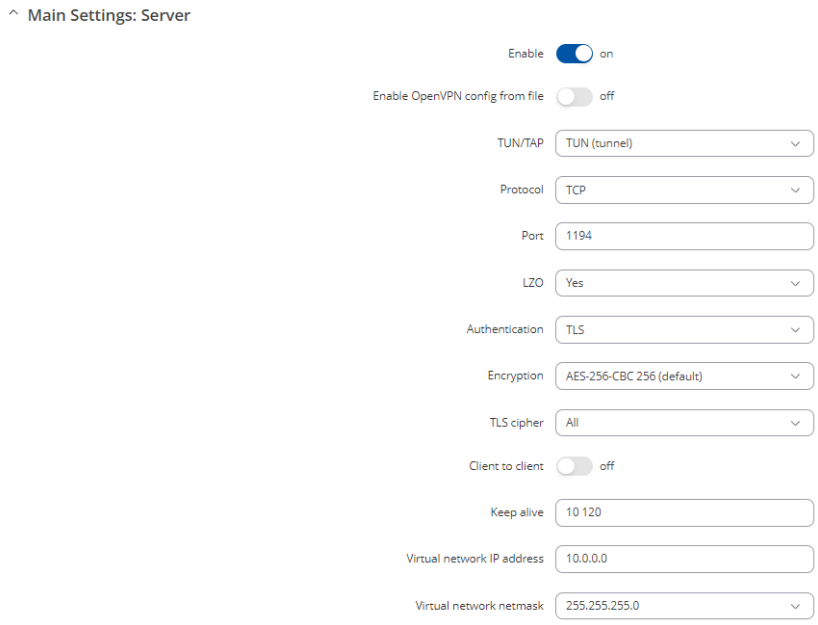
Prisijungus, susirandame *OpenVPN* nustatymus, susikuriame naują serverio sąsają. Susikūrus suvedame visus reikalingus duomenis. Serverio sąsajos pasirinkimas grafinėje sąsajoje atvaizduojamas 3.7 paveiksle.



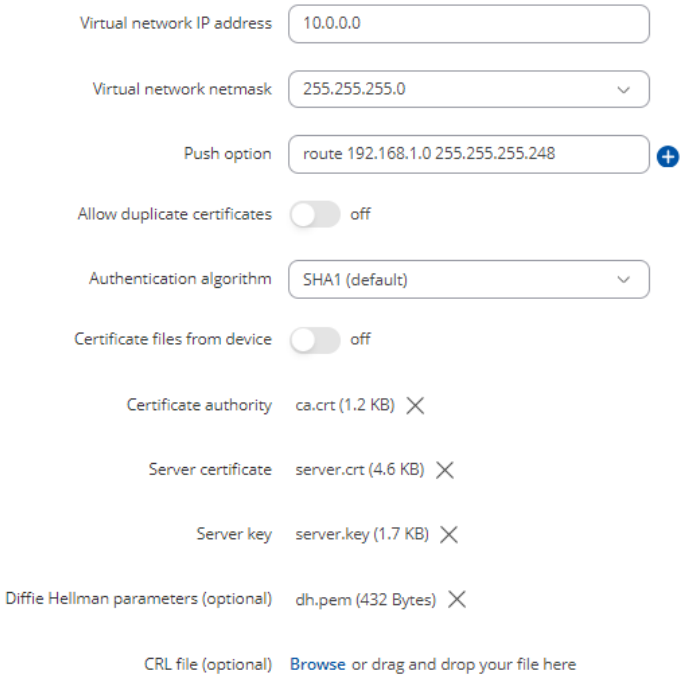
3.7 pav. Sukuriama *OpenVPN* serverio sąsaja

Toliau, suvedame visus reikiamus duomenis, kurių yra prašoma, taip pat, sukeliame prieš tai sugeneruotus sertifikatus bei raktus. Suvesti duomenys atvaizduojami 3.8 ir 3.9 paveiksluose. Suvedus visus reikiamus duomenis, spaudžiamas išsaugojimo mygtukas, kad visos konfigūracijos

būtų išsaugotos. Šiuo metu vedami duomenys yra tik serverio įrenginio ir šie vedami duomenys skirsis nuo *OpenVPN* klientų konfigūracijų.



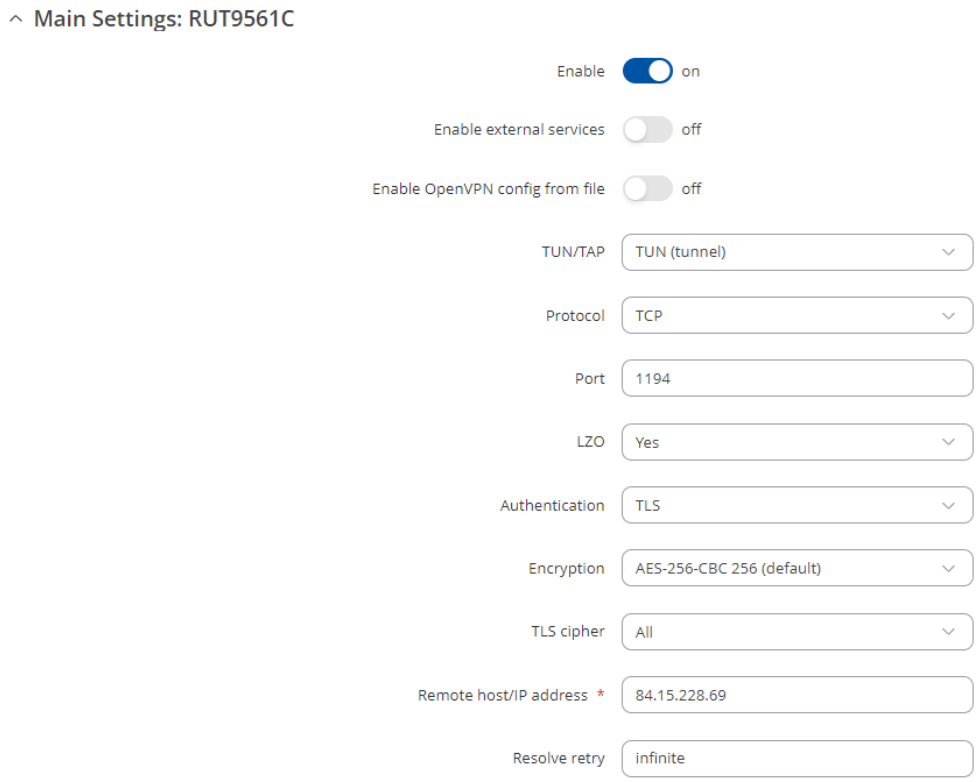
3.8 pav. Pirmoji dalis suvestų duomenų *OpenVPN* serverio sąsajai



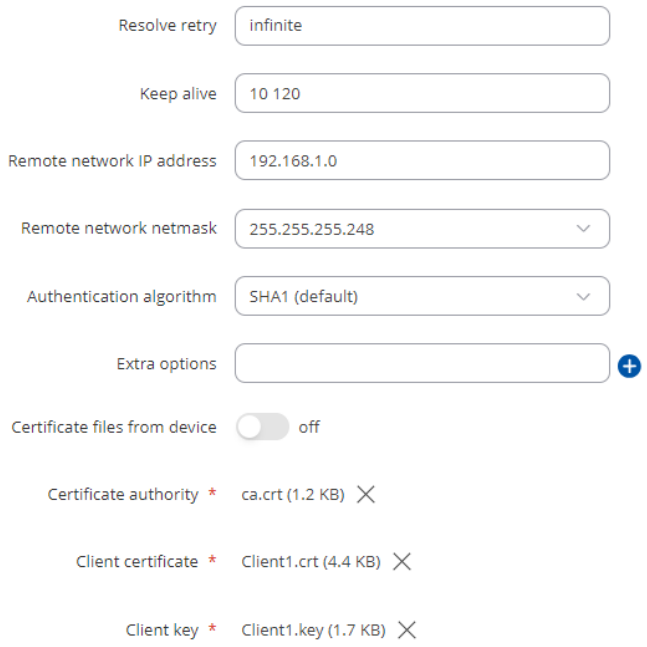
3.9 pav. Antroji dalis suvestų duomenų *OpenVPN* serverio sąsajai

Toliau lieka sukonfigūruoti *OpenVPN* klientų sąsajas. Norint pasiekti įrenginius, kurie dirbs kaip VPN klientai, reikia atlikti tuos pačius žingsnius, kaip kad buvo nurodyta siekiant pasiekti RUTX11 įrenginį, pasiekti jo grafinę sąsają bei susirasti *OpenVPN* konfigūracijos puslapį. Sėkmingai

pasiekus RUT956 įrenginio grafinę sąsają bei susiradus *OpenVPN* konfigūracijos puslapį, reikia suvesti visus reikiamus duomenis ir nepamiršti paspausti konfigūracijų išsaugojimo mygtuką. *OpenVPN* kliento konfigūracijos matomos 3.10 ir 3.11 paveiksluose.

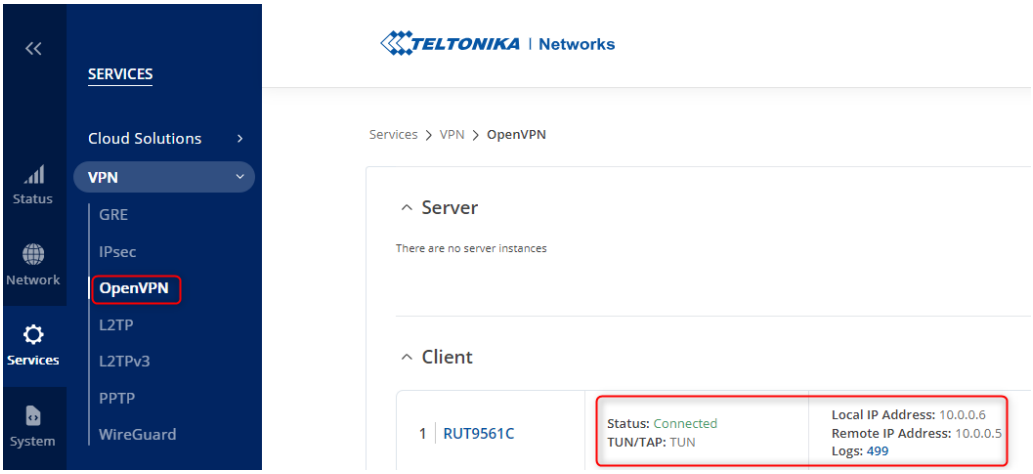


3.10 pav. Pirmoji dalis suvestų duomenų *OpenVPN* kliento sąsajai

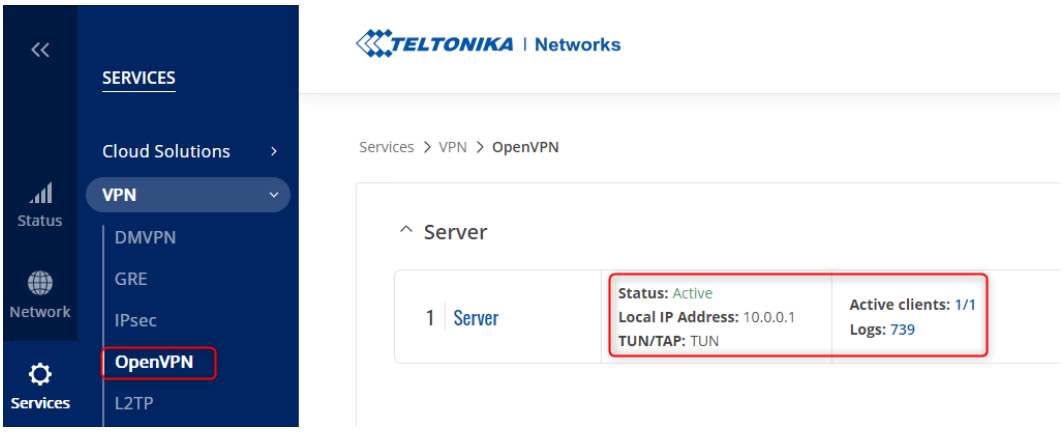


3.11 pav. Antroji dalis suvestų duomenų *OpenVPN* kliento sąsajai

Sėkmingai suvedus reikiamus teisingus duomenis tiek serverio sąsajoje, tiek klientų sąsajose, galima matyti, kad VPN statusas pasikeičia į prijungtą, taip pat galime matyti priskirtus VPN IP adresus. Statusą bei priskirtų IP adresų išvedimą galima pamatyti 3.12 ir 3.13 paveiksluose.



3.12 pav. *OpenVPN* kliento sąsajos status bei IP adresai



3.13 pav. *OpenVPN* serverio sąsajos statusas bei IP adresai

Matant aktyvaus ir prisijungusio statuso žymas, žinome, kad visi suvesti duomenys yra teisingi ir komunikacija VPN tuneliu yra galima. Visos *OpenVPN* klientų sąsajos sukonfigūruojamos beveik identiškai, skiriasi tik sertifikatai ir raktai.

Įdiegto VPN serverio bei klientų IP adresai yra atvaizduojami 10 lentelėje.

10 lentelė. *OpenVPN* klientų bei serverio IP adresai, statusas

	RUT956_1	RUT956_2	RUT956_3	RUT956_4	RUT956_5	RUTX11
Lokalus VPN IP adresas	10.0.0.6	10.0.0.8	10.0.0.10	10.0.0.12	10.0.0.14	10.0.0.1
Nutolęs VPN IP adresas	10.0.0.5	10.0.0.7	10.0.0.9	10.0.0.11	10.0.0.13	-
Statusas	Prisijungęs	Prisijungęs	Prisijungęs	Prisijungęs	Prisijungęs	Aktyvus

Matoma, kad klientai gauna du IP adresus, vienas lokalus VPN IP adresas, kitas nutolęs VPN IP adresas. Lokalus VPN IP adresas yra skirtas įrenginiui komunikuoti VPN tinkle bendrai su visais kitais tinklo įrenginiais, o nutolęs VPN IP adresas yra naudojamas komunikacijoje tik tarp tam tikro kliento ir serverio. Daugiau su jokiu kitu įrenginiu per nutolusį VPN IP adresą įrenginys negali komunikuoti. RUTX11 neturi nutolusio VPN IP adreso, nes pats įrenginys dirba kaip *OpenVPN* serveris.

3.2. Projektuojamo objekto aparatūros posistemė

Aparatūros posistemė. Tinklo įrenginiai privalo atitikti nurodytus specifinius kriterijus, kad būtų užtikrintas nepertraukiamas tinklo įrangos darbas.

Specializuota aparatūra. Projektuojamo objekto tinklo įrenginiai priskiriama specializuotai, industrinėse aplikacijose naudojamai tinklo įrangai. Ši tinklo įranga pasižymi atsparumu aukštoms ir žemoms temperatūroms, taip pat apsauga nuo elektros iškrovų, atsparumu vandens purslams, atsparumu netyčiniams fiziniams pažeidimams, tokiems kaip, netyčiniai numetimai, sutrenkimai, korpuso pažeidimai.

Aparatūrinė įranga. Kaip ir pradiniame objekte, taip ir projektuotame objekte, tinklo įranga naudojama ta pati. Nutolę įrenginiai yra RUT956, ofiso įrenginys RUTX11. Specifiniai aparatūriniai nurodymai galioja tik RUT956 gaminiams, nes jie yra nutolę ir įmontuoti į neįprasta vietą. Ofiso maršrutizatorius, RUTX11, turi kelis pagrindinius nurodymus – 3 LAN prievadai, 4G palaikymas, 1 WAN prievadas, Wi-Fi palaikymas. Atitikimas aparatūrinės įrangos specifiniams kriterijams pateikiamas 11 lentelėje.

11 lentelė. Aparatūrinės įrangos specifinių kriterijų atitikimo lentelė

	RUT956	**RUTX11**
Darbinė temperatūra -20°C iki 70°C	Atitinka	Atitinka
3 LAN prievadai	Atitinka	Atitinka
RS232	Atitinka	Neatitinka, bet ir nereikalinga
RS485	Atitinka	Neatitinka, bet ir nereikalinga
Užmaitinimas 9-30VDC srove	Atitinka	Atitinka
4G mobiliojo ryšio palaikymas	Atitinka	Atitinka
2 SIM kortelių vietos	Atitinka	Atitinka
1 WAN prievadas	Atitinka, bet nereikalinga.	Atitinka
Wi-Fi palaikymas	Atitinka, bet nereikalinga.	Atitinka
Kaina ne didesnė nei 350 eurų	Atitinka	Atitinka

Matoma, kad visi svarbiausi kriterijai, kurie liečia aparatūrinius parametrus, nurodytus specifikacijose atitinka, todėl galima teigti, kad tinklo įranga yra pasirinkta gera.

Programinės priemonės. Projektuojamam objektui yra labai svarbūs aparatūrinių parametrų atitikimai, tačiau ne mažiau svarbu ir programinė įrangą.

Abu maršrutizatorių modeliai yra gamina Teltonika Networks įmonės ir jie naudoja RutOS operacinę sistemą. RutOS operacinė sistema yra pagrįsta *OpenWrt*. Ši operacinė sistema suteikia lengvai valdomą intuityvią grafinę sąsają, taip yra sumažinamos inžinierių mokymo išlaidos diegiant įrenginius. Taip pat, ši sistema palengvina migravimą tarp skirtingų įrenginių ir platformų. RutOS palaiko įvairias technologijas, pradedant bevielio ryšio Wi-Fi, baigiant industriniais protokolais (wiki.teltonika-networks.com, 2020)

Projektuojamame objekte svarbiausios programinės įrangos funkcijos apima technologijas, pasiekti nutolusius įrenginius, SIM kortelių valdymą, ugniasienės valdymą, slaptažodžių valdymą. Pasiekti nutolusius įrenginius naudojamas yra VPN, SIM kortelių valdymas būtinas, kad galėtumėme pakeisti IP adresą iš viešojo į privatų, taip pat, užtikrinti, kad nulūžus vienai SIM kortelei, įrenginys vis tiek turėtų interneto prieigą. Ugniasienės bei slaptažodžių valdymas yra svarbūs kibernetinio saugumo aspektai. Programinės įrangos kriterijų atitikimai matomi 12 lentelėje

12 lentelė. Programinės įrangos kriterijų atitikimo lentelė

	RUT956	**RUTX11**
Ugniasienės valdymas	Atitinka	Atitinka
SIM kortelių valdymas	Atitinka	Atitinka
VPN galimybės	Atitinka	Atitinka
Slaptažodžių valdymas	Atitinka	Atitinka

Kaip matome, pagrindiniai programinės įrangos kriterijai atitinka, todėl galima teigti, kad įrenginiai puikiai tinka objektui, tiek iš aparatūrinės įrangos pusės, tiek iš programinės įrangos pusės.

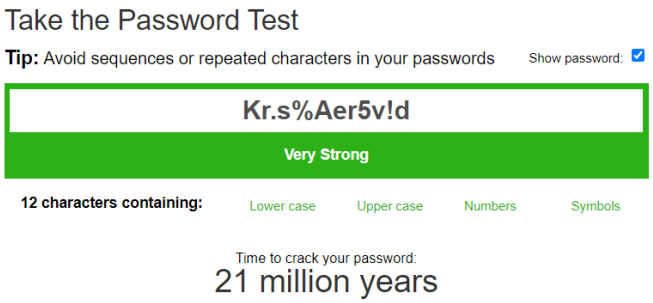
3.3. Slaptažodžių saugumo politikos nustatymas

Projektuojamo objekto tinklo įrenginiai apsaugomi saugiais prisijungimo slaptažodžiais. Slaptažodžius sukuria tinklo inžinierius, administruojantis objektą. Kuriant slaptažodį vadovaujamasi šiomis taisyklėmis :

- Slaptažodį sudaro minimaliai 12 simbolių
- Naudojami specialieji simboliai, skaičiai, mažosios ir didžiosios raidės.
- Tas pats slaptažodis nenaudojamas ant skirtingų įrenginių
- Slaptažodis keičiamas kas 3 mėnesius
- Gero slaptažodžio pavyzdys : Kr.s%Aer5v!d

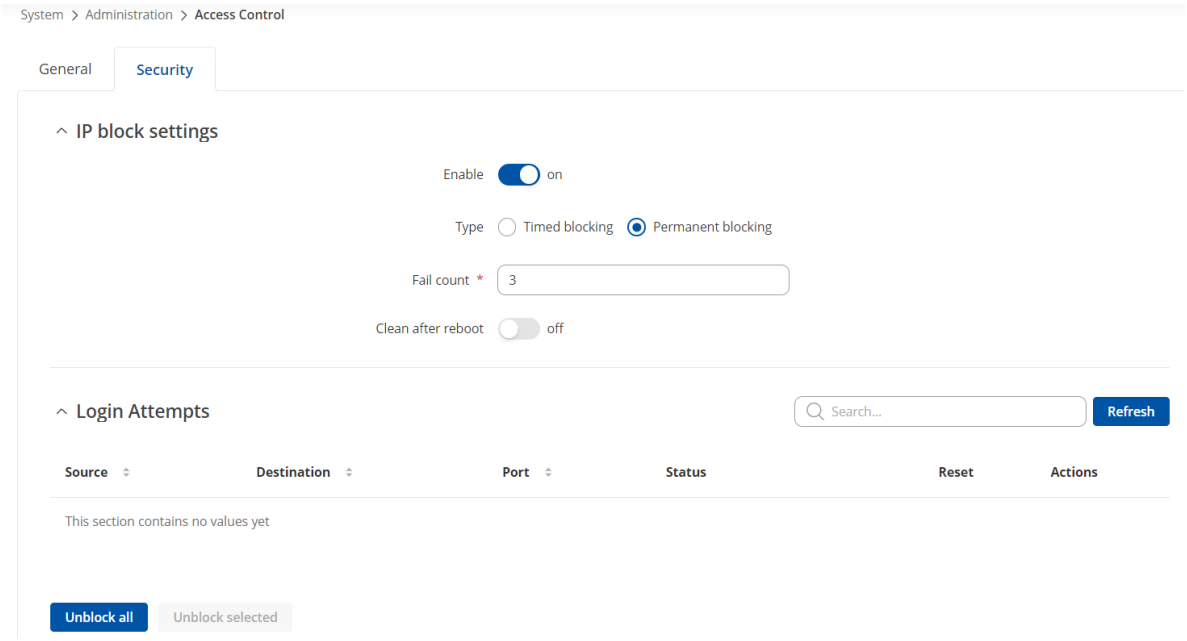
Laikantis nustatytos slaptažodžių saugumo politika, stiprinama bendra kibernetinės saugos politika, taip mažinama kibernetinių nusikaltėlių galimybė sukelti žalą tinklo infrastruktūrai, bei pačiai įmonei. Pateiktas gero slaptažodžio pavyzdys, kurio nulaužimo laiką patikrinome su viešai prieinamu įrankiu ir įsitikiname, kad tai tikrai stiprus slaptažodis, kurį nulaužti užtruktų 21 milijoną

metų. Pavyzdinio slaptažodžio nulaužimo laikas viešai prieinamame įrankyje atvaizduojamas 3.14 paveiksle.



3.14 pav. Pavyzdinio slaptažodžio nulaužimo laikas

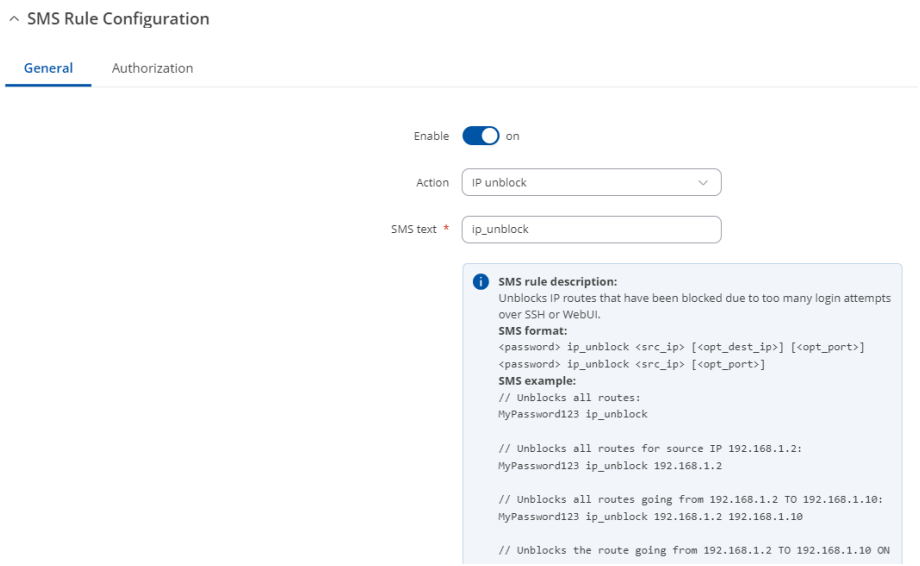
Taip pat, įgyvendinama įrenginio prieigos blokavimo funkcija, suvedus neteisingą slaptažodį. Nustatyta, kad įrenginys užblokuos įrenginio pasiekimą iš tam tikro IP adreso, jei slaptažodis bus suvestas daugiau nei 3 kartus neteisingai. Kai įrenginys automatiškai užblokuos prieigą, tinklo inžinierius prisijungęs galės matyti iš kokio IP buvo bandoma pasiekti įrenginį, kokiu būdu buvo bandoma pasiekti įrenginį. Prieigos blokavimo funkcijos konfigūracija maršrutizatoriaus grafinėje sąsajoj atvaizduojama 3.15 paveiksle.



3.15 pav. Prieigos blokavimo funkcijos konfigūracija

Svarbu paminėti, kad tinklo inžinierius, kuris jungiasi prie nutolusių įrenginių, turi būti labai atidus, kad neužsiblokuotų pats savęs. Jeigu nutiktų taip, kad inžinierius užsiblokuoja pats save, įrenginį reikėtų atstatyti į gamyklinius parametrus, o to nutolusiam įrenginiui padaryti bus

neįmanoma, neiškėlus jo iš objekto. Norint užtikrinti, kad niekada nereiktų to atlikti, surandama alternatyva, kaip būtų galima atsiblokuoti, netyčia užblokuotą, tinklo inžinieriaus prieigą. Kaip jau žinoma, įrenginiuose dedasi SIM kortelės, tai reiškia, kad įmanoma išsiųsti ir gauti žinutes panaudojant SIM korteles. Parinkti įrenginiai turi funkcijas, leidžiančias gauti ir siųsti SMS žinutes, taip pat, SMS žinutės gali būtų panaudojamos įvykdant tam tikras funkcijas pačiame įrenginyje. Yra numatytoji taisyklė, kuri atblokuoja užblokuotus IP adresus, bandant prisijungti prie įrenginio. Taisyklės konfigūracija atvaizduojama 3.16 paveiksle.



3.16 pav. SMS taisyklės, atblokuojančios įrenginio prieigą, konfigūracija

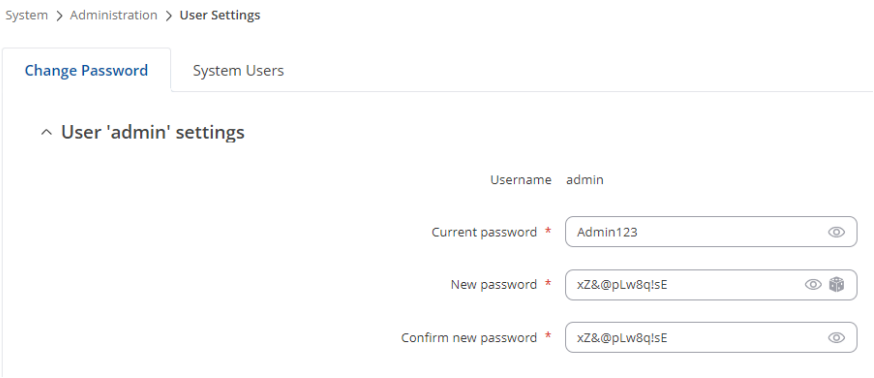
Į slaptažodžių politika, ši taisyklė yra įtraukiama, norint užtikrinti, kad netyčia inžinieriui užsiblokavus prieigą, nereiktų įrenginio iškėlinėti iš vėjo jėgainės.

Visų įrenginių numatytieji slaptažodžiai buvo pakeisti vadovaujantis naujai nustatytai slaptažodžių politikai. Slaptažodžio pakeitimas atliekamas jungiantis prie maršrutizatoriaus grafinės sąsajos. Visi naujieji įrenginių slaptažodžiai pateikiami 13 lentelėje.

13 lentelė. Nustatyti naujieji slaptažodžiai

	RUT956_1	RUT956_2	RUT956_3	RUT956_4	RUT956_5	RUTX11
Naujas slaptažodis	xZ&@pLw8q!sE	y.#sTb9@r!d2	!N!dGv5k!.@L	5-El.a2@,dpk	Obd#.W[svmdl	;Xpw5#.1@d$v,
Senas slaptažodis	Admin123	Admin123	Admin123	Admin123	Admin123	Admin123

Pakeistas slaptažodis RUT956_1 įrenginio matomas 3.17 paveiksle. Prisijungus prie grafinės sąsajos, susirandamas slaptažodžio pakeitimų konfigūracijos puslapis.



3.17 pav. Naujasis RUT956_1 slaptažodis

Naudojant saugius slaptažodžius, uždedamas papildomas saugumo sluoksnis. Jeigu nutiktų taip, kad būtų nulaužtas *OpenVPN* serveris ir kibernetiniai nusikaltėliai galėtų pasiekti nutolusius įrenginius per jų *OpenVPN* IP adresus, prie įrenginių nebus galima prisijungti atspėjanti slaptažodžius.

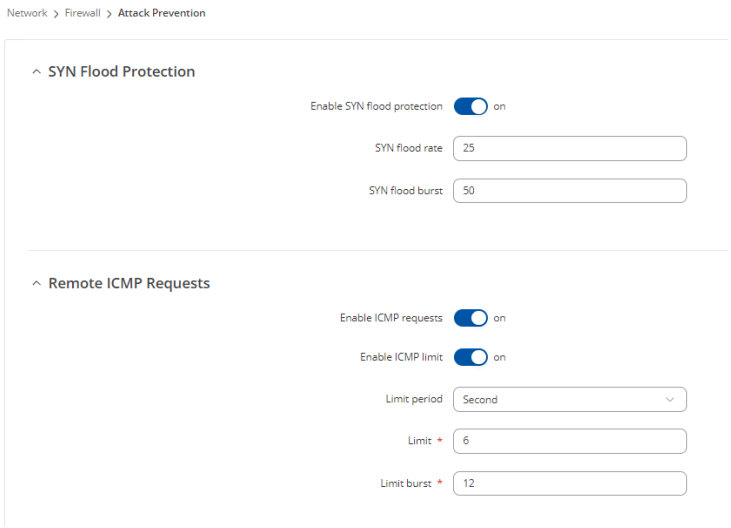
3.4. Kibernetinių atakų prevencijos funkcijos

Norint užtikrinti aukštą kompiuterinio tinklo įrenginių saugumą, rekomenduojama įgalinti papildomas funkcijas, kurios sukurtos atpažinti bei užkirsti kelią kibernetiniams išpuoliams. Parinkta tinklo įranga, turi kelias funkcijas, kurios gali dar labiau padidinti kibernetinio saugumo situaciją objekte. Visos funkcijos, jų aprašymai bei reikalingumas aprašomas 14 lentelėje.

14 lentelė. Atakų prevencijos funkcijų aprašas (Sudaryta autoriaus pagal wiki.teltonika-networks.com pateikiama informaciją, 2024)

Funkcijos pavadinimas	Funkcijos aprašymas	Reikalingas/Nereikalingas
SYN paketų užtvindymo apsauga	SYN paketų užtvindymo ataka yra DDoS atakos forma, kai užpuolikas siunčia gausybę SYN užklausų į taikinį, bandydamas išnaudoti visus įrenginio resursus. Sėkmingos atakos metu, įrenginys tampa neveiksnus ir nebeatlieka visų privalomų funkcijų.	Reikalingas
Nuotolinių ICMP protokolo paketų limitavimas	ICMP potvynių ataka yra įprasta DDoS ataka, kai užpuolikas bando įrenginį užlaužti siųsdamas eilę ICMP užklausų.	Reikalingas
SSH atakos apsauga	SSH atakos taip pat yra DDoS atakos forma, kai bandoma įrenginį užlaužti siunčiant eilę SSH užklausų į įrenginį.	Reikalingas
HTTP protokolu grįsta užtvindymo ataka	HTTP protokolu pagrįsta užtvindymo ataka taip pat yra DDoS atakos forma, kurios metu užpuolikas siunčia daug HTTP užklausų į įrenginį.	Reikalingas
HTTPS protokolu grįsta užtvindymo ataka	HTTPS ataka yra tokia pati kaip ir HTTP, tik šiuo atveju siunčiamos HTTPS užklausos.	Reikalingas
Prievadų skenavimo apsauga	Prievadų nuskaitymo procesu yra siunčiamos užklausos į įvairius įrenginio prievadus, siekiant rasti aktyvius ir atidarytus prievadus.	Reikalingas

Šios atakų prevencijos funkcijos yra konfigūruojamos įrenginio grafinėje sąsajoje. Sukonfigūruotos funkcijos atvaizduojamos 3.18, 3.19, 3.20 paveiksluose.



3.18 pav. SYN bei ICMP atakų prevencijos konfigūracijos

SYN atakos prevencijos nustatymai paaiškinami 15 lentelėje. ICMP atakos prevencijos nustatymai paaiškinami 16 lentelėje.

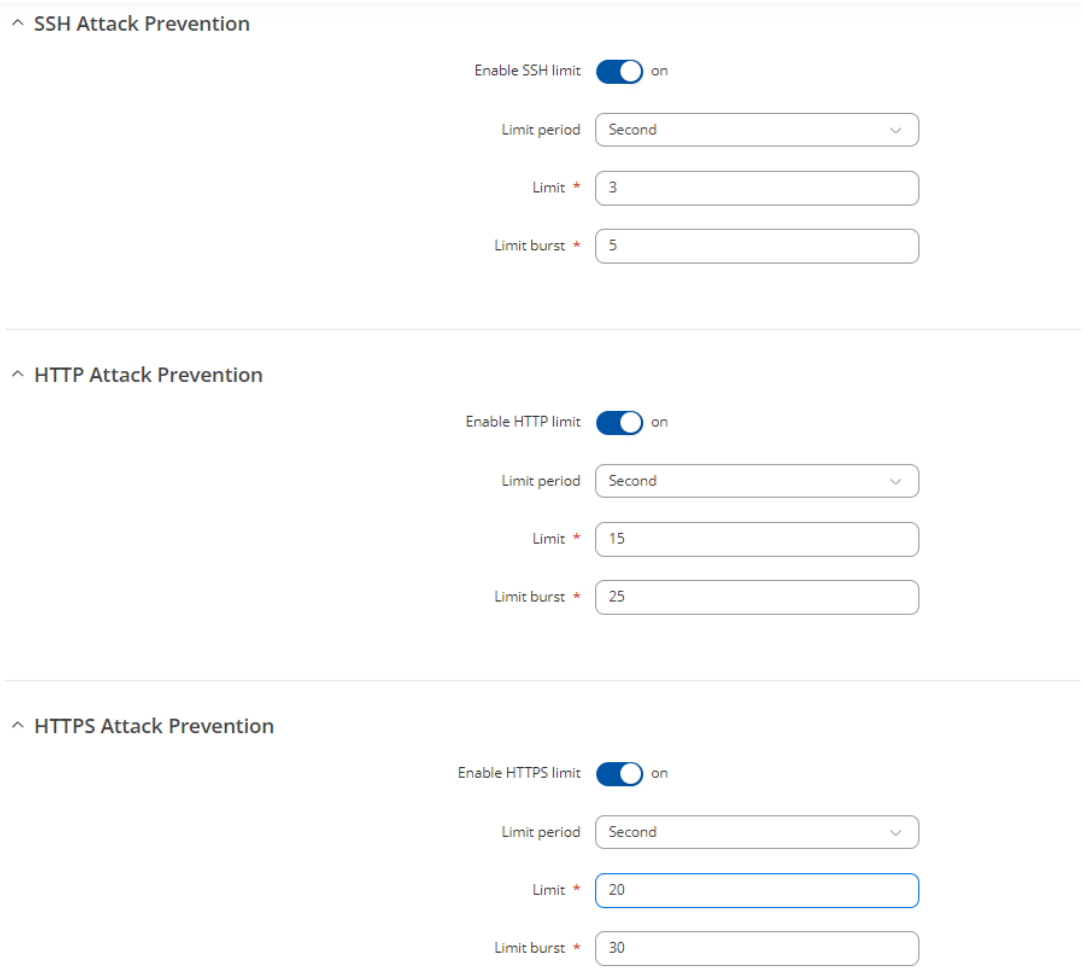
15 lentelė. SYN atakos prevencijos nustatymai (Sudaryta autoriaus pagal wiki.teltonika-networks.com pateikiama informaciją, 2024)

Nustatymas	Pasirinkta reikšmė	Paaiškinimas
SYN potvynio rodiklis (angl. SYN *flood rate)*	25	Nustatomas SYN paketų greičio limitas (paketų per sekundę), kurį viršijus srautas laikomas užtvindytu
SYN potvynio sprogimo rodiklis (angl. SYN *flood rate*)	50	Nustatomas SYN paketų serijos limitas, kurį viršijus srautas laikomas užtvindytu, jei jis viršija leistiną spartą

SYN apsauga nuo potvynių leidžia apsisaugoti nuo atakų, kurios išnaudoja dalį įprasto TCP trijų krypčių rankų paspaudimo, kad sunaudotų tikslinio serverio išteklius ir jis nereaguotų.

16 lentelė. ICMP atakos prevencijos nustatymai (Sudaryta autoriaus pagal wiki.teltonika-networks.com pateikiama informaciją, 2024)

Nustatymas	Pasirinkta reikšmė	Paaiškinimas
Limito periodas (angl. *Limit period*)	Sekundė (angl. *Second*)	Taisyklės sąlygų atitikimo laikotarpio trukmė.
Limitas (angl. *Limit*)	6	Didžiausias ICMP užklausų skaičius per laikotarpį.
Limito sprogimo rodiklis (angl. *Limit burst*)	12	Nurodo didžiausią ištisinę užklausų seriją prieš pradedant limituoti aukščiau nurodytą ribą.



3.19 pav. SSH, HTTP, HTTPS atakų prevencijos nustatymai

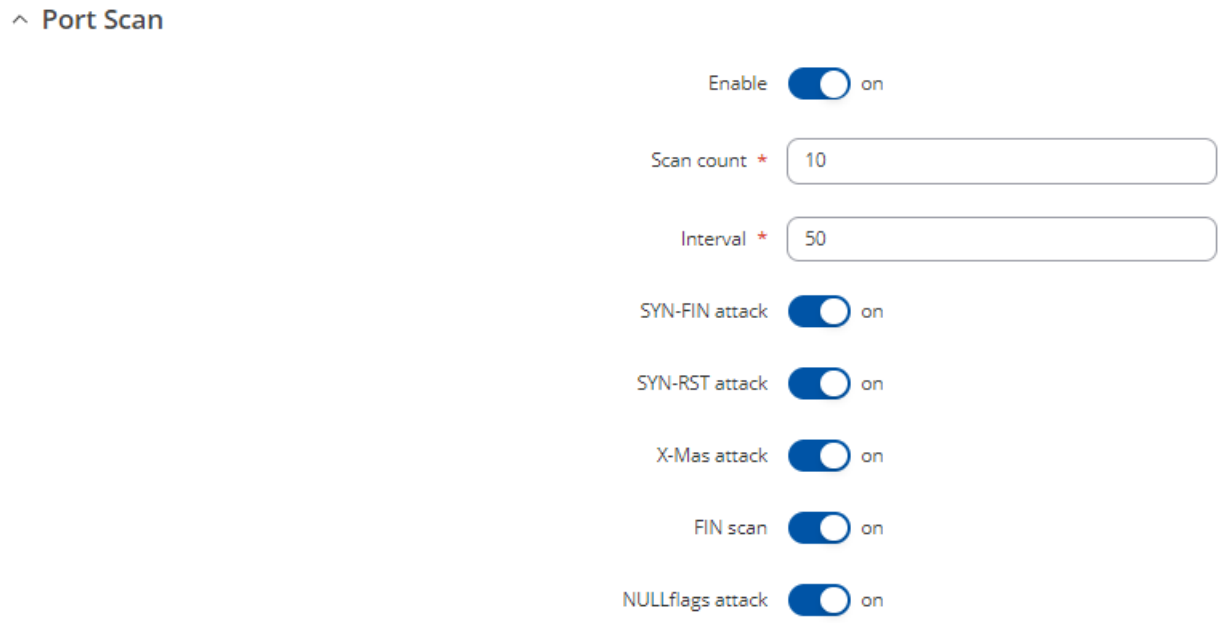
SSH, HTTP ir HTTPS atakos prevencijos nustatymai paaiškinami 17 lentelėje.

17 lentelė. SSH, HTTP(S) atakų prevencijos nustatymai (Sudaryta autoriaus pagal wiki.teltonika-networks.com pateikiama informaciją, 2024)

Nustatymas	Pasirinkta reikšmė	Paaiškinimas
SSH Limito periodas (angl. *Limit period*)	Sekundė	Taisyklės sąlygų atitikimo laikotarpio trukmė.
SSH Limitas (angl. *Limit*)	3	Maksimalus SSH jungčių skaičius nustatytu laikotarpiu
SSH Limito sprogimo rodiklis (angl. *Limit burst*)	5	Nurodo didžiausią ištisinę užklausų seriją prieš pradedant limituoti aukščiau nurodytą ribą.
HTTP(S) Limito periodas (angl. *Limit period*)	Sekundė	Taisyklės sąlygų atitikimo laikotarpio trukmė.
HTTP(S) Limitas (angl. *Limit*)	15 (20)	Maksimalus HTTP(S) jungčių skaičius per nustatytą laikotarpį.
HTTP(S) Limito sprogimo rodiklis (angl. *Limit burst*)	25 (30)	Nurodo didžiausią ištisinę užklausų seriją prieš pradedant limituoti aukščiau nurodytą ribą.

HTTP atakos principas, tai kai užpuolikas siunčia visą HTTP antraštę, kurioje yra laukas „turinio ilgis“, kad būtų nurodytas sektino pranešimo teksto dydis. Tačiau užpuolikas siunčia tikrąjį

pranešimo turinį labai lėtai (pvz., 1 baitas / 100 sekundžių). Kadangi visas pranešimas yra teisingas ir užbaigtas, tikslinis įrenginys bandys paklusti laukui „turinio ilgis“. antraštėje ir lauks, kol bus perduotas visas pranešimo tekstas. Tokiu būdų įrenginys gali būti sulėtinimas arba visiškai užlaužiamas.



3.20 pav. Prievadų skenavimo atakos apsauga

Įjungus prievadų skenavimo atakos apsaugos funkciją, suteikiama galimybė vartotojui įjungti apsaugą nuo tam tikrų tipų užklausų atakų.

Pasinaudojant visomis prieinamomis apsaugos funkcijomis, užtikriname, kad įrenginys yra atsparesnis nuo įvairių tipų atakų. Tai padeda dar labiau užtikrinti kibernetinės saugos stiprumą objekto kompiuteriniame tinkle.

3.5. Interneto prieigos užtikrinimas įrenginiuose

Nenutrūkstama interneto prieiga objekto kompiuterinio tinklų įrenginiuose yra labai svarbus faktorius. Nutolę tinklo įrenginiai, turėdami interneto prieigą, gali jungtis prie *OpenVPN* serverio, taip užtikrinant, kad nutolusius įrenginius galima pasiekti saugiai. Taip pat, kaupiami duomenys siunčiami į nutolusį serverį, dėl to interneto prieigą irgi yra privaloma. Ofiso maršrutizatorius, RUTX11, taip pat visada turėti interneto prieigą. Šis maršrutizatorius veikia kaip *OpenVPN* serveris, prie jo prisijungę tinklo inžinieriai gali pasiekti *OpenVPN* klientus, kurie yra nutolę įrenginiai. Norint, kad *OpenVPN* serveris būtų aktyvūs ir nutolę įrenginiai pasiekiami, interneto prieigą ir viešasis IP

adresas yra privalomas. Taip pat, ofiso darbuotojai visą darbo dieną turi turėti interneto prieigą, kad galėtų atlikti ne tik nutolusių įrenginių monitoringą bei valdymą, bet ir kad galėtų užsiimti kitais darbais, reikalaujančiais interneto.

Interneto prieigos užtikrinimui, pasitelkiamos RutOS operacinės sistemos funkcijos, leidžiančios turėti kelias skirtingas WAN sąsajas, bei automatiškai jas keisti, priklausomai nuo sąlygų. Tiek RUT956, tiek RUTX11 įrenginiuose yra automatinė WAN sąsajų perjungimų funkcija (angl. *Failover*). Ši funkcija leidžia sukurti atsarginę pirminio WAN ryšio alternatyvą, jei ji nutrūktų. Pagrindinė bei atsarginės WAN sąsajos nurodomos lentelėje.

18 lentelė. Pagrindinės bei atsarginės WAN sąsajos

	RUT956_1 – RUT956_5	**RUTX11**
SIM1 WAN	Pagrindinė WAN sąsaja. Iš interneto tiekėjo gaunamas privatus IP adresas.	Pagrindinė WAN sąsaja. Iš interneto tiekėjo gaunamas viešasis IP adresas.
SIM2 WAN	Atsarginė WAN sąsaja. Iš interneto tiekėjo gaunamas viešasis IP adresas.	Atsarginė WAN sąsaja. Iš interneto tiekėjo gaunamas privatus IP adresas.
Wi-Fi	-	Atsarginė WAN sąsaja. Iš interneto tiekėjo maršrutizatoriaus gaunamas privatus IP adresas.
Laidinis WAN	-	Atsarginė WAN sąsaja. Iš interneto tiekėjo maršrutizatoriaus gaunamas privatus IP adresas.

Pagal pateiktą lentelę, matome, kad nutolę tinklo įrenginiai RUT956 turi vieną pagrindinę WAN sąsają ir vieną atsarginę WAN sąsają. RUT956 įrenginių pagrindinės WAN sąsajos IP adresas yra privatus, vadinasi per šį IP adresą niekas negali pasiekti įrangos iš išorinio tinklo. Atsarginės RUT956 įrenginių WAN sąsajos IP adresas yra viešasis. Taip buvo nuspręsta pagrindžiant, kad jeigu pagrindinė WAN sąsają atsijungtų, būtų prarandamas įrenginio pasiekiamumas per *OpenVPN* tinklą. Tokiu būdu, atsijungus pagrindei WAN sąsajai, įrenginys persijungtų ant atsarginės ir gavus viešąjį IP adresą, įrenginį vis tiek būtų galimą pasiekti, prisijungti ir išsiaiškinti kodėl pagrindinė WAN sąsaja neaktyvi.

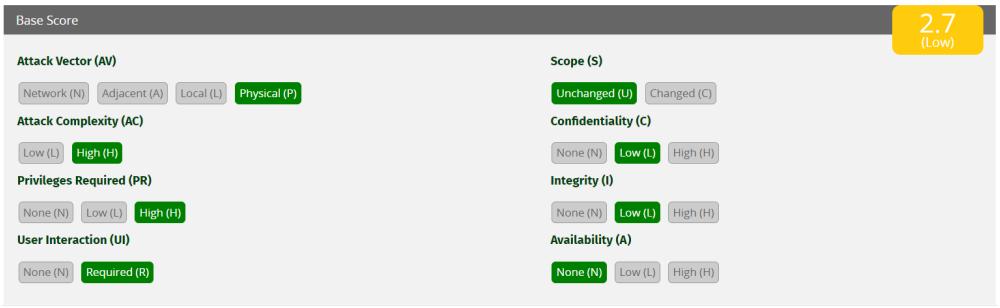
Ofiso maršrutizatoriaus RUTX11 pagrindinės WAN sąsajos IP adresas yra viešasis, nes to reikalaujama konfigūruojant *OpenVPN* serverį. Atsarginės WAN sąsajos yra 3 – WiFi WAN, laidu pajungtas WAN, antra SIM kortelė. Jeigu nulūžtų interneto prieiga iš pagrindinio WAN, *OpenVPN* serveris nustotų veikti, vadinasi nutolę įrenginiai taptų nepasiekiami. Tačiau, interneto prieigą darbuotojam vis tiek bus teikiama ir jie galės toliau darbuotis nepertraukiamai.

Atsitikus taip, kad RUTX11 pagrindinė WAN sąsaja nulūžtų ir jos neitų atstatyti, tinklo įrenginius vis tiek reiktų pasiekti, nevažiuojant į objektą. Tam būtų pasitelkiamos SMS žinutes taisyklės. Siunčiant SMS žinutę į nutolusius RUT956, galime per nuotolį pakeisti jų pagrindinę WAN sąsają į atsarginę. Pakeitus WAN sąsają, įrenginiai būtų pasiekiami per viešuosius IP adresus. Tokiu

būdų, būtų galima perkonfigūruoti *OpenVPN* klientų nustatymus, nurodant naują *OpenVPN* serverio viešąjį adresą. Kai klientai taptų vėl pasiekiami per VPN, galima vėl atkeisti WAN sąsają į pagrindinę, suteikiant įrenginiams privačius IP adresus ir atstatant kibernetinės saugos būklę.

3.6. Naujo tinklo pažeidžiamumo įvertinimas CVSS sistemoje

Nustatytas naujas pažeidžiamumo įvertinimo balas CVSS sistemoje. Įvertinus bei nustačius naujo tinklo pažeidžiamumo vektorių reikšmes, gautas įvertinimas yra lygus 2,7 balo. Nustatomas vektorius bei galutinis balas atvaizduojamas 3.21 paveiksle. Išsamūs vektorių pasirinkimo paaiškinimai matomi 4 priede.



3.21 pav. Naujo tinklo nustatytas pažeidžiamumo vektorius bei galutinis balas

Gautas naujasis vektoriaus balas nurodo, kad sistema yra saugi bei atspari kibernetinių nusikaltėlių atakoms. Lyginant pradinio tinklo vektoriaus balą, su naujuoju, sistema tapo 4,5 balais saugesnė.

3.7. Apibendrinimas

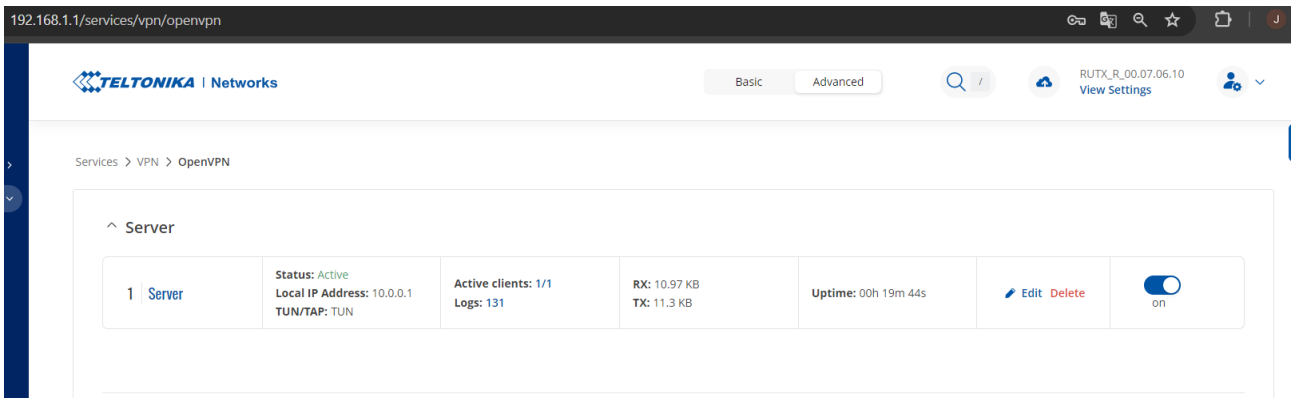
Galime teigti, kad projektuojamas objektas rekonstruotas, žvelgiant iš kibernetinės saugos pusės. Pakeistos technologijos, kaip yra pasiekiami nutolę įrenginiai, iš nesaugios viešųjų adresų technologijos, į saugią VPN technologiją. Sukurta bei įgyvendinta slaptažodžių saugumo politika, nustatytos atakų prevencijos funkcijos, taip uždedant papildomus saugumo sluoksnius. Šie saugumo sprendimai tinklą padaro žymiai atsparesnį kibernetinėms atakoms. Tai patvirtina ir suskaičiuotas naujas CVSS balas, kuris gavosi žymiai mažesnis, negu pradinio tinklo.

4. EKSPERMENTINĖ-PRAKTINĖ DALIS

Eksperimentinę dalį sudaro bandymai susiję su tinklo įrenginių pasiekimu, slaptažodžių saugumu, prieigos blokavimu. Įsitikinant, kad tinklas yra saugus, nutolę įrenginiai privalo būti pasiekiami tik per VPN IP adresus, įrenginių slaptažodžiai turi būti nebe senieji, o naujieji, sudaryti pagal nustatytą slaptažodžių politiką. Bandant nesėkmingai jungtis 3 kartus prie įrenginių, turi būti blokuojama prieiga ir tas atsispindėti grafinėje įrenginio sąsajoje.

4.1. Įrangos pasiekiamumo testavimas

Žinoma, kad nutolę įrenginiai privalo būti pasiekiami tik per *OpenVPN* IP adresus. Įrangos pasiekiamumo testavimo procesas prasideda įjungiant vieną nutolusį įrenginį, prijungiant darbinį kompiuterį prie RUTX11 maršrutizatoriaus, kuris veikia kaip *OpenVPN* serveris ir įsitikinant, kad VPN tunelis yra aktyvus. Prijungėme maršrutizatorių ir grafinėje sąsajoje, matome, kad serverio sąsają yra aktyvi ir kad vienas aktyvus *OpenVPN* klientas yra prisijungęs prie virtualaus tinklo, tai atvaizduojama 4.1 paveiksle.



4.1 pav. VPN serverio aktyvumas, atvaizduojamas grafinėje sąsajoje

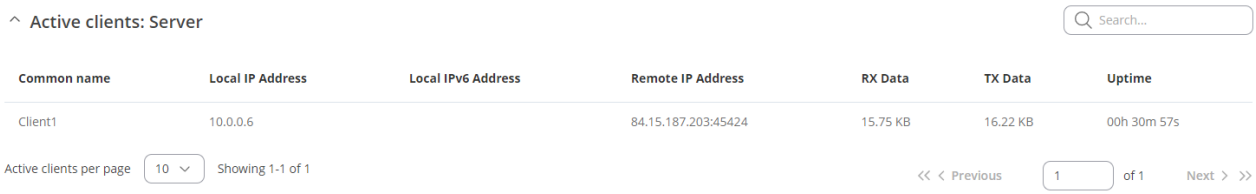
Užtikrinimui, prisijungiame prie RUTX11 maršrutizatoriaus komandinės eilutės ir suvedame */etc/init.d/openvpn* status komandą. Komandos rezultatas matomas 4.2 paveiksle.

```
root@RUTX11:~# /etc/init.d/openvpn status
running
root@RUTX11:~#
```

4.2 pav. */etc/init.d/openvpn* komandos rezutaltas

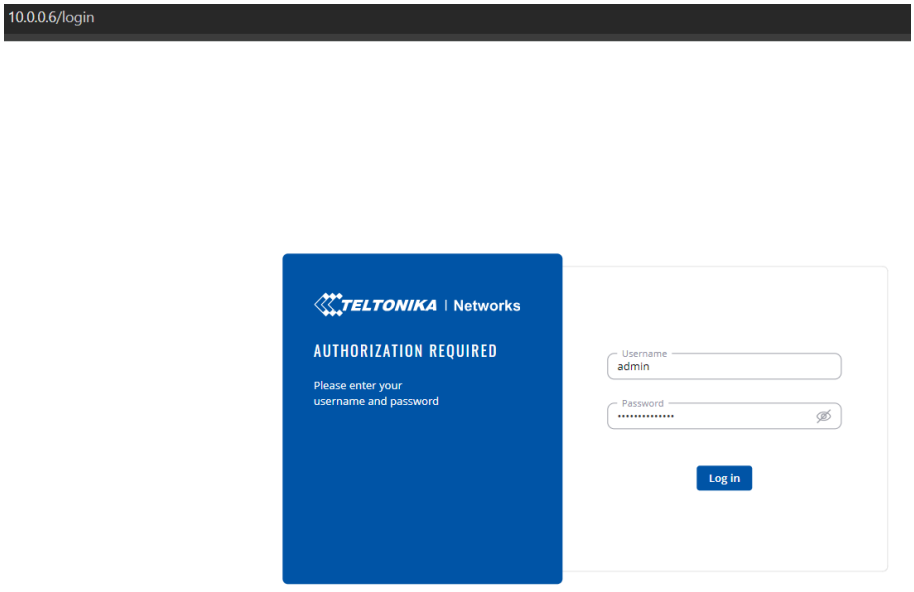
Matoma, kad */etc/init.d/openvpn status* komandos išvestis yra „vykdoma“ (angl. *running*), tai reiškia, kad *OpenVPN* paslauga šiuo metu sistemoje yra veiksni, aktyviai klausosi įeinančias

OpenVPN klientų užklausas jungtis prie VPN tinklo, bei nukreipia srautą atitinkamai pagal konfigūracijas. Įsitikinę, kad *OpenVPN* serveris yra tikrai aktyvūs, turime sužinoti prisijungusio *OpenVPN* kliento VPN IP adresą, per kurį turime pasiekti nutolusį įrenginį. Šią informaciją galime gauti grafinėje sąsajoje, paspaudę ant serverio aktyvių klientų sąrašo. Šis sąrašas atvaizduojamas 4.3 paveiksle.



4.3 pav. Aktyvių *OpenVPN* klientų sąrašas

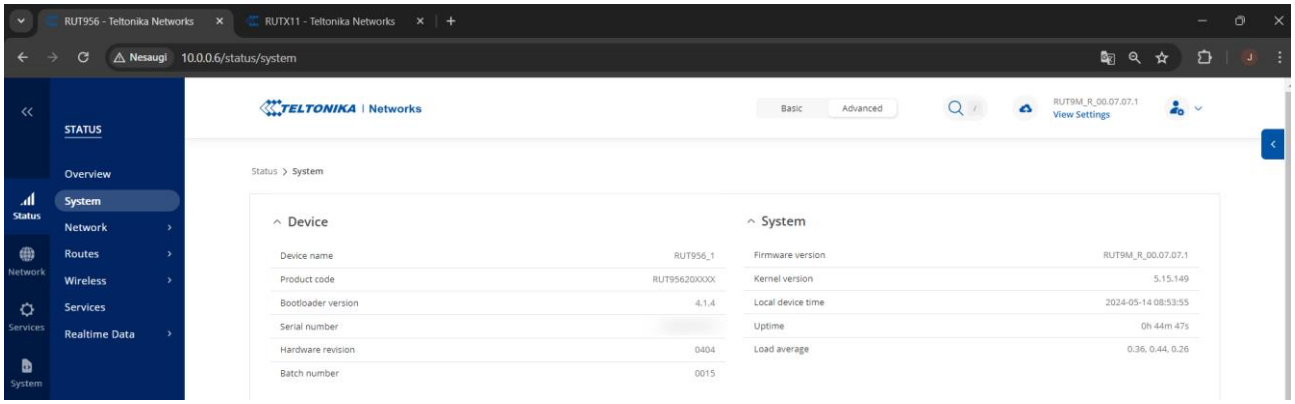
Žinome, kad šiuo metu yra įjungtas tik vienas nutolęs tinklo įrenginys, tai yra RUT956_1. Klientų sąraše, matome šio įrenginio adresą, per kurį jis komunikuoja su *OpenVPN* serveriu. Matomas IP adresas yra pasiekiamas tik per VPN tinklą, tuo įsitikiname pirmiausia bandant pasiekti adresą iš kompiuterio, kuris prijungtas į *OpenVPN* serverį. Įvedus 10.0.0.6 IP adresą į naršyklės paieškos lauką, atidaromas nutolusio įrenginio prisijungimo puslapis, kuriame suvedame reikiamus duomenis, kad prisijungti prie įrenginio. Prisijungimo langas, pasiekiamas per 10.0.0.6 IP adresą, atvaizduojamas 4.4 paveiksle.



4.4 pav. Prisijungimo langas pasiekiamas per *OpenVPN* kliento IP adresą

Suvedus reikiamus duomenis, sėkmingai prisijungiame prie nutolusio įrenginio RUT956_1 per *OpenVPN* IP adresą. Įsitikinimui, ar čia tikrai nutolęs įrenginys, įrenginio grafinėje sąsajoje

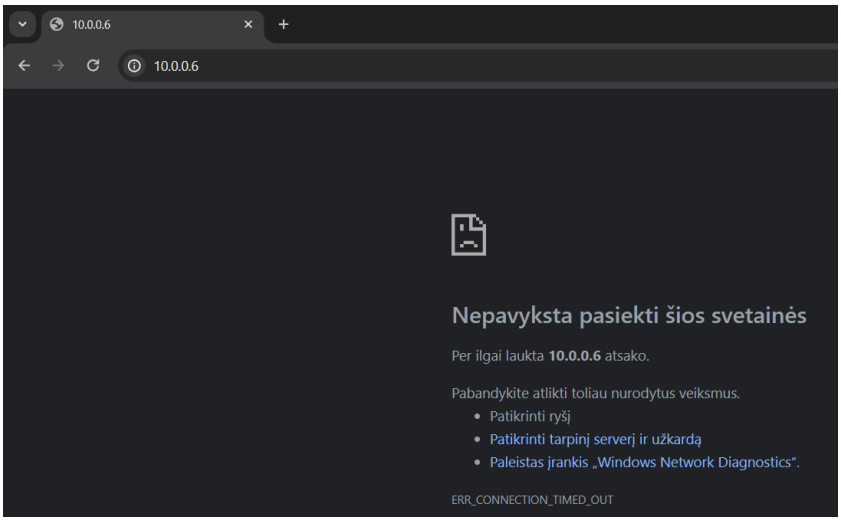
susirandame puslapį, kuriame nurodytas įrenginio pavadinimas. Šis puslapis atvaizduojamas 4.5 paveiksle.



4.5 pav. Įrenginio informacijos puslapis

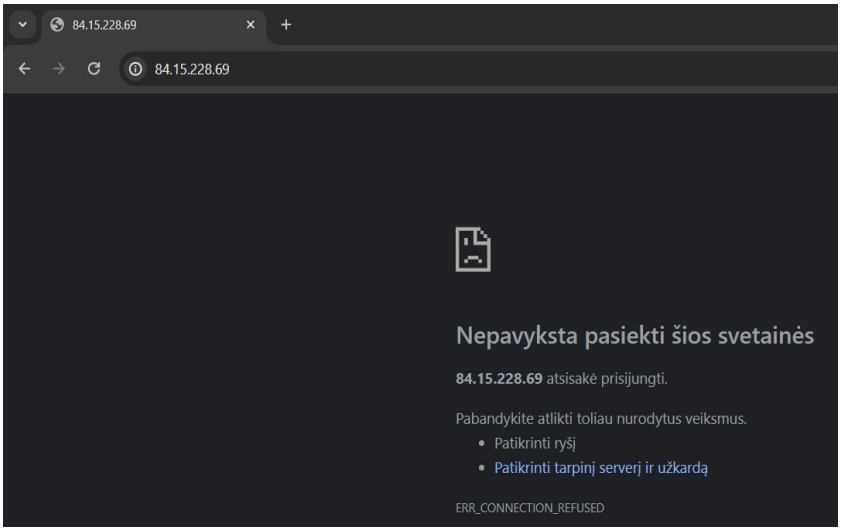
Šiame puslapyje matoma, kad įrenginio pavadinimas (angl. *Device name*) yra RUT956_1, taigi esame pilnai užtikrinti, kad įrenginys, pasiektas per *OpenVPN* kliento IP adresą, yra nutolęs įrenginys. Nutolusių įrenginio pasiekiamumas per VPN tinklą yra sėkmingas.

Antroji šio bandymo dalis yra įsitikinti, kad įrenginys nėra pasiekiamas iš išorinio tinklo per jo VPN IP adresą. Atlikti šį bandymą, atjungiame RUTX11 maršrutizatorių nuo darbinio kompiuterio ir prijungiame kitą internetą tiekiantį įrenginį į darbinį kompiuterį. Tokiu būdų mes esame išoriniame tinkle, o ne VPN tinkle. Atlikus šiuos veiksmus, bandome vėl į naršyklės paieškos lauką įvesti 10.0.0.6 IP adresą, kuris yra nutolusio įrenginio *OpenVPN* adresas. Bandant pasiekti šį adresą iš išorinio tinklo, puslapis yra kraunamas kelias sekundės ir neužkraunamas, o atsiranda „Nepavyksta pasiekti šios svetainės“ užrašas. Tai atvaizduojama 4.6 paveiksle.



4.6 pav. Nepasiekiamas įrenginio IP adresas iš išorinio tinklo

Žinoma, kad RUTX11 turi viešąjį 84.15.228.69 IP adresą, nes to reikalaujama konfigūruojant *OpenVPN* serverį. Tačiau yra užtikrinta, kad per viešąjį IP adresą RUTX11 įrenginio grafinė sąsają nėra pasiekiama per išorinį tinklą. Tai ištestuoti, vedame nurodytą adresą į naršyklės paieškos lauką ir bandome pasiekti įrenginį. Matome, kad įrenginys atsisako prisijungti, vadinasi viskas veikia, taip, kaip buvo suprojektuota. Gaunamas rezultatas atvaizduojamas 4.7 paveiksle.

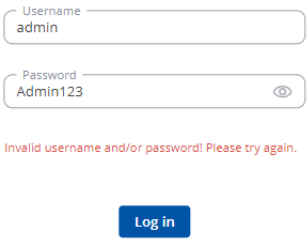


4.7 pav. Bandymas prisijungti per viešąjį RUTX11 IP adresą

Atlikus šiuos pasiekiamumo bandymus, įsitikiname, kad viskas veikia teisingai. Nutolę įrenginiai yra pasiekiami tik per VPN tinklo IP adresus, RUTX11 įrenginys yra nepasiekiamas per viešąjį IP adresą.

4.2. Įrangos slaptažodžių bei prieigos blokavimo testavimas

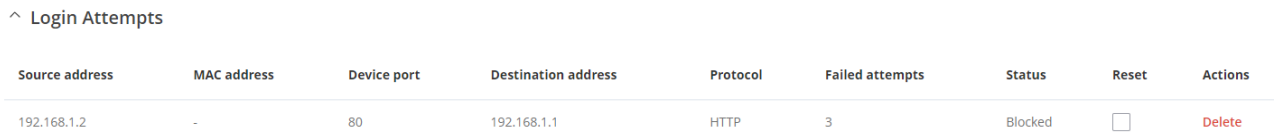
Įrangos slaptažodžių testavimo procesas labai paprastas. Pasiekiame nutolusį įrenginį RUT956_1 per jo VPN IP adresą ir bandome prisijungti su senuoju slaptažodžiu ir naujuoju slaptažodžiu. Vedant senąjį slaptažodį, prisijungti negalima, išvedama, kad slaptažodis neteisingas. Tai atvaizduojama 4.8 paveiksle.



4.8 pav. Nesėkmingas bandymas prisijungti

Su naujuoju 12 simbolių slaptažodis prisijungti galima.

Prieigos blokavimo testavimas vykdomas prijungianti prie RUTX11 dar vieną kompiuterį, skirtą testavimo tikslais ir lokaliai jungdamiesi prie grafinės sąsajos suvedame slaptažodį 3 kartus nesėkmingai. Atlikus šį bandymą, iš testavimo kompiuterio nebegalima pasiekti įrenginio grafinės sąsajos, taip pat, iš kito kompiuterio prisijungus į grafinę sąsają matome, kad yra vienas užblokuotas IP adresas. Tai atvaizduojama 4.9 paveiksle.



4.9 pav. Užblokuotas IP adresas

Galime teigti, kad bandymas yra sėkmingas ir viskas veikia taip, kaip numatyta. Slaptažodžiai įrenginių yra pakeisti į saugius, prieigos blokavimo funkcija veikia nepriekaištingai.

4.3. Apibendrinimas

Galime teigti, kad įrenginių konfigūracijos paruoštos teisingai ir viskas veikia teisingai. Nutolę įrenginiai yra pasiekiami tik iš VPN tinklo per VPN IP adresus, nesaugūs slaptažodžiai pakeisti saugiais, sudarytais vadovaujantys naująja saugių slaptažodžiu politika, prieigos blokavimas veikia taip, kaip numatyta. Visi bandymai atlikti sėkmingai.

5. EKONOMINĖ DALIS

Ekonominėje dalyje įvertinami įrangos pirkimo kaštai, darbo užmokesčio kaštai ir taip sužinomi visi reikalingai kaštai, reikalingi aprūpinti vieną objektą kompiuterinių tinklų įranga.

Įrangos pirkimo kaštai. Objektą sudaro 5 vėjo jėgainės, kiekvienoje jėgainėje yra po 1 Teltonika „RUT956“ maršrutizatorių. Taip pat yra centrinis maršrutizatorius Teltonika „RUTX11“, kurio dėka, galime pasiekti nutolusius įrenginius. Išviso gaunasi, kad reikiami 6 kompiuterinio tinklo įrenginiai, reikalingi projektuojamojo objekto sprendimui įgyvendinti. Taip pat, yra apgalvota apie atvejus, jei reikės greitai keisti nustojusį veikti nutolusį įrenginį ar patį ofiso maršrutizatorių. Priimtas sprendimas, kad ofise visada turėti 5 atsarginius RUT956 įrenginius ir dar 1 atsarginį RUTX11 įrenginį. Taip pat, įskaičiuojamos ir SIM korteles bei jų planai. Užsakomos išvis 24 SIM kortelės, nes į vieną nutolusį įrenginį, taip pat ir į ofiso maršrutizatorių, įsideda 2 SIM korteles, taip pat, užsakoma 12 atsarginių SIM kortelių. Į SIM kortelių kainą, įeina ir interneto plano kaina. Įrenginių kiekiai, kainos bei sumos matomos 19 lentelėje.

19 lentelė. Įrangos pirkimo kaštai

Nr.	Įrangos pavadinimas	Mato vienetas	Kiekis	Kaina, Eur	Suma, Eur
1.	RUT956	vnt.	10	242,00	2420,00
2.	RUTX11	vnt.	2	314,70	619,40
3.	SIM kortelės	vnt.	24	3,00	72,00
				Iš viso, Eur	3111,40
				Taikomas PVM, 21%	653,39
				Suma su PVM, Eur	3764,79

Apskaičiavus sužinome, kad vienam objektui reikalingos įrangos, su atsargine įranga, suma yra 3764,79 eurai.

Darbo užmokesčio kaštai. Norinti sužinoti bendrą viso projekto kainą, reikia įsivertinti projekto trukmę bei apsiskaičiuoti inžinieriaus darbo užmokestį. Inžinierius, pradėsiantis darbą prie naujo objekto, pirmiausia turi konfigūruoti įrenginius, tada juos testuoti ir galiausiai sumontuoti į pačią vėjo jėgainę. Įrenginio montavimo procesas į vėjo jėgainę yra užtikrinimas iš pačio kliento, kuris yra vėjo jėgainių savininkas, pusės. Tai reiškia, kad klientas pasirūpina transportu iki jėgaines, priėjimu ir reikiama įranga, saugiai pasiekti įrenginio montavimo vietą bei jį įmontuoti. Kadangi ši darbo funkcija yra sudėtingesnė ir rizikingesnė, nei įprastos darbo funkcijos, darbuotojas, montuodamas įrenginius, į valandą gauna 20% didesnį darbo užmokestį, nei kad atliktų visas kitas savo darbo funkcijas. Montuoti tenka tik keliais atvejais. Pirmasis, tai kai atsiranda naujas klientas ir visa įrangą yra paruoša naudojimui bei ištestuota. Antrasis atvejis yra, kai jau esama tinklo įrangą vienoje iš vėjo jėgainių nustoja veikti, yra nepasiekiama ir nebesiunčia duomenų. Tokiu atveju, inžinierius išmontuoja seną įrangą ir iškart pakeičia ja veikiančia naująją. Į vėjo jėgainę įmontuoti

vieną įrenginį, su visais pasiruošimo, priėjimo darbais užtrunka apie valandą. Įrenginiai yra montuojami į budeles, kurios pastatytos šalia vėjo jėgainių. Žinant, kad objekte yra 5 vėjo jėgainės, montavimas užims 5 valandas. Šio projekto darbo laiko įvertinimas pateikiamas 20 lentelėje.

20 lentelė. Projekto įgyvendinimo laiko įvertinimas

Darbo Specifika	Darbo trukmė
Įrangos montavimas	5 val.
Įrangos konfigūravimas	80 val.
Įrangos testavimas	16 val.

Šioje įmonėje, tinklų inžinieriaus darbo užmokestis, neatskaičius mokesčių, yra 16,00 eurų į valandą. Žinoma, kad už montavimo darbus inžinierius gauna 20% didesnį valandinį atlyginimą, nei už kitas atliekamas darbo funkcijas, tai už montavimą inžinierius gauna 19,20 eurų į valandą, neatskaičius mokesčių.

Inžinieriaus darbo dieną sudaro 8 valandos, tai įrangos testavimui bus skiriama 16 valandų, įrangos konfigūravimui bus skiriama 80 valandų, o montavimui 5 valandos. Bendrai gaunasi 96 valandos darbo konfigūruojant ir testuojant įrangą, ir 5 valandos montavimo, kad įgyvendinti šį projektą.

Žinodami valandų kiekį bei valandinį įkainį, galime suskaičiuoti inžinieriaus darbo užmokestį neatskaičius mokesčių, dirbant prie šio projekto.

1. 16 Eur. Valandinis įkainis x 96 konfigūravimo ir testavimo trukmė, val. = 1536,00 Eur.
2. 19,20 Eur. Valandinis įkainis x 5 montavimo trukmė, val. = 96,00 Eur.
3. 1536,00 + 96,00 = 1632,00 Eur. Projekto rengėjo atlyginimo, neatskaičius mokesčių, sąnaudos, Eur.

Nuo 1632,00 Eur., darbdavys papildomai turi sumokėti 28,89 Eur. įmoką sodrai. Darbo vietos kaina darbdaviui gaunasi 1660,89 Eur. Šis skaičius gaunamas sudedant atlyginimo sąnaudas su įmoka sodrai (Auditum.lt, 2024).

Projekto sąmata. Žinant įrangos pirkimo kainą bei darbo užmokestį, galime įvertinti visą projekto sąmatą. Projekto sąmatos skaičiavimas pateikiamas 21 lentelėje.

21 lentelė. Projekto sąmatos skaičiavimas

Pavadinimas	Suma, Eur.
Darbo užmokestis	1660,89
Įrangos pirkimas	3677,67
Viso:	5338,56
Administracinės sąnaudos (10%)	533,85
Viso:	5872,41

Projekto įgyvendinimo kaina, gaunama sudėjus darbo užmokesčio sąnaudos bei įrangos pirkimo sąnaudos. Gaunama galutinė projekto įgyvendinimo kaina lygi 5872,41 Eur.

IŠVADOS

1. Išanalizuotas esamas administruojamas įmonės kompiuterinis tinklas, išanalizuotos naudojamos technologijos, skirtos pasiekti tinklo įrangą iš nuotolio. Išanalizuotas esamas tinklas yra nesaugus, aptiktos kelios saugumo spragos. Aptartos saugesnės technologijos, kurios galėtų būti naudojamos.
2. Atlikta tinklo įrenginių vidinių nustatymų analizė bei nustatyta bendra esamo tinklo kibernetinio pažeidžiamumo rizika, kuri lygi 7.2 balo.
3. Parinkta saugi alternatyvi technologija, vadinama VPN, kuri padeda užtikrinti tinklo kibernetinę saugą.
4. Sudarytas projektas įrenginių vidinių nustatymų pakeitimams, siekiant, kad būtų užtikrinimas kuo didesnis įrenginių saugumas ir pasiekiamumas. Sudarytas projektas iš įvairių funkcijų bei taisyklių rinkinių, tokių kaip, saugių slaptažodžių politikos, atakų prevencijos ir atsarginių WAN sąsajų automatinio perjungimo funkcijų.
5. Įgyvendinti projektuojami sprendimai, kurie padidino kibernetinės saugos lygį tiek pačio kompiuterinio tinklo, tiek individualių įrenginių. Paskaičiuotas bei įvertintas naujai suprojektuoto kompiuterinio tinklo kibernetinio pažeidžiamumo rizikos balas, kuris yra 2 kartais mažesnis, negu gautas analizuojant pradinį tinklą.
6. Apskaičiuota projekto įgyvendinimo sąmata, kuri gavosi lygi 5872,41 Eur.

LITERATŪRA IR KITI INFORMACIJOS ŠALTINIAI

1. Ahlawat, S., Anand, A. (2014). *An Introduction to Computer Networking. International Journal of Computer Science and Information Technology Research*: recenzuotų straipsnių rinkinys. https://www.researchpublish.com/upload/book/Computer%20Networking-318.pdf
2. Bendovschi, A. (2015). *Cyber-Attacks – Trends, Patterns and Security Countermeasures*. https://doi.org/10.1016/S2212-5671(15)01077-1
3. Hussain, H. *(2022). Password Security: Best Practices and Management Strategies. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136333*
4. Sharma, Y.K, Kaur, C. *(2020). The vital role of VPN in making secure connection over internet world. International Journal of Recent Technology and Engineering (IJRTE):* recenzuotų straipsnių rinkinys. https://doi.org/10.35940/ijrte.F8335.038620
5. Tasevski, P. (2015). *Password Attacks and Generation Strategies*. https://doi.org/10.13140/RG.2.1.1247.8807

KITI ŠALTINIAI

1. Auditum.lt, (2024). Atlyginimo skaičiuoklė https://www.auditum.lt/index.php/atlyginimu-skaiciuokle/atlyginimo-skaiciuokle.html
2. Bello, G. (2023). *What is HTTP?* https://blog.postman.com/what-is-http/
3. Cloudflare.com, (n.d) *WAN vs. LAN* https://www.cloudflare.com/learning/network-layer/what-is-a-wan/
4. cloudflare.com, (n.d). *What is UDP?* https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/
5. Comptia.org, (n.d). *What Is a Wide Area Network (WAN)?* https://www.comptia.org/content/guides/what-is-a-wide-area-network
6. Coursera.org, (2023). *What Is DHCP?* https://www.coursera.org/articles/dhcp
7. Digicert.com, (n.d). *What are tls/ssl certificates?* https://www.digicert.com/tls-ssl/tls-ssl-certificates
8. Fastercapital.com, (2024). *Network Security: Securing Your Network: IP Insights and Best Practices.* https://fastercapital.com/content/Netwo rk-Security--Securing-Your-Network--IP-Insights-and-Best-Practices.html#Understanding-IP-Addresses-and-Subnets
9. First.org, (n.d). *Common Vulnerability Scoring System.* https://www.first.org/
10. Fortinet.com, (2024). *What Is An IP Address? How Does It Work?* https://www.fortinet.com/resources/cyberglossary/what-is-ip-address

11. French, J. (2023) *Voltage: What are DC and AC Voltage?* https://www.gridpoint.com/blog/vdc-voltage-what-is-vdc-voltage/
12. geeksforgeeks.org, (2024). *What is Transmission Control Protocol (TCP)?* https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/
13. Gillis, A. S. (2023). *LTE (Long-Term Evolution).* https://www.techtarget.c om/searchmobilecomputing/definition/Long-Term-Evolution-LTE
14. KasperskyLAB, (2018*). The dangers of public IPs.* https://www.kaspersky.com/blog/public-ip-dangers/24745/
15. Kelly, J. (2024*). RS-485 Serial Interface Explained* https://www.cuidevices.com/blog/rs-485-serial-interface-explained#what-is-rs-485-
16. Kumar, S. (2023). *What is ISAKMP?* https://www.tutorialspoint.com/internet-security-as sociation-and-key-management-protocol-isakmp
17. Manageengine.com, (2024). *What is SSH?* https://www.manageengine.com/privileged-access-management/what-is-ssh-secure-shell.html
18. Microsoft.com, (n.d.). *Create and use strong passwords. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb*
19. Openvpn.net, (2024). Reference manual for OpenVPN. https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/
20. Passwordmonster.com, (n.d). *How Secure is Your Password?* https://www.passwordmonster.com/
21. Pgitl.com, (2023). *Mitigating the risks of public IP addresses.* https://www.pgitl.com/insights/mitigating-the-risks-of-public-ip-addresses
22. Pol, T. (2024). *What Is HTTPS?* https://www.semrush.com/blog/what-is-https/
23. Ruggedtooling.com, (2018*). What are DDoS attacks?* https://ruggedtooling.com/what-are-ddos-attacks/
24. Teltonika-networks.com, (2024). RUT956 https://teltonika-networks.com/products/routers/rut956
25. Teltonika-networks.com, (2024). RUTX11 https://teltonika-networks.com/products/routers/rutx11
26. uk.rs-online.com, (2023). What is RS-232? https://uk.rs-online.com/web/content/disco very/ideas-and-advice/rs232-guide
27. Usnews.com, (2023). *What Is Wi-Fi?* https://www.usnews.com/360-reviews/privacy/what-is-wifi
28. vodafone.co.uk, (n.d). *What's a SIM card?* https://www.vodafone.co.uk/mobile/best-for/glossary/sim

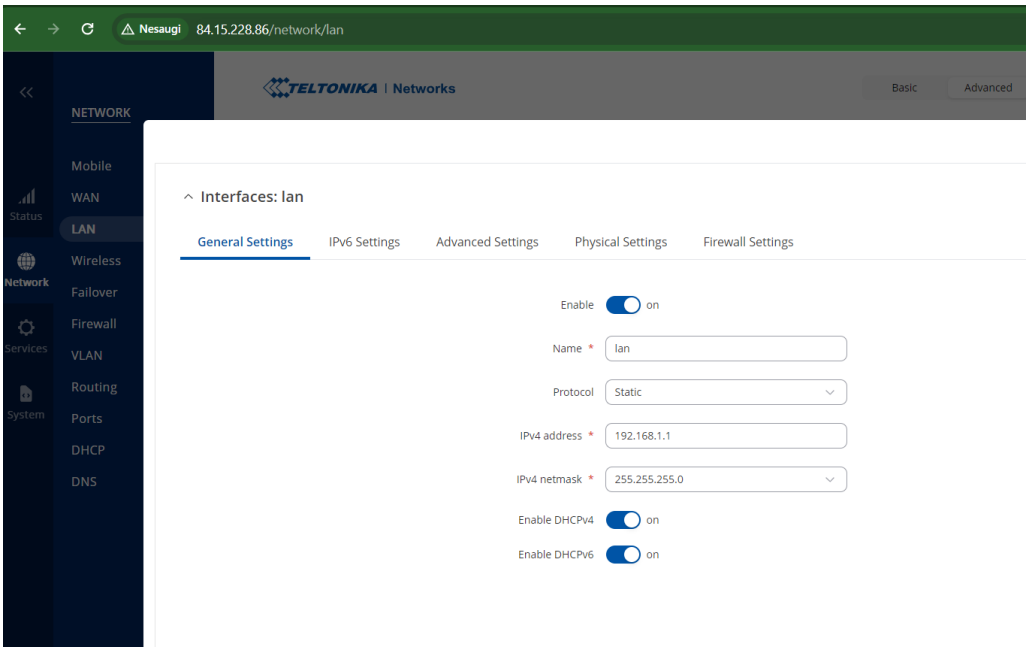
29. Wiki-teltonika.networks.com, (2020). *Teltonika-Networks Operating System – RutOS.* https://wiki.teltonika-networks.com/view/Teltonika-Networks_Operating_System_-_RutOS
30. Wiki-teltonika.networks.com, (2024). *RUT956 Firewall* https://wiki.teltonika-networks.co m/view/RUT956_Firewall#Attack_Prevention

PRIEDAI

1 priedas.

LAN bei WAN konfigūracijų atvaizdavimas įrenginio grafinėje sąsajoje.

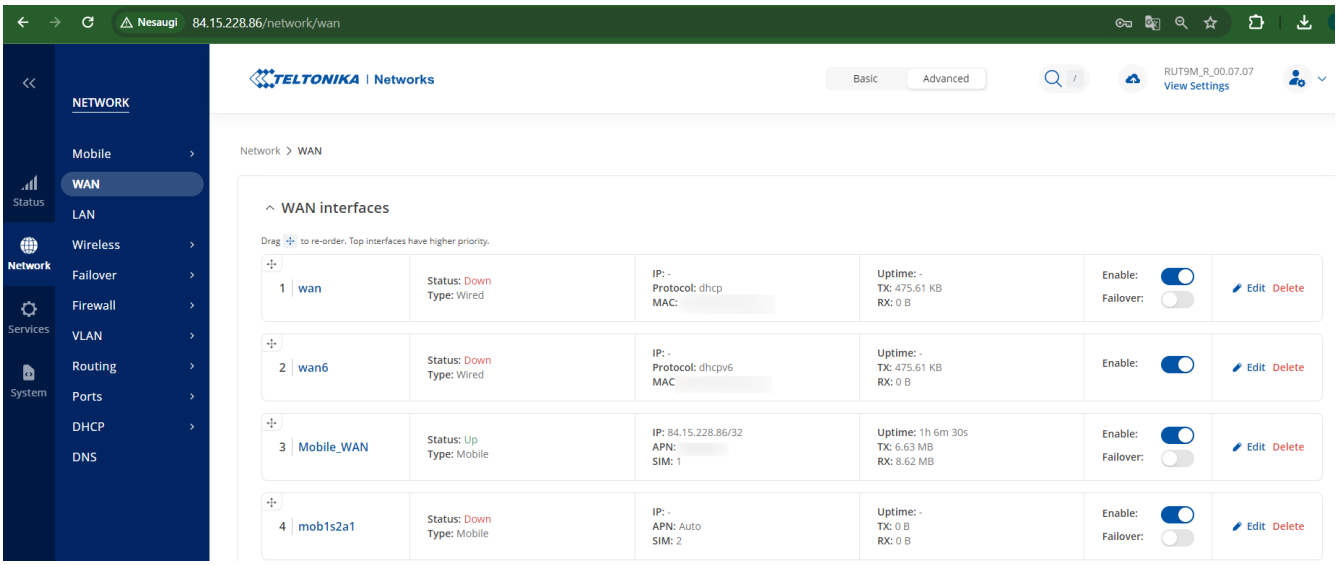
RUTX11 įrenginio grafinėje sąsajoje LAN konfigūracijos atvaizduojamos P1.1 paveiksle.



P1.1 pav. RUTX11 LAN konfigūracijos

Pagal pateiktą P1.1 paveikslą, užsitikriname, kad RUTX11 įrenginio LAN IP adresas yra 192.168.1.1, o potinklis 255.255.255.0.

RUTX11 WAN IP adresas taip pat surandamas grafinėje maršrutizatoriaus sąsajoje ir atvaizduojamas P1.2 paveiksle.



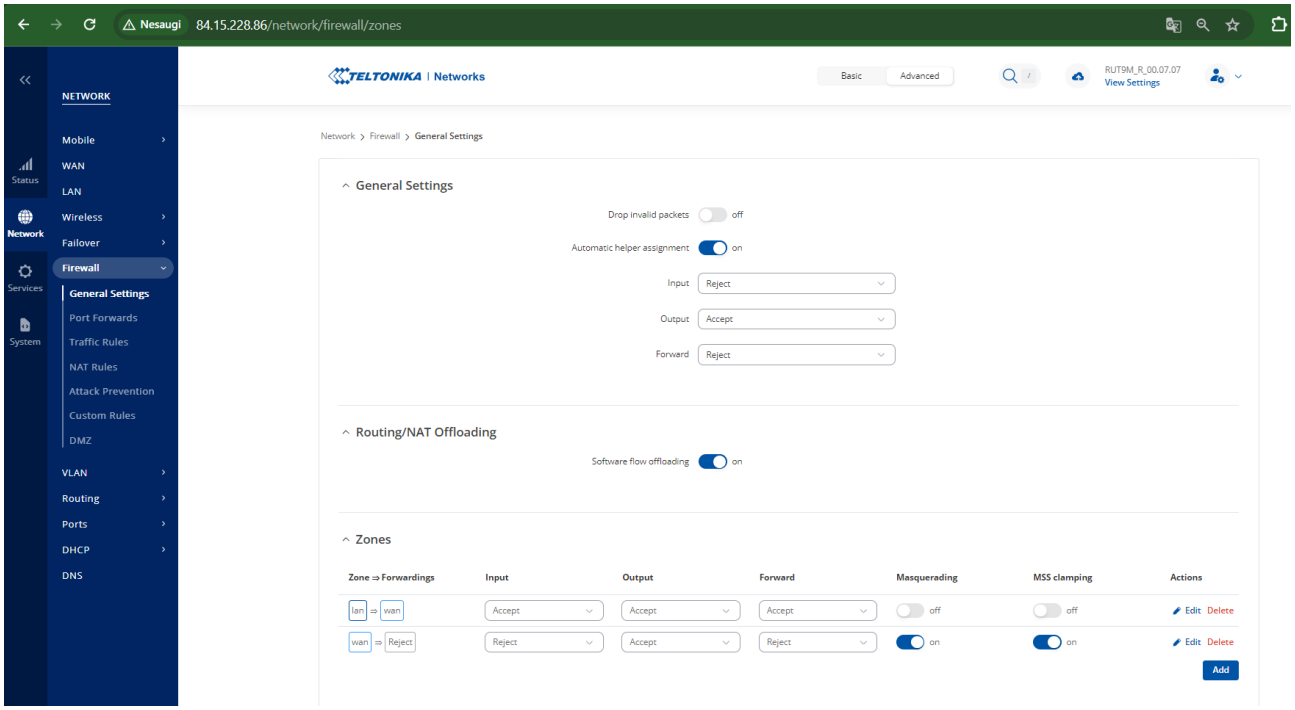
P1.2 pav. RUTX11 WAN konfigūracijos

Pagal pateiktą P1.2 paveikslą, užsitikriname, kad RUTX11 įrenginio WAN IP adresas yra 84.15.228.86

2 priedas.

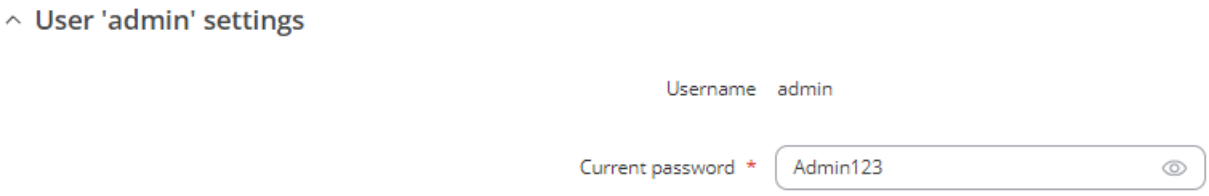
Ugniasienės ir slaptažodžio nustatymų atvaizdavimas.

Ugniasienės bendrieji nustatymai, matomi grafinėje sąsajoje, atvaizduojami P2.1 paveiksle.



P2.1 pav. Ugniasienės bendrieji nustatymai

Naudojamas numatytasis Admin123 įrenginio slaptažodis matomas P2.2 paveiksle.



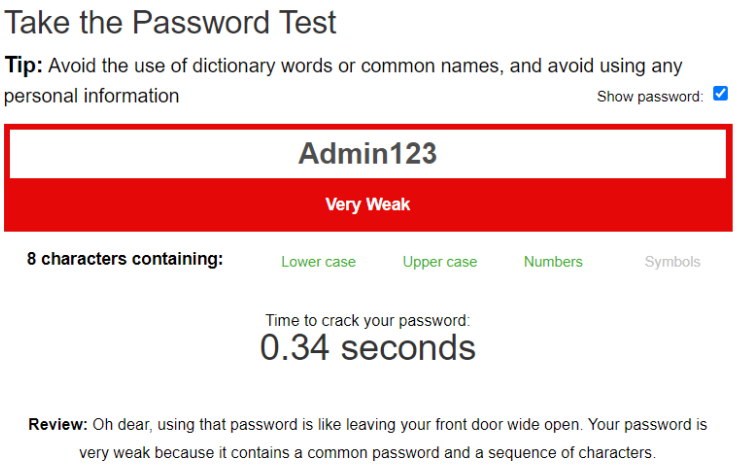
P2.2 pav. Numatytojo slaptažodžio atvaizdavimas

.

3 priedas.

Slaptažodžio nulaužimo laikas.

Numatytojo slaptažodžio „Admin123“ nulaužimo laiko įvertinimas viešai prieinamu įrankiu matomas P3.1 paveiksle.



P3.1 pav. Numatytojo slaptažodžio nulaužimo laikas

4 priedas.

CVSS vektoriaus detalus skaičiavimas.

Atakos per tinklą vektoriaus įvertinimas. Ši metrika atspindi kontekstą, iš kur galimas pažeidžiamumo išnaudojimas. Atakos vektoriaus metrikos įvertinimai paaiškinami P4.1 lentelėje.

P4.1 lentelė. Atakos per tinklą vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Sąlyga	Taip/ Ne	Veiksmas	Žymė-jimas	Balas	Paaiškinimas
Ar atakuotojas išnaudoja pažeidžiamumą per tinklą	Taip	Ar pažeidžiamumas galimas programiškai?	Ne	Pažeidžiamumas galimas iš nutolusio tinklo	N	0,85	Sename tinkle : Tinklo įrenginiai yra pasiekiami per viešuosius IP adresus, todėl bet kas, turintys prieiga prie interneto, gali bandyti užpulti tinklo įrenginius.
			Taip	Atakos yra sąlygotas informacijos perdavimo protokolo?	A	0,62	
	Ne	Ar pažeidžiamumas galimas fiziškai prisijungus prie tinklo?	NE	Ar pažeidžiamumas galimas naudojant vietinę taikomąją programą ir jungiantis lokaliai	L	0,55	
			Taip	Atakuotojas turi fiziškai prisijungti prie taikinio	P	0.2	Naujame tinkle : Tinklo įrenginiai yra pasiekiami tik per VPN adresus, o juos galima pasiekti tik prisijungus prie VPN serverio.

Senojo tinklo įvertinimas: AV:N=0,85

Naujojo tinkle įvertinimas: AV:P=0,22

Atakos sudėtingumo vektoriaus įvertinimas. Ši metrika apibūdina sąlygas, kurių užpuolikas negali kontroliuoti, jos turi egzistuoti be užpuoliko pagalbos, kad būtų įmanoma išnaudoti pažeidžiamumą. Atakos sudėtingumo metrikos įvertinimai paaiškinami P4.2 lentelėje.

P4.2 lentelė. Atakos sudėtingumo vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Veiksmas	Žymė-jimas	Balas	Paaiškinimas
Ar atakuotojas gali savarankiškai panaudoti pažeidžiamumą ?	Taip	Atakuotojas gali panaudoti pažeidžiamumo bet kuriuo metu	L	0,77	Sename tinkle : Specialiosios sąlygos nėra reikalingos užpuolikui norint patekt į sistemą. Taip pat, užpuolikas gali sėkmingai atkartoti ataką prieš tinklo komponentą, nes informacinė sistema veikia 24 valandas per parą, nepaliaujamai
	Ne	Atakuotojas gali panaudoti pažeidžiamumo esant tam tikromis sąlygomis	H	0,44	Naujame tinkle: Atakuotojas gali išnaudoti pažeidžiamumą tik fiziškai prisijungęs prie VPN serverio, o tam jam reikėtų patekti į ofiso patalpas.

Senojo tinklo įvertinimas: AC:L=0,77

Naujojo tinklo įvertinimas: AC:H=0,44

Bendradarbiavimo atakos metu vektoriaus įvertinimas. Ši metrika apima būtinybę vartotojo, kuris nėra užpuolikas, o darbuotojas, dalyvauti atakoje. Bendradarbiavimo atakos metu vektoriaus metrikos įvertinimai paaiškinami P4.3 lentelėje.

P4.3 lentelė. Bendradarbiavimo atakos metu vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Veiksmas	Žymė-jimas	Balas	Paaiškinimas
Ar atakuo-tojui reikia kito vartotojo pagalbos atakos įvykdymui?	Ne	Sėkmingai atakai nereikia vartotojų sąveikos (bendradarbiavimo)	N	0,85	Sename tinkle: Užpuolikas gali išnaudoti pažeidžiamą sistemą be jokio tiesioginio bendradarbiavimo su sistemos naudotojais. Užpuolikas gali bandyti tiesiogiai paveikti sistemą, pagal savo nusistatytus tikslus, neturėdamas jokio bendravimo su sistemos naudotojais.
	Taip	Sėkmingai atakai reikia vartotojų sąveikos (bendradarbiavimo)	R	0,62	Naujame tinkle: Ataka prieš tinklo įrenginius galima tik iš VPN serverio pusės, tam atakuotojui reiktų fiziškai prisėsti prie darbinio kompiuterio, suvesti jo slaptažodį, jungiantis prie nutolusių įrenginių, vėl reiktų suvesti slaptažodžius, kuriuos turi tik autorizuotas darbuotojas.

Senojo tinklo įvertinimas: UI:N=0,85

Naujojo tinklo įvertinimas: UI:R=0,62

Atakuotojo privilegijų vektoriaus įvertinimas. Ši metrika apibūdina privilegijų, kurias privalo turėti užpuolikas, kad sėkmingai išnaudotų pažeidžiamumą, lygį. Atakuotojo privilegijų vektoriaus metrikos įvertinimai paaiškinami P4.4 lentelėje.

P4.4 lentelė. Atakuotojo privilegijų vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Sąlyga	Taip/ Ne	Veiksmas	Žymė-jimas	Balas	Paaiškinimas
Ar atakuotojas turi būti autorizuotas prie pažeidžiamo komponento prieš pradedant ataką?	NE	Atakuotojas neautorizuotas	Ne		N	0,85	
	Taip	Ar reikia administratoriaus teisių	NE	Reikalinga vartotojo lygmens prieiga	L	0,62	
			Taip	Reikalinga administratoriaus lygmens prieiga	H	0.27	Užpuolikas privalo gauti administratoriaus vartotojo teises, su kuriomis įgaunamas didžiausias įmanomas komponento valdymas.

Senojo tinklo įvertinimas: PR:H=0,27

Naujojo tinklo įvertinimas: PR:H=0,27

Atakuotojo aprėpties vektoriaus įvertinimas. Vieno komponento pažeidžiamumo galimybė paveikti kitus išteklius. Atakuotojo aprėpties vektoriaus metrikos įvertinimai paaiškinami P4.5 lentelėje.

P4.5 lentelė. Atakuotojo aprėpties vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Veiksmas	Žymė-jimas	Balas	Paaiškinimas
Ar atakuotojas gali paveikti komponentą, kurio autorystė skiriasi nuo pažeidžiamo komponento autorystės?	Taip	Įtaka atsiranda iš sistemos, kuriais nepriklauso pažeidžiamas komponentas	C	0,00	
	Taip	Įtaka atsiranda sistemoje, kuriai priklauso pažeidžiamas komponentas	U	0,00	Sename tinkle: Išnaudojant pažeidžiamumą yra paveikiama visa sistema, kuri yra už pažeisto komponento ribų. Tai reiškia, kad svarbi ne tik pažeista sistemos dalis, bet jos įtaka visam sistemos darbui. Naujame tinkle: Išlieka ta pati.

Senojo tinklo įvertinimas: S:C=0,00

Naujojo tinklo įvertinimas: S:C=0,00

Įtakos konfidencialumui vektoriaus įvertinimas. Ši metrika vertina komponento valdomų išteklių konfidencialumą sėkmingai išnaudoto pažeidžiamumo atveju. Įtakos konfidencialumui vektoriaus metrikos įvertinimai paaiškinami P4.6 lentelėje.

P4.6 lentelė. Įtakos konfidencialumui vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Sąlyga	Taip/ Ne	Veiksmas	Žymėjimas	Balas	Paaiškinimas
Ar tai įtakoja informacijos konfidencialumą?	Taip	Ar atakuotojas gali gaut visą informaciją iš komponento; ar informacijos atskleidimas kritiškas	Taip	Visa informacija prieinama atakuotojui; arba kritinė informacija prieinama	H	0,56	Sename tinkle: Visa paveikto komponento informacija tampa prieinama užpuolikui. Kadangi užpuolikas turėtų administratoriaus teises, jis galėtų matyti visus sisteminius failus, taip pat matyti bei modifikuoti duomenų srautą, tiek įeinanti, tiek išeinantį.
			Ne	Kai kuri informacija prieinama arba atakuotojas nevaldo informacijos	L	0,22	Naujame tinkle: Atakuotojui nulaužus VPN serverį, visa VPN serverio informacija būtų jam prieinama, tačiau jis negalėtų prieiti prie informacijos, kuri yra nutolusiuose įrenginiuose.
	Ne	Ar reikia administratoriaus teisių	NE	Informacija neatskleidžiama	N	0,00	

Senojo tinklo įvertinimas: C:H=0,56

Naujojo tinklo įvertinimas: C:L=0,22

Įtakos integralumui vektoriaus įvertinimas. Metrika įvertina sėkmingai išnaudoto pažeidžiamumo įtaką vientisumui. Įtakos integralumui vektoriaus metrikos įvertinimai paaiškinami P4.7 lentelėje.

P4.7 lentelė. Įtakos integralumui vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Sąlyga	Taip/ Ne	Veiksmas	Žymėjimas	Balas	Paaiškinimas
Ar tai įtakoja informacijos integralumą?	Taip	Ar atakuotojas gali keisti informaciją atakuojamame komponente; ar informacijos modifikavimas kritiškas	Taip	Atakuotojas gali modifikuoti nekritinę informaciją; arba kai kurią kritinę informaciją	H	0,56	Sename tinkle: Informacijos integralumas visiškai prarandamas, kadangi užpuolikas galėtų matyti bei modifikuoti visą duomenų srauto informaciją, esančią pažeistame komponente.
			Ne	Kai kuri informacija Gali būti modifikuojama arba atakuotojas negali keisti informacijos kritiškumo laipsnį	L	0,22	Naujame tinkle: Įsilaužęs į VPN serverį, atakuotojas negalės modifikuoti ar sunaikinti informacijos, einančios iš nutolusių įrenginių. Jis galės tik modifikuoti patį VPN serverį.
	Ne		NE	Informacijos integralumas nepažeidžiamas	N	0,00	

Senojo tinklo įvertinimas: I:H=0,56

Naujojo tinklo įvertinimas: I:L=0,22

Įtakos pasiekiamumui vektoriaus įvertinimas. Ši metrika įvertina poveikį pažeisto komponento pasiekiamumui. Įtakos integralumui vektoriaus metrikos įvertinimai paaiškinami P4.8 lentelėje.

P4.8 lentelė. Įtakos pasiekiamumui vektoriaus įvertinimo lentelė

Sąlyga	Taip/ Ne	Sąlyga	Taip/ Ne	Veiksmas	Žymėjimas	Balas	Paaiškinimas
Ar gali būti įtaka informacijos pasiekiamumui?	Taip	Ar atakuotojas gali vykdyti DDOS ataką; ar informacijos šaltinio pasiekiamumas kritinis	Taip	Informacijos šaltinis yra visai nepasiekiamas ar esminiai nepasiekiamas	H	0,56	Sename tinkle: Atakuotojas gali vykdyti DDOS ataką ir jos pasisekimo metu sistema taps visiškai nepasiekiama, o jos pasiekiamumas yra kritinis.
			Ne	Informacijos šaltinio nepasiekiamumas yra nekritinis	L	0,22	
	Ne		Ne	Informacijos pasiekiamumas nepažeidžiamas	N	0,00	Naujame tinkle: Įsilaužėlis negali vykdyti DDoS atakos, nebent jis yra nulaužęs VPN serverį.

Senojo tinklo įvertinimas: A:H=0,56

Naujojo tinklo įvertinimas: A:N=0,00

Seno tinklo gaunamas pažeidžiamumo balas: 7,2

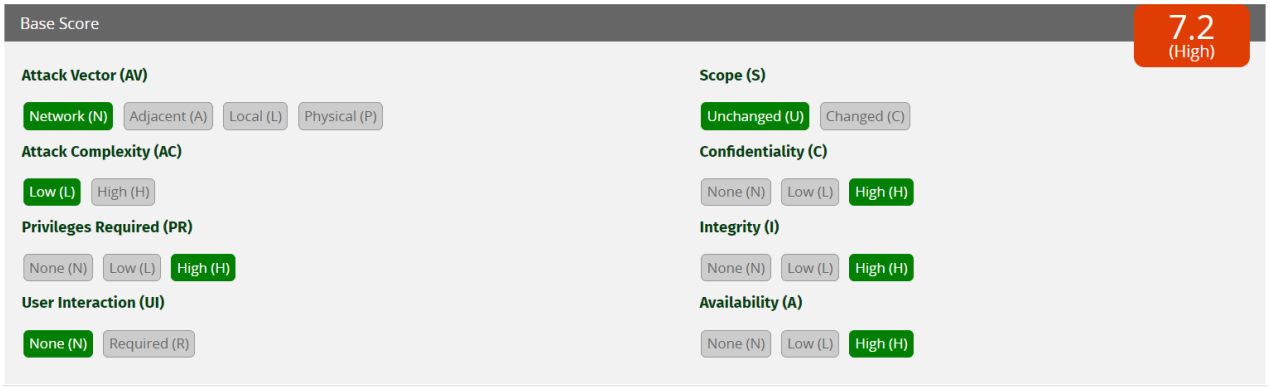
Seno tinklo gaunamas vektorius : CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Seno tinklo vektoriaus nustatymas bei gautas balas atvaizduojamas P4.1 paveiksle.

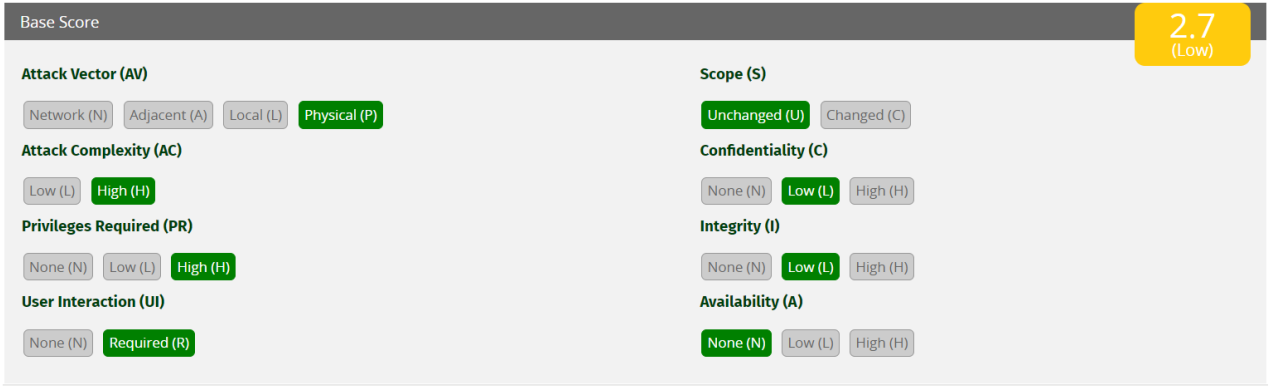
Naujo tinklo gaunamas pažeidžiamumo balas:2,7

Naujo tinklo gaunamas vektorius: CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N

Naujo tinklo vektoriaus nustatymas bei gautas balas atvaizduojamas P4.2 paveiksle.



P4.1 pav. Seno tinklo vektoriaus nustatymas bei gautas balas



P4.2 pav. Naujo tinklo vektoriaus nustatymas bei gautas balas