IMPLEMENTACIJA VATROZIDA NOVE GENERACIJE U SLOŽENO POSLOVNO OKRUŽENJE PREMA NULTO-POVJERENJE MREŽNOM MODELU

Vujković, Dženi

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:399944

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

IMPLEMENTACIJA VATROZIDA NOVE GENERACIJE U SLOŽENO POSLOVNO OKRUŽENJE PREMA NULTO-POVJERENJE MREŽNOM MODELU

Dženi Vujković

Zagreb, veljača 2023.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, 28.02.2023..

Predgovor

Iskreno se zahvaljujem mentoru Karlu Josiću na kvalitetnom usmjeravanju u pisanju ovog završnog rada. Zahvaljujem se i svim predavačima na Algebri koji su mi u kratkom vremenskom roku omogućili znanje širokog spektra tehnologija.

Temeljem članka 8. Pravilnika o završnom radu i završnom ispitu na preddiplomskom studiju Visokogučilišta Algebra sačinjena je ova

Potvrda o dodjeli završnog rada

kojom se potvrđuje da studentica Dženi Vujković, JMBAG 1191193921, OIB 74459567505 u šk. godini 2021./2022., studij: Primjenjeno računarstvo - Preddiplomski studij, smjer: Sistemsko inženjerstvo, od strane povjerenstva za provedbu završnog ispita, dana 17.02.2022. godine, ima odobrenu izradu završnog rada

s temom: **Implementacija vatrozida nove generacije u složeno poslovno okruženje premanulto-povjerenje mrežnom modelu**

i sažetkom rada: Uslijed promjene paradigme o nadzoru mrežnog prometa koji se odvijao isključivo na perimetru mreže, nove smjernice upravljanja mrežnom sigurnošću po modelu "nulto-povjerenje" upućuju na nužnost implementacije internih vatrozida za kontrolu korisničkih pristupa servisima kompanije. U ovome radu biti će prikazan i uspoređen "nulto-povjerenje" model s postojećim modelima upravljanja mrežnom sigurnošću, temeljen na vatrozidima nove generacije tvrtke Fortinet, na primjeru iz prakse u složenom poslovnom okruženju. Prema modelu rada "nulto-povjerenje internivatrozid filtrira promet isključivo na korisnički pristup servisma preko domenskih korisničkih grupa.Rad prikazuje sve potrebne korake za implementaciju vatrozida u korisničko okruženje, te prikazujebenefite i izazove takve implementacije. Prikazat će se važnost temeljitog poznavanja svih servisa koje kompanija koristi u svom svakodnevom radu, te koliko propusti napravljeni od strane sistem inženjera mogu utjecati na sigurnost kompanije.

Mentor je: Karlo Josić.

Odobrenjem završnog rada studentici je omogućen upis kolegija "Izrada završnog projekta/Praksa" te je sukladno članku 8. Pravilnika o završnom radu i završnom ispitu dužan najkasnije do početkanastave ljetnog semestra u sljedećoj školskoj godini, uspješno obraniti završni rad uspješnim polaganjem završnog ispita.

U protivnom studentica može zatražiti novog mentora/icu i temu te ponovo upisati kolegij "Izrada završnog projekta/Praksa" budući da rad koji nije predan i obranjen na završnom ispitu u roku određenom Pravilnikom završnom radu i završnom ispitu prestaje vrijediti. Izrada novog završnog rada se izvodi sukladno rokovima određenima za školsku godinu u kojoj je studentici određen novi mentor/ica i dodijeljen novi završni rad.

Potpis studentice:	Potpis mentora:	Potpis predsjednika povjerenstva:

Sažetak

Rad prikazuje računalnu mrežu zagrebačke tvrtke srednje veličine i nedostatke zatečene u sigurnosnom dijelu postojeće implementacije servisa. Naime, sigurnost mreže korisnika najviše se oslanjala na tradicionalni pristup zaštiti koju pruža rubni vatrozid što je značilo da, ukoliko korisnik primjerice uđe pomoću VPN konekcije u mrežu, ima pravo pristupa na sve poslužitelje i ostalu opremu. Kako bi se pronađene potencijalne ranjivosti uklonile, odlučeno je pratiti najbolje prakse nulto povjerenje mrežnog modela, koje je objašenjeno u prvom dijelu rada. Drugi dio rada prikazuje implementaciju internog segmentacijskog vatrozida, od odabira istog do konfiguracije granularnih pravila filtiranja prometa. Time je omogućen najmanji funkcionalan pristup svakom zaposleniku dok je sve ostalo zabranjeno. Nadalje, rad prikazuje osnovne principe nultog povjerenja, implementaciju po koracima te daje uvid u izazove implementacije takvog rješenja.

Ključne riječi: nulto povjerenje, interni vatrozid, segmentacija mreže, upravljanje mrežnim pristupom

Abstract

This paper shows computer network of a medium-sized Zagreb company and shortcomings found in the security part of the existing service implementation. Namely, the security of the users network relied mostly on the tratitional approach to protection provided by the edge firewall, which meant that if, for example, the user enters the network using a VPN connection, he has the right to access all servers and other equipment. In order to remove the found potential vulnerabilities, it was decided to follow the best practices of the zero-trust network model, whis was explained in the first part of the paper. The second part of the paper shows the implementation of the internal segmentation firewall, from its selection to the configuration of granular traffc filtering uses. This enables the least functional access to each employee while everything else is denied. Furthermore, the paper presents the basic principles of zero-trust, its implementation by steps and provides an insight into the challenges of implementing such a solution.

Key words: zero-trust, internal firewall, network segmentation, network access control

Sadržaj

1. Uvod

Sigurnost informacijskog sustava sastoji se od komponenti poznatih pod nazivom CIA trokut, naziv dolazi od Povjerljivost (engl *Confidentiality*), Integritet (engl *Integrity*) i Dostupnost (engl *Availability*). Povjerljivost se osigurava kriptiranjem, korištenjem korisničkog imena i lozinke te mehanizmima poput višestruke autentifikacije, a definira se većinom korporacijskim sigurnosnim politikama. Integritet označava da su podaci konzistentni za vrijeme cijelog svog životnog ciklusa te da se u prijenosu ne mijenjaju, zato su većinom implementirane zaštite poput *hash* funkcije, no na razini organizacije bitno je prvo dati prava na osjetljive podatke jedino korisnicima koji zaista trebaju pristup istima. Dostupnost se postiže kvalitetnim održavanjem softvera i hardvera kompanije te izradom backupa podataka. Donedavno su organizacije štitile svoj podatkovni prostor isključivo od vanjskih napada no ubrzo se pokazalo kako to nije nimalo kvalitetan pristup zaštiti podataka, jer unutarnje ugroze ponekad mogu i nenamjerno napraviti znatno veću štetu. Rad pojašnjava temeljne principe nulto povjerenje modela, no trenutno je takvo stanje u organizacijama da još uvijek mali broj koristi potpune benefite nultog povjerenje jer izazovi s kojima se susreću prilikom implementacije i možda i manjak svijesti o bitnosti istog rezultiraju parcijalnom implementacijom, što i dalje nije zadovoljavajuće sigurnosno rješenje. Temeljni dio rada je rješavanje nedostataka postojećeg rješenja kod korisnika kroz implementaciju modela nulto povjerenje. Nulto povjerenje je postignuto pomoću internog segmentacijskog vatrozida, a prikazano je stanje prije i nakon migracije prijašenjeg toka prometa na novi vatrozid u mreži. Rad zaključno navodi sve moguće izazove s kojima se organizacije susreću pri implementaciji nulto povjerenje mrežnog modela.

2. Vatrozid

Vatrozidi su sigurnosni uređaji čija primarna namjena je filtriranje ulaznog i izlaznog prometa i time zaštita lokalne mreže organizacije. Vatrozid može biti softverski definiran na samom uređaju korisnika, hardverski mrežni uređaj ili virtualna mašina kod korisnika ili u oblaku proizvođača. Virtualni vatrozidi su sve popularniji i svaki proizvođač vatrozida nudi obje inačice no nameće se pitanje glavne razlike između hardverskog i softverskog rješenja vatrozida. Pogledajmo kako zapravo virtualni uređaj radi: smješten je na nekom hipervizoru lokalno ili u oblaku i moguće je implementirati vatrozid otvorenog koda (engl *Open Source*) i tako dobiti jeftiniji proizvod. No, performanse virtualnih uređaja ovise o tome gdje su smješteni i koliko memorijskih i procesorskih jedinica je za njih alocirano. S druge strane, hardverski vatrozid projektiran je isključivo za tu namjenu i svi njegovi dijelovi služe toj namjeni, primjerice ASCI čip proizveden je da radi jedan jedini zadatak konstanto te pomaže poboljšanju sigurnosti jer može obraditi znatno više podataka i omogućiti akceleraciju rada vatrozida te samim time ponuditi veću brzinu mrežnog prometa. Kod hipervizora postoji veća „površina“ za napad, dok fizički vatrozidi imaju pojačane operacijske sustave kako bi se smanjila mogućnost kompromitiranja sustava. Uostalom, vatrozidi bi trebali štititi hipervizora, a ne obratno.

U idućoj tablici navedene su neke značajke vatrozida te njihove vrijednosti za fizički i virtualni uređaj istog proizvođača:

Značajka	Fizički uređaj	VM – 32CPU, 56 GB
Propusnost aplikacija	43.5 Gbps	28 Gbps
Propusnost zaštite prijetnji	26.7 Gbps	20 Gbps
Propusnost IPSec VPN	21 Gbps	6 Gbps
Konekcija u sekundi	270 000	120 000
Broj sesija	3 600 000	10 000 000
Sigurnosih pravila	30 000	20 000

NAT pravila	6 000	15 000
Adresnih objekata	80 000	40 000
Adresnih grupa	40 000	4 000

Tablica 1 – komparacija performansi virtualnog i fizičkog vatrozida**Pogreška! Izvor reference nije pronađen.** – vlastiti rad autora

Neovisno o vrsti vatrozida, svi filtriraju promet na isti način: po korisniku, uređaju, sadržaju ili aplikaciji, no svaki neautoriziran pristup se zabranjuje. U idućim poglavljima obrađene su teme poput povijesti vatrozida kao i razvoj njihovih značajki kroz desetljeća razvoja istih.

2.1. Povijesni pregled vatrozida

- 1988 Digital Equipement Corporation izbacili Packet-Filter Firewall – paket prometa mogao je proći samo ako je zadovoljavao pravila filtera – izvorišna, odredišna IP, protokoli i portovi na obje strane - radili samo na mrežnom sloju OSI modela – naziv vatrozidi mrežnog sloja ili vatrozidi svjesni samo jedne konekcije (engl *stateless* te se tako dalje i naziva u tekstu)

- 1989 AT&T Bell Labs proizveo Cirsuit Level Gateway – prvi vatrozid svjestan svih konekcija (engl *stateful* i dalje u tekstu tako navođen)– snima sav promet koji prolazi kroz njega, prati sve konekcije. Ako paket ne zadovoljava aktivnu konekciju, evaluira se kroz pravila napravljenih za uspostavljane nove konekcije, te ukoliko zadovoljava te uvjete nove konekcije, propušta se. Promatra se dolazni i odlazni promet zajedno sa stanjima konekcija, popunjava se dinamička tablica u kojoj ostaje samo onaj promet koji je propušten. Sesije spremljene u tablicu brišu se nakon definiranog perioda bez protoka prometa po sesiji. Poznati su kao drugi tip vatrozida mrežnog sloja iako su radili i na transportnom sloju.

- 1991 DEC vatrozid aplikacijskog sloja – treća generacija vatrozida radila je na aplikacijskom sloju analizirajući pritom kompletan softverski promet koji prolazi kroz vatrozid, primarna namjena bila im je zaštita računala od malvera, monitoriran je web promet, FTP, Telnet.. U tom periodu na tržište dolaze i Check Point, Firewall Toolkit i slični.

- 2004 International Data Corporation predstavlja izraz Unified Threat Management (UTM) kojim počinje era zaštite u realnom vremenu koja je omogućila mrežnim inženjerima

promjenu pristupa arhitekturi mreže imajući na raspolaganju paletu alata poput Web Filteringa, Gateway Antivirus, Intrusion Prevention Sastem, Anti-Spam, VPN...

- 2009 uveden pojam Next-Generation FireWall koji obuhvaća sve benefite prijašnjih generacija nadograđene Deep Packet Inspection, Sandboxing, Application Control, URL Filtering, Advanced Malware protection, Network Profiling, Identity Policy

2.1.1. Povijest informacijske sigurnosti

Zaštita osjetljivih podataka kompanije oduvijek je bila mrtva trka s napadačima koji su se do sad pokazali motiviranijima i poprilično često su pronalazili puteve unatoč postavljenim preprekama. Nekad je bilo dovoljno na rubnom usmjerniku ili vatrozidu imati pristupne liste koje su propuštale promet temeljeno na IP adresi, protokolu i portu. No, ubrzo je postalo jasno kolike nedostatke takav pristup donosi.

Potrebe prosječne organizacije su kroz zadnje desetljeće eksponencijalno porasle, posebice od 2020 godine kada je pojavom korona virusa svijet bio primoran promijeniti primarni način funkcioniranja. Mnoge kompanije su bile prisiljene dobrom dijelu radnika omogućiti udaljeni pristup u privatnu mrežu i osjetljivim podacima. Zaštita mreže na perimetru pokazala se ubrzo nedovoljnom te su posljedično nastali mrežni modeli nulto povjerenje.

Područje informacijske sigurnost ne označava samo sigurnost informacija koje koriste tehnologiju kako bi došle od pošiljatelja do primatelja. Pojam informacijske sigurnosti odnosi se na bilo koji oblik sigurnog transporta osjetljivih podataka. Ovaj rad donosi onaj dio temeljen na korištenju mrežnih uređaja u privatnim i javnim mrežama za prenošenje informacija.

2.1.2. Usporedba *stateless*, *stateful* i *proxy* vatrozida

Stateless vatrozidi monitoriraju promet i filtriraju ga po odredišnoj i/ili polaznoj IP adresi ili nekoj drugoj definiranoj statički podešenoj vrijednosti. Po izlasku istih na tržište bili su poznati kao filter paketa. Potpuno su lišeni svijesti o ostalom prometu, svaki paket se proučava zasebno. Statistički se pomoću listi pristupa definiraju izvorišna i/ili odredišna IP adresa, specifičan protokol ili port te smjer. Obzirom da su radili na samo prva tri sloja OSI

modela veće funkcionalnosti i nisu mogli imati. Sve osim definiranih kriterija propuštanja prometa biti će odbačeno kao nedozvoljen promet. Unatoč nemogućnosti praćenja prometa kao cjeline i identificiranja koji tip prometa se analizira stateless vatrozide odlikuje brzina, lakše podnose povećanje prometa te imaju dobar odnos cijene i kvalitete. Naravno sigurnosti aspekt nedostaje jer je poprilično lako probiti ACK bit i izvorišnu IP adresu.

Stateful vatrozidi koriste *stateful* inspekciju prometa tako da dinamički kreira pravila kako bi se dozvolio povratni promet. Za svaku konekciju kreira se sesija i uzima izvorišnu adresu, izvorišni port, TCP sesije, odredišna adresa, odredišni port. Automatski kreira pravilo na vanjskom sučelju koje dozvoljava povratni promet jer je iznutra prema van obično uvijek dozvoljeno. Paketi su analizirani i vatrozid donosi odluke na temelju ostalih koreliranih paketa te aktivno ažurira konekcijske informacije u tablici konekcija. Prate se TCP redni brojevi kako bi se prevenirali potencijalni napadi.

Proxy vatrozidi se smatraju najsigurnijima obzirom da su u stanju raditi s prometom na aplikativnom sloju i mogu brzo i efikasno prepoznati pokušava li neka aplikacija zaobići vatrozid po nekom portu. Zapravo je posrednik između klijenta i servera, a ujedno sprema web stranice i time smanjuje broj zahtjeva. Proxy vatrozid ima odlike da može maskirati server i prema klijentima se ponašati kao server te tek nakon analize prometa isti uputiti prema serveru. Benefiti proxy vatrozida:

- Sigurnost – štite privatne mreže od direktne komunikacije s vanjskim mrežama
- Prikupljanje logova – imaju sposobnost prikupljanja informacija o svim paketima u mreži, što je izuzetno važno kod analize incidenta
- Kontrola i granularnost – nude konfiguraciju pravila za korisnike i grupe i sadrže temeljite logove korisničkog prometa

Eventualni nedostaci su usporavanje prometa mreže zbog alociranja resursa za analizu prometa te ukoliko dođe do prestanka rada takvog vatrozida cijela organizacija je ugrožena.

2.2. Mrežni model nulto povjerenje

Nulto povjerenje (engl *zero-trust*) je sigurnosna strategija koja nalaže kako nipošto ne treba garantirati implicitno povjerenje bilo korisniku, uređaju ili aplikaciji. Nemoguće je postići mrežni model nultog povjerenja uvođenjem samo jedne tehnologije već je više zajedničko udruživanje promišljeno složene mrežne arhitekture i pomno odabranog zaštitnog uređaja, većinom vatrozida. Zbog nemogućnosti određivanja preciznog perimetra privatne mreže

bitno je imati precizno definiran promet. Dosadašnji koncepti povjerenja previše su se oslanjali na ljudsku prirodu što je, očito, prepuno mana. Bez mrežnog modela nultog povjerenja, jednom kad napadač uđe u mrežu, omogućeno mu je potpuno lateralno kretanje bez dodatne provjere. Nulto povjerenje nalaže tri principa implementacije.

- Prvi princip glasi „Nikad ne vjeruj, uvijek potvrdi“ što znači da svaki put kad korisnik, uređaj ili aplikacija požele napraviti novu konekciju taj pokušaj mora biti autentificiran i autoriziran.
- Drugi princip nalaže implementaciju najmanje privilegija kojim se korisnicima, uređajima i aplikacijama dodjeljuje najmanje moguće prava pristupa kako bi rad tekao neometano. Privilegirano upravljanje pristupom omogućuje minimalan pristup primjerice Admin Users domenskoj grupi.
- Treći princip „Očekuj napad“ motivira sve zadužene za mrežnu zaštitu da se pripreme na najgori mogući scenarij te izgrade robusnu i testiranu infrastrukturu kako bi odgovor na napad bio brz i učinkovit, a moguće mete svedene na minimum pomoću segmentacije mreže.

Razlog zbog kojeg je prvi princip postao toliko važan zadnjih godina leži u preseljenju s isključivo hardverske infrastrukture u barem hibridni model računarstva u oblaku što je dovelo do značajnih izazova o kojima se ranije ili nije znalo ili se nije obraća toliko pažnja. Primjerice, koliko organizacija zasigurno zna gdje im se diljem korporacije nalaze osjetljivi podaci? Neke studije navode kako se radi o samo 7% organizacija. Jasno je kako je upravljanje osjetljivim informacijama poprilično teško u hibridnim ili potpunim oblak rješenjima poslovanja. Nulto povjerenje mrežni model napokon je omogućio precizno adresiranje izazova u zaštiti podataka kako bi se omogućilo znanje o lokaciji i zaštiti istih. Današnji model zaštite svodi se zapravo na izazov kako jedino određenom korisniku dati minimalno određena prava kako bi pristupio jedino potrebnim informacijama i jedino s valjanim razlogom.[2]

2.3. Upravljanje pristupom, identitetom i prijetnjama

Upravljanje identitetom i pristupom u suštini odgovara na pitanje tko ima pristup čemu i analizira valjanost pristupa kako bi se isti mogao korigirati u implementaciji nulto povjerenje mrežnog modela. Upravljanje privilegiranim računima je posebna vrsta izazova koja može, ukoliko se ne prate najbolje prakse, dovesti do sigurnosne katastrofe, pogotovo jer većina organizacija prirodno prioritizira eksterne prijetnje. Adaptivna autentifikacija korisnika, posebice u hibridnom oblak okruženju dozvoljava postavljanje nužnog levela multifaktorske

autentifikacije kako bi se omogućio pristup s najmanjim rizikom. U zaštiti podataka bitno je identificirati i klasificirati iste, no primarno je znati gdje se uopće osjetljivi podaci nalaze, bilo da se radi o fizičkoj infrastrukturi ili oblaku. Jedna od najpopularnijih kontrola je enkripcija i upravljanje enkripcijskim ključevima, nakon koje slijedi limitiranje pristupa. Na kraju, najteže je odrediti imaju li korisnici valjan razlog za pristup traženim informacijama. U nulto povjerenje mrežnom modelu sugerira kako bi bilo dobro primijeniti jedan od algoritama za detekciju prijevara u zadanom vremenskom periodu koji će temeljito analizirati pristup osjetljivim podacima. Upravljanje rizikom pristupa osjetljivim podacima posebice kad se radi o infrastrukturi u oblaku omogućuje sanaciju eventualnih pristupnih propusta načinjenim pri implementaciji nultog povjerenja. Upravljanje prijetnjama: Način na koji većina organizacija upralja prijetnjama jest metoda koja omogućuje traženje „igle u plastu sijena“, pronaći sumnjivu aktivnost koja može upućivati na sigurnosni propust. Čak se kaže da nije traženje „igle u plastu sijena“ nego traženje „ igle u plastu igala“ jer u tim situacijama gotovo sve izgleda kao prijetnja. Čak i kad se pronađe navedeni plast igala bitno je biti sposoban prepoznati koja igla je dovoljno oštra da zaista učini štetu te ukoliko postoji takva mogućnost pronaći način da se potencijalna šteta popravi. Prirodan način obuhvaća sakupljanje, organiziranje i monitoriranje logova korištenjem SIEM alata (engl *Security Information Event Management*) no ti alati služe kako bi bilo moguće vidjeti što se već dogodilo. Zato je bitno ozbiljno pristupiti analizi protoka mrežnog prometa i korisničkog ponašanja. U svrhu određivanja koja neobična aktivnost je ujedno i prijetnja moguće je ručno koristiti klasične internet pretraživače no statistika pokazuje da je samo 20% prijetnji indeksirano i moguće pronaći tim načinom. Zato je bitno koristiti jače pretraživače bazirane na umjetnoj inteligenciji koji značajno ubrzavaju analizu potencijalne prijetnje. Nakon pronalaska nužno je da organizacija ima ažuriranu i temeljitu „kuharicu“ za odgovor na incidente.[3]

3. Servisi za implementaciju modela nulto povjerenje

Tradicionalna kontrola pristupa omogućavala je korisnicima i uređajima u mreži potpuno povjerenje, sigurnosni model koji je funkcionirao dobro dok su lokalne mreže bile zaista lokalne, odnosno fizički su se nalazile na jednom geografskom mjestu. Povećanjem broja uređaja interneta stvari (engl *IoT - Internet of Things*) te korporacijskih politika koje dozvoljavaju zaposlenicima donošenje vlastitog uređaja (engl *BYOD – Bring your own device*) dovelo je do povećanja sigurnosnih rizika i tradicionalni pogledi na lokalu mrežu i zaštitu iste više nisu bili dovoljni. Sve navedeno sudjelovalo je u nestajanju tradicionalnog perimetra mreže, a „površina" dostupna za napade je znatno povećana. Nažalost, s vremenom i napadači postaju sve sofisticiraniji, te ukoliko nađu način i uđu u mrežu, bez modela nulto povjerenje imaju pristup svemu unutar mreže. Kako bi se to spriječilo potrebno je uvesti kontinuiranu verifikaciju korisnika i uređaja, granularnu segmentaciju lokalne mreže te povećanjem kontrolnih točaka smanjiti broj pristupnih točaka napadača te omogućiti najmanji funkcionalan pristup svakom korisniku i uređaju. Tako se uklanja predefinirano povjerenje dano autentifikacijom i autorizacijom ulaska u lokalnu mrežu, verifikacija se odvija za svaku korisničku „transakciju" i uvijek iznova nitko u lokalnoj mreži ne posjeduje povjerenje za pristup podacima. Nulto povjerenje pristup (engl *Zero-trust Access*) glavni je element modela nulto povjerenje i fokusira se na informacije tko i kada pristupa mreži. Komponenta zadužena za funkcioniranje nulto povjerenje pristupa je pristup baziran na ulogama (engl *Role-based assecc control – RBAC*) jer tek kad organizacije točno znaju tko je kakav korisnik i kojim podacima treba pristup može se u potpunosti konfigurirati adekvatan pristup korisniku definiran na ulozi korisnika u kompaniji. Nulto povjerenje mrežni pristup je dio nulto povjerenje pristupa koji je prirodno nastao evolucijom udaljenog pristupa mreži organizacije. Većina udaljenog pristupa odvijala se kroz zastarjeli i neefektivan pristup sigurnosti temeljen na postojanju jasnog perimetra mreže. Ukoliko korisnik ima pristupne podatke za udaljeno povezivanje na sigurnosni uređaj na perimetru mreže svi ostali uređaji u mreži su mu predefinirano dostupni. Nulto povjerenje mrežni pristup kreće od premise da je potpuno nebitna lokacija korisnika te garantira pristup aplikacijama bazirano na pojedinim sesijama tek nakon što su korisnik i uređaj uspješno

autentificirani korištenjem multifaktorske autentifikacije i provjere krajnjeg uređaja. Postoje dva načina implementacije nulto povjerenje mrežnog pristupa:

Klijent inicira nulto povjerenje mrežni pristup – pretpostavlja instalaciju agenta na krajnjem uređaju koji kreira siguran tunel. Po zahtjevu korisnika prema određenoj aplikaciji, agent prikuplja informacije o korisniku, uređaju i aplikaciji i kreira sigurnosni profil pristupa. Ukoliko navedeni profil zadovoljava sigurnosne politike organizacije dopušta pristup korisnika prema aplikaciji.

Servis inicira nulto povjerenje mrežni pristup – ne zahtjeva instalaciju agenta na krajnjem uređaju nego koristi pretraživačke dodatke za kreiranje sigurnog tunela. Nedostatak je svakako što je ovakav pristup ograničen na aplikacije u oblaku, jer su aplikacijski protokoli bazirani na HTTP/HTTPS protokolima, smanjen je pristup web aplikacijama i protokolima poput SSH i RDP preko HTTP.

Slika 3.1 Nulto povjerenje jednostavan prikaz[16]

Organizacije bi trebale pažljivo odabrati nulto povjerenje mrežni pristup u postojećoj infrastrukturi jer ukoliko se implementiraju proizvodi različitih proizvođača koji rade na različitim operacijskim sustavima i koriste različite upravljačke konzole što dodatno otežava implementaciju navedenog modela.[14]

3.1. Model nulto povjerenje temeljen na rješenju tvrtke Fortinet

U radu će bit prikazana implementacija modela nulto povjerenje temeljena na proizvodima američke tvrtke Fortinet, te će biti prikazane bitne komponente takvoga rješenja. Fortinet je kreirao platformu koja omogućava kompletan sigurnosni pristup arhitekturi mreže jednostavnom integracijom različitih produkata. Povećanim sposobnostima fizičkih vatrozida poput softverski definiranim širokopojasnim (engl *SD-WAN*) mrežnim mogućnostima poboljšana je sigurnost mrežne infrastrukture u oblaku. Također nulto povjerenje mrežni model od strane Fortineta ne zahtjeva posjedovanje novih licenci već samo uključivanje takvih značajki na obje strane, korisnika i vatrozida. Tako se Fortinet nulto povjerenje sastoji od poznavanja i monitoriranja svakog korisnika, uređaja i aplikacije na mreži. [13]

3.1.1. FortiClient Endpoint Management Server

FortiClient Endpoint Management Sever omogućava skalabilno i centralno nadziranje i upravljanje krajnjim uređajima korisnika. Osim toga EMS štiti krajnje uređaje od virusa i prijetnji poput primjerice ransomware. Ransomware je maliciozan softver koji napada žrtvino računalo i kriptira datoteke. Napadač zaključava žrtvino računalo i tada zahtjeva otkupninu. FortiClient pomaže otkriti i blokirati korisničko računalo, a dovoljno je samo u konfiguraciji EMS-a definirati traženu opciju i željene foldere kao i tipove podataka te potom se definira akcija od FortiClient EMS-a. Moguće je podesiti i backup podataka koji omogućava povratak kriptiranih podataka ukoliko se ransomware ipak dogodi. Ransomware će bit terminiran, korisnik obaviješten i svi podaci vraćeni u početni folder nakon provjere. Osim navedenog primjera, EMS omogućava centralizirano upravljanje krajnjim uređajima, bilo da se radi o udaljenoj konfiguraciji FortiClient softvera na računalo, ažuriranju antiviruse, web filtera ili VPN-a imajući pri tome sve informacije o krajnjem uređaju. Servisi, protokoli i portovi koji se koriste

Komunikacija	Servis	Port
Registracija uređaja	File transfer	8013

Samba	SMB	445
Konekcija prema računalima	DCE-RPC	135
AD server	LDAP	389
Windows	HTTP	80
IIS	HTTPS	443, 10443

Tablica 2 EMS protokoli

FortiClient je lako integrirati u proizvoljan postojeći sustav i na jednom mjestu pratiti definirane sigurnosne politike.

3.1.2. FortiToken

FortiToken je dio Fortinet dvofaktorske autentifikacije, ne zahtjeva instalaciju softvera na strani klijenta. Jednostavan za korištenje, primjerenog odnosa cijene i kvalitete pružajući snažnu autentifikacijsku zaštitu. Jednostavan je upravljanje s administratorske strane, dinamički generirane zaporke minimiziraju izloženost trećoj strani. Aktiviraju se online direktno na FortiGate vatrozidu ili FortiAuthenticatoru korištenjem FortiGuard centra. Jednom kad se aktivira zaporka više nije dostupna na FortiGuard strani, već samo korisniku i to određeni vremenski period. FortiGate posjeduje integrirani autentifikacijski server za validaciju OTP zaporki kao sekundarni autetikacijski faktor za SSL VPN, IPSec VPN, Captive Portal i administrativni login. Time je eliminirana potreba za eksternim Radius serverom koji je inače potreban za dvofaktorsku autentifikaciju.

3.1.3. FortiAuthenticator

FortiAuthenticator je rješenje za upravljanje pristupom i identitetom koje olakšava praćenje korisničkih aktivnosti unutar mreže pritom omogućavajući integraciju i s rješenjima ostalih proizvođača, ne nužno samo Fortinet produkata. Značajke koje nosi sa sobom su:

- Autentifikacija – uključuje udaljenu RADIUS autentifikaciju, TACACS+, LDAP i SAML koje se koriste za razmjenu autentifikacijskih i autorizacijskih podataka između pružatelja identiteta i pružatelja usluge.
- Dvofaktorska autentifikacija – FortiAuthenticator se koristi kao dvofaktorski autenitkacijski server za pružanje jednokratnih zaporki korištenjem FortiToken rješenja, SMS ili elektroničke pošte
- IEEE802.1X – podržava 802.1X za FortGate bežične i žičane mreže
- Identifikacija korisnika – neovisno radi li se o AD, desktop klijentu, gostu portala, RADIUS, Kerberos ili REST API (engl *Represantional State Transfer*) i komunicira ih s FortiGate ili FortiMail u primjeni pravila baziranih na pristupu identitetom
- Upravljanje certifikatima – može kreirati i potpisivati certifikate za korištenje primjerice FortiGate VPN-a

Kao kritičan sustav poželjno je da se nalazi u odvojenoj mreži i da je nemoguć neautoriziran pristup.

3.1.4. FortiAnalyzer

FortiAnalyzer je moćan alat za upravljanje, analizu i prikaz logova unutar cijele organizacije. Orkestrira sigurnosnim alatima, automatizira akcije te odgovara na prijetnje u realnom vremenu. Operativno djeljuje u idućim koracima:

- Registrirani uređaji šalju logove na FortiAnalyzer
- FortiAnalyzer obrađuje i pohranjuje logove
- Administratori imaju uvid povezivanjem pomoću CLI ili jednostavnog GUI sučelja na FortiAnalyzer

Izvještaji sadrže detaljan prikaz mrežnih događaja i aktivnosti i kreira upozorenja ovisno o definiranim uvjetima od strane administratora. Radi u dva načina rada, kao kolektor i kao analizator. Predefinirani način rada je analizator i tada uređaji šalju logove direktno na FortiAnalyzer dok u slučaju rada kao kolektor, više FortiAnalyzer uređaja radi u kolektor načinu rada, njima krajnji uređaji šalju logove, te oni iste prosljeđuju glavnom FortiAnalyzer-u u anaylzer načinu rada čime se poboljšava funkcionalnost. Jednostavan je za integraciju s produktima drugih proizvođača, a dolazi kao fizički uređaj, virtualna mašina, može biti smješten u oblaku ili direktno kod Fortineta. Idealan je produkt za reduciranje kompleksnosti i povećanje automatizacije korištenjem REST API skripti i konektora kako bi se proširio adekvatan sigurnosni odgovor na prijetnje kao i njihova detekcija. Također pruža mogućnost kreiranja vremenskog zapisa incidenta pružajući temeljit vremenski i životni tijek pojedinog incidenta. U konačnici, FortiAnalyzer integrira mrežne logove, analizu i izvještaje na jednoj centralnoj lokaciji.

3.1.5. FortiManager

Čak i u manjim mrežnim infrastrukturama pristup informacijama i aplikacijama brzo pobjegne izvan kontrole i zato je poželjno imati upravljanje svim mrežnim uređajima na za to dediciranoj lokaciji. FortiManager može biti implementiran u oblaku, kao virtualna mašina ili fizički uređaj. Benefiti, osim centraliziranog upravljanja, su centralna konfiguracija svih mrežnih uređaja, zatim postojanje više administrativnih domena (ADOMs) pomoću kojih je olakšan stroži pristup administratorima ovisno o tome na koje uređaje trebaju više ili manje prava pristupa. Olakšava ažuriranje vatrozida kojima upravlja kao i svih značajki na vatrozidima poput antivirusa, web filtera i slično, posebice ukoliko želimo da vatrozidi niti nemaju pristup internetu. Štoviše, moguće je prvo testirati svako ažuriranje prije nego postanu dostupni FortiGate uređajima, posebice kad se radi o ažuriranju softvera i utjecaja ažuriranja na postavke vatrozida i pravila na istom. Podržava automatizaciju skriptama i laku integraciju s FortiAnalyzer-om i ostalim Fortinet produktima, tako da su sve informacije potrebne za temeljitu sigurnost mrežnog prometa dostupne na jednom mjestu.

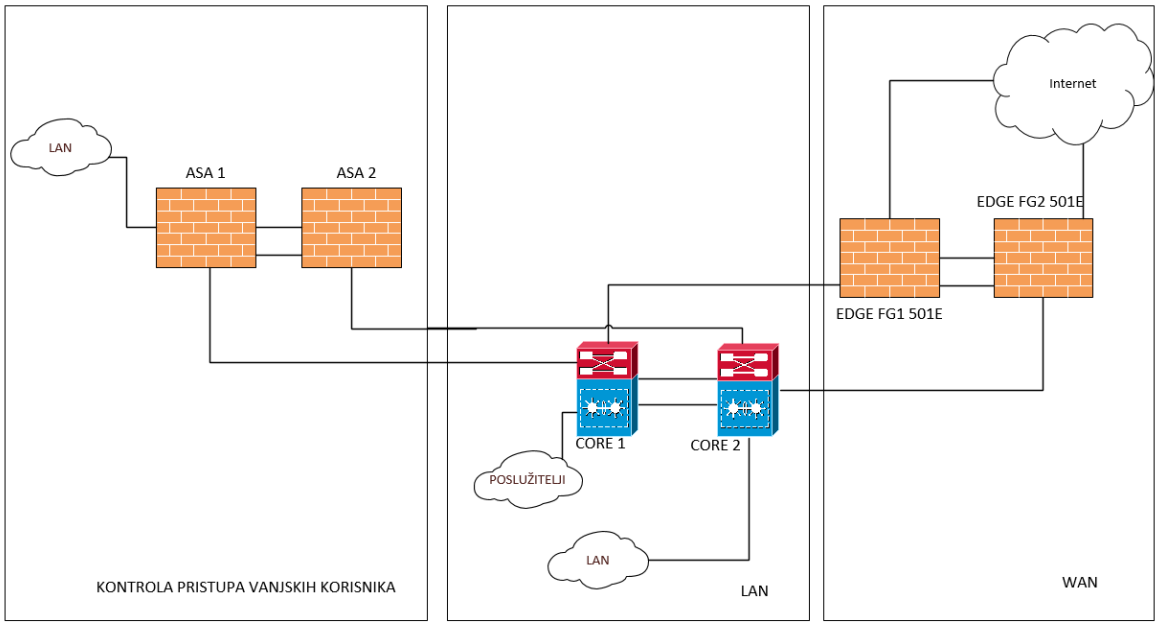
3.2. Vatrozid u službi segmentacije mreže

Segmentacija mreže je jedan od najbitnijih detalja ako je konačan cilj implementacija mrežnog modela nulto povjerenje. Segmentacija se postiže stvaranjem zasebnih logičkih podmreža unutar organizacije. Tako se smanjuje *broadcast* domena, a povećava propusnost (engl *bandwidth*) jer se ukloni nepotreban promet u mreži. Možda najbolji pristup segmentaciji jest postavljanje internog vatrozida unutar mreže organizacije koji će nadzirati i filtrirati sav promet koji se događa u mreži organizacije, ne samo onaj koji dolazi na rubni vatrozid. Tako se izbjegava fizička segmentacija obzirom da virtualna ipak koristi znatno manje preklopnika drugog sloja. Zaštita krajnjih uređaja u tradicionalnoj zaštiti mreže odnosio se na zaštitu uređaja od prijetnji i većinom se bazirao na instalaciji antivirusnog desktop rješenja i pravovremenim ažuriranjem istog. Nažalost, pokazano je kako takav način zaštite nije kompletan i time nije moguće u potpunosti zaštiti kranji uređaj. Mrežni model nulto povjerenje donosi razvoj na tom području pod nazivom detekcija i odgovor krajnjeg uređaja (engl *Endpoint Detection and Response*, kasnije u tekstu EDR). EDR pomoću

agenta na krajnjem uređaju konstantno prikuplja podatke, koristi automatizirane odgovore na prijetnje te analizira iste u realnom vremenu. Po nailasku na prijetnju, EDR koristi segmentaciju mreže kako bi se spriječilo ugrožavanje ostatka mreže. Što granularnija segmentacija mreže, to prijetnja ostaje u manjim okvirima i lakše ju je ukloniti. Segmentacija mreže je jedan od prikladnijih načina osiguravanja najmanjeg a funkcionalnog pristupa podacima organizacije. Interni vatrozidi su jedan od načina kako implementirati nulto povjerenje mrežni pristup pomoću granularne mikrosegmentacije mreže kreiranjem zona povjerenja. Mikrosegmentacija dodaje dinamičke elemente u segmentaciju mrežnog prometa, bazirane na pravilima i tako omogućava kvalitetniji mrežni pristup korisnicima i uređajima.

4. Opis postojeće korisničke infrastrukture

Korisnik posjeduje dvije domene na dvije poprilično bliske lokacije, neka se zovu Domena 1 i Domena 2. Svaka lokacija ima svoje pristupne, distribucijske i jezgrene preklopnike te svoje vatrozide. Na Domeni 1 nalaze se Cisco ASA, a na Domeni 2 FortiGate 501E, na obje lokacije u visokoj dostupnosti. Lokacije su povezane preko Cisco6880 šasija koje se nalaze također u visokoj dostupnosti.



Slika 4.1 Topologija korisničke mreže – vlastiti rad autora

Iduća poglavlja donose zatečena stanja korisničke opreme prije implementacije internog segmentacijskog vatrozida.

4.1. Kontrola pristupa na prvoj lokaciji

Cisco ASA uređaj je vatrozid i u korisničkom okruženju služi za:

- kontrolu udaljenog pristupa na LAN mrežu Korisnika
- kontrolu prometa između logičkih cjelina LAN mreže (VRF-ova)
- kontrolu pristupa Internetu za korisnike koji se nalaze unutar nekog od VRF-ova Korisnika

Ovakav smještaj ASA vatrozida stavlja ga na raskrižje prometa između logički odvojenih cjelina korisničke mreže, što omogućava kontrolu prometa između ranije spomenutih cjelina

na ASA vatrozidu. Kontrola prometa vrši se putem pristupnih lista konfiguriranih na sučeljima. Prilikom prolaska prometa kroz ASA vatrozid događaju se sljedeći koraci:

- Promet stiže na ASA vatrozid na logičko sučelje koje terminira VRF (npr. VRF Internet)
- Provjerava se ishodišna i odredišna IP adresa prometa
- Na temelju odredišne adrese definira se sučelje na koje će promet biti proslijeđen
- Npr. ukoliko je odredište u LAN-u, promet će biti proslijeđen na ulazni sučelje, ukoliko je promet na internetu promet se prosljeđuje na vanjsko sučelje
- Provjerava se pristupna lista primijenjena na dolazno sučelje
- Npr. ukoliko promet dolazi iz VRF-a Internet, provjerava se pristupna lista primjenjena na dolaznom (IN) smjeru na sučelju 'internet'
- Ukoliko promet nije dozvoljen u pristupnoj listi, odbacuje se
- Ukoliko je promet dozvoljen u pristupnoj listi, provjeravaju se NAT pravila
- Promet koji izlazi prema internetu mora biti translatiran na javni IP. U tom slučaju vrši se NAT translacija na javnu IP adresu X.X.X.X
- Promet koji ima odredište u LAN-u ili nekom od VRF-ova u pravilu se ne translatira
- Kreira se zapis o konekciji na ASA vatrozidu kako bi se povratni promet uspješno vratio inicijalnom pošiljatelju
- Povratni promet usmjerava se obratnim redoslijedom te se propušta natrag prema inicijalnom pošiljatelju ako je kreirana konekcija u stateful tablici ASA vatrozida

Promet zaprimljen na nekom od VRF sučelja, a čija se destinacija nalazi na internetu, usmjerava se putem izlaznog sučelja GigabitEthernet0/1 na ASA vatrozidu prema CPE uređajima pružatelja internet usluge. Izlazno sučelje smješteno je u VLAN-u javnog adresnog prostora Korisnika te ima adresu X.X.X.X. Osnovni smjer za promet prema internetu je HSRP IP adresa CPE uređaja Y.Y.Y.Y. Kod Korisnika postavljeni su redundantni ASA uređaji u načinu rada migracije prilikom kvara (engl *Active/Standby Failover*). Spomenuti način rada omogućava da u slučaju pada aktivnog uređaja istovjetni pričuvni uređaj u minimalnom roku preuzme funkcionalnost jedinice koja je postala nedostupna. Jedinica koja je aktivna koristi primarne IP adrese i MAC adrese sučelja, dok jedinica koja je u pričuvi koristi pričuvne adrese koje ne prosljeđuju promet, nego služe samo za komunikaciju između jedinica i za administrativni pristup pričuvnoj jedinici. Na ASA uređaju nije aktiviran niti jedan dinamički usmjerivački protokol, tako da se svi putovi podataka definiraju pomoću statičkih ruta. Sve javne adrese usmjeravaju se prema CPE usmjerivaču pružatelja usluge. Privatne mreže usmjeravaju se prema odgovarajućem sučelju distribucijskih preklopnika (prema odgovarajućem VRF-u). Mreže koje se koriste za IPSec site-to-site tunele usmjeravaju se prema CPE usmjerivaču, odnosno internetu. Sve konekcije inicirane iz lokalne mreže Korisnika prema javnom adresnom prostoru potrebno je translatirati u javne IP adrese čemu služi naredba nat. Od translacija je izuzet promet usmjeren prema adresama VPN korisnika te promet između različitih VRF sučelja ili

ulaznih sučelja na ASA vatrozidu. Ovaj promet se eksplicitno definira kao netranslatiran. Za NAT koristi se manual section konfiguracija. Inicijalno ponašanje ASA uređaja podrazumijeva da se promet iniciran iz mreža s većim sigurnosnim indeksom prema mrežama s manjim indeksom propušta, dok se sav ostali promet blokira. Dodatno, eventualni promet između sučelja s jednakim indeksom bio bi propušten. Na sva sučelja ASA uređaja primijenjene su liste koje služe za preciznije određivanje prometa koji se propušta. Postoji li ovakva lista na sučelju, ona automatski ima veći prioritet od sigurnosnih indeksa i sav se promet provjerava po pravilima iz liste. Dio komunikacijskih protokola za rad koristi više od jedne konekcije, pri čemu su neke od njih inicirane sa strane klijenta, a neke sa strane servera. Pri tome se često kroz već uspostavljene komunikacijske kanale dinamički određuju parametri novih konekcija. ASA uređaj prati konekcije dobro poznatih protokola (primjerice FTP-a) na aplikacijskom sloju i dinamički otvara pristup povratnom prometu koji bi, da nije tako, mogao biti blokiran od strane pristupne liste ili sigurnosnih indeksa. Dubinska inspekcija prometa primjenjuje se naredbom service-policy te se može primijeniti globalno ili na pojedina sučelja. Također, primjenom ranije spomenute naredbe postavljaju se i neka druga ograničena, npr. QoS (engl *Quality of Service*). Na Cisco ASA uređajima omogućen je VPN pristup s interneta, korištenjem Cisco VPN klijenta, koji omogućava uspostavljanje sigurnosnog kanala između udaljenog računala i Cisco ASA uređaja. Korisnici koji se povezuju preko VPN-a grupirani su u nekoliko skupina i sukladno tome im je omogućen pristup različitim segmentima mreže. Za svaku grupu definiran je način autentifikacije koji može biti:

- LOCAL - lokalno kreirani korisnički račun na Cisco ASA uređaju
- LDAP – autentifikacija LDAP-om na Active Directory poslužitelju
- ACS – autentifikacija TACACS+-om na Cisco ACS poslužitelju

Različite grupe korisnika imaju potrebu pristupati različitim skupinama resursa unutar mreže Korisnika. Da bi krajnji korisnik mogao ostvariti pristup resursima, mora se spojiti pomoću Cisco Anyconnect VPN klijenta. Unutar Cisco Anyconnect VPN klijenta, potrebno je unijeti IP adresu ASA vatrozida koja se nalazi na Domena 1. Nakon toga će klijent pokušati uspostaviti komunikaciju s vatrozidom i podesiti SSL VPN tunel.

Na ACS poslužiteljima konfigurirano je dinamičko mapiranje korisnika iz vanjske baze podataka. U ovom slučaju kao direktorij korisnika koristi se domenska baza podataka. Budući da kontroleri bežične mreže ne mogu komunicirati izravno s domenskim kontrolerom, koristi se mapiranje preko ACS poslužitelja.

- Korisnik na WLAN mreži šalje autentifikacije podatke kontroleru bežične mreže u 802.1x EAP okvirima
- Kontroler bežične mreže podatke putem RADIUS paketa prosljeđuje ACS poslužitelju
- ACS poslužitelj u LDAP komunikaciji traži provjeru korisničkih podataka od DC poslužitelja
- DC poslužitelj (domenski kontroler) provjerava ispravnost unesenog korisničkog imena i lozinke te vraća odgovor ACS poslužitelju
- ACS poslužitelj informaciju prosljeđuje kontroleru bežične mreže koji na temelju informacija u RADIUS paketima korisnika autentificira na mreži ili pak odbija povezivanje

4.2. Kontrola prometa na drugoj lokaciji

Na drugoj korisničkoj lokaciji u Domena 1 nalaze se FortiGate501E uređaji podešeni u visokodostupnom načinu rada, čime je osigurano nesmetano funkcioniranje sustava, u slučaju ispada pojedinog uređaja.

Također, uređaji su opremljeni redundantnim napajanjem čime se dodatno podiže dostupnost sustava. Kako bi se osigurala neprekidna komunikacija te nesmetani rad usluga, unutar mreže korisnika postavljena su dva Fortigate 501 E uređaja. Uređaji su podešeni u tzv. Active/Standby načinu rada. U slučaju ispada aktivnog vatrozida iz sustava, standby preuzima aktivnu ulogu. Za sinkronizaciju postavki, kao i za nadgledanje ispravnosti rada „susjednog“ uređaja, koriste se dva „ha“ sučelja, međusobno direktno povezana. Dodatno, podešeno je nadgledanje ispravnosti produkcijski sučelja. U slučaju neispravnosti pojedinog sučelja, pokreće se „failover“ proces. Na Fortigate 501 E uređaju ne postoji konfiguracija za neki od dinamičkih usmjerivačkih protokola, već je svo usmjeravanje promet podešeno pomoću statički definiranih putanji. Sve javne adrese usmjeravaju se prema CPE usmjerivaču pružatelja Internet usluge. Za određene privatne mreže, podešeno je usmjeravanje prema jezgrenom preklopniku. U svrhu sprječavanja petlje unutar mreže, za RFC 1918 (sve privatne adrese) adrese, podešeno je *„Blackhole“* sučelje.

Za korisnike koji pristupaju uređaju iz administrativnih razloga ili ostvarivanja pristupa u VPN, potrebno je izvršiti autentifikaciju i autorizaciju. Radi lakše administracije takvih korisnika, na uređaju su podešeni sustavi čija je namjena centralizirana autentifikacija i autorizacija korisnika. Konkretno, podešeni su protokoli LDAP i RADIUS. Sustavi su podešeni da koriste najmanje dva poslužitelja kako bi se osigurala potrebna funkcionalnost u slučaju nedostupnosti jednog od poslužitelja. Osim standardne inspekcije prometa na razini L3 i L4, Fortigate 501 E uređaj u stanju je analizirati promet i na višim razinama OSI modela.

Konkretno, sav promet koji prolazi kroz uređaj moguće je analizirati na aplikativnoj, tj. L7 razini. Inspekcija prometa na aplikativnoj razini podešava se pomoću tzv. sigurnosnih profila. Ukoliko se želi iskoristiti maksimum od ove tehnologije, potrebno je vršiti SSL inspekciju na samom uređaju. U suprotnome, uređaj neće moći vršiti dubinsku analizu kriptiranog prometa, međutim, unatoč tome, još uvijek je moguće znatno podići razinu sigurnosti korištenjem određenih sigurnosnih profila. Iz tog razloga, na uređaju su podešeni sljedeći sigurnosni profili:

DNS filter – sprječava pristup malicioznim i/ili zabranjenim destinacijama inspekcijom DNS protokola. Korištenjem ove tehnologije, Fortigate 501 E presreće DNS upite prema Internetu, te ukoliko se radi o rezoluciji imena za malicioznu i/ili zabranjenu kategoriju, uređaj ubacuje lažni odgovor te na taj način sprječava pristup sadržaju. Nadalje, budući da se kao odgovor ubacuje unaprijed definirana IP adresa, pregledom zapisa događaja moguće je identificirati računalo koje je pokušalo pristupiti zabranjenom sadržaju.

IPS – korištenjem unaprijed definiranih potpisa te primjenom različitih tehnika prilikom skeniranja prometa, moguće je spriječiti napade usmjerene prema propustima unutar pojedinih aplikacija.

Antivirus – skeniranjem prometa, moguće je spriječiti preuzimanje zaraženog sadržaja s Interneta.

Na Fortigate 501 E uređaju, omogućen je VPN pristup s Interneta, korištenjem Forticlient aplikacije. Ista omogućava uspostavljanje sigurnosnog kanala između udaljenog korisnika i Fortigate 501 E uređaja, odnosno interne mreže Korisnika. Korisnici koji se povezuju putem VPN-a grupirani su određene skupine te im je sukladno istoj omogućen pristup različitim segmentima mreže.

4.3. Nedostaci zatečenog stanja

Trenutno korisničko stanje koristi rubne vatrozide za zaštitu organizacije od ugroza, no jednom kad korisnici prođu početnu autentifikaciju omogućen im je pristup svim internim servisima i uređajima. Potpuno nekontroliran pristup neovisno o ulozi zaposlenika organizacije te jednom nakon što su se identificirali na uređaju bio im je omogućen pristup svim servisima i uređajima u mreži. ASA vatrozid kontrolira VRF povezivanja i kroz definirane VLAN-ove propušta promet, te rubni FortiGate koji prati isključivo promet prema Internetu i udaljeni pristup u organizaciju. Svjestan mogućih ugroza, korisnik je zatražio

implementaciju sigurnijeg rješenja. Predložena je implementacija internog segmentacijskog vatrozida kako bi se u potpunosti pratio i unutranji mrežni promet te osigurao mrežni pristup nulto povjerenje.

4.4. Proces odabira i fizička implementacija internog segmentacijskog vatrozida

Odabiru vatrozida prethodila je analiza korisničkog mrežnog prometa, broj korisnika i njihov način povezivanja u organizaciju, jednostavnost konfiguriranja, odnos cijene i kvalitete te i već postojeća korisnička oprema.

Iduće tablice donose performanse i značajke nekoliko sličnih modela različitih proizvođača:

NAZIV FUNKCIONALNOSTI	**UREĐAJ**			
	Fortigate 501E	**ASA 5545-X w/FirePOWER**	**Palo Alto PA-5020**	**Check Point 5100**
Virtualizacija	✓	✓	✓	✓
Next Generation Firewall	✓	✓	✓	✓
Antivirusna zaštita	✓	✓	✓	✓
Web zaštita	✓	✓	✓	✓
Kontrola aplikacija	✓	✓	✓	✓
Zaštita od upada	✓	✓	✓	✓
Sprječavanje curenja podataka	✓	☒	✓	✓
SSL inspekcija	✓	✓	✓	✓
Centralizirano upravljanje	☒	✓	☒	✓
Izrada izvještaja	☒	✓	✓	✓
Jednostavno upravljanje	✓	☒	✓	✓

Tablica 3 Usporedba značajki različitih proizvođača

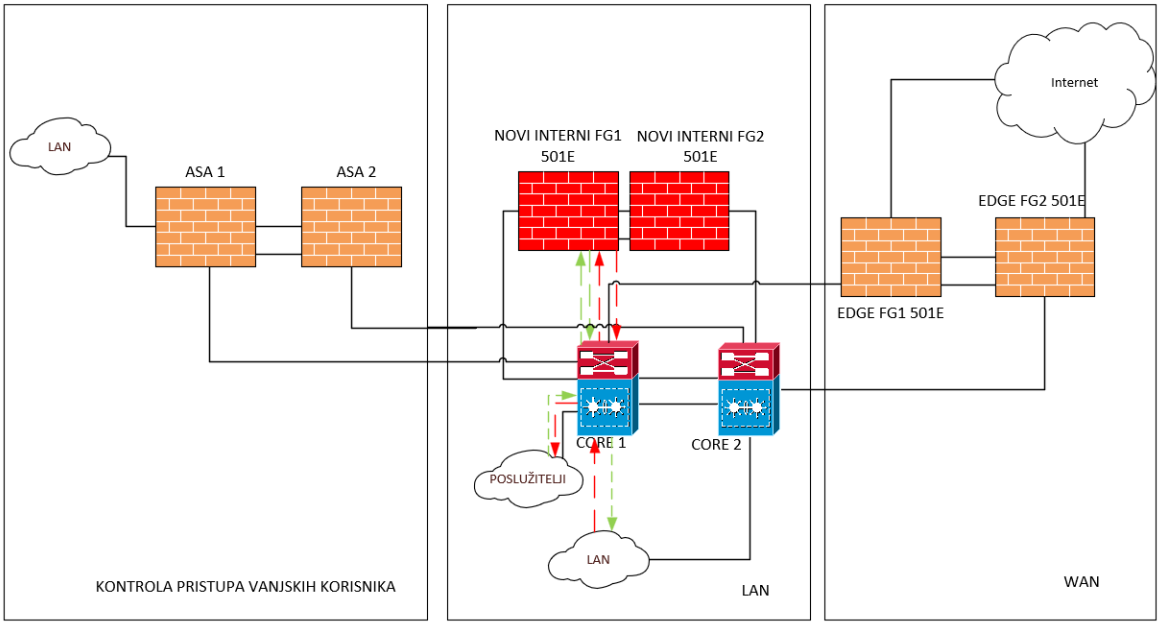
Pregled funkcionalnosti svakog od uređaja donosi iduća tablica:

NAZIV FUNKCIONALNOSTI	UREĐAJ			
	Fortigate 200E	**ASA 5545-X w/FirePOWER**	**Palo Alto PA-5020**	**Check Point 5100**
Propusnost vatrozida	20 / 20 / 9 Gbps	-	-	14.5 Mbps
Propusnost s uključenom kontrolom aplikacija	-	1.5 Gbps	5 Gbps	-
Propusnost s uključenom kontrolom aplikacija i IPS zaštitom	-	1 Gbps	-	2.2 Gbps
Stateful propusnost (maksimalno)[22]	-	3 Gbps	-	-
Stateful propusnost (kombinacija protokola)[23]	-	1.5 Gbps	-	-
Broj istovremenih konekcija	2 miliona	750 000	1 milion	3.2/6.4 miliona
Broj novih konekcija/s	135 000	30 000	120 000	110 000
IPsec VPN propusnost	9 Gbps	400 Mbps	2 Gbps	1.6 Gbps
IPS propusnost	6 / 2.2 Gbps	-	-	2.45 Gbps
Propusnost SSL inspekcije	1 Gbps (IPS, HTTP)	-	-	-

Tablica 4 Usporedba funkcionalnosti između pojedinih modela vatrozida

Zbog količine mrežnog prometa bilo je nužno odabrati fizički uređaj s dostatnom akceleracijom za korisničku infrastrukturu. Nakon usporedbe proizvoda sličnih performansi različitih proizvođača, te uzevši u obzir da korisnik već posjeduje rubni FortiGate 501E vatrozid, donesena je odluka o implementaciji internog segmentacijskog vatrozida FortiGate 501E. Performansama zadovoljava i budući eventualni rast korisničke infrastrukture, zaposlenici u informatičkom odjelu korisnika već imaju dovoljna znanja za održavanje istog, te ono najbitnije, omogućuje traženi mrežni model nulto povjerenje. Nakon odabira uslijedila je fizička implementacija vatrozida.

Korisnik posjeduje dvije glavne server sobe, Soba1 i Soba2 gdje se nalazi sva ostala mrežna oprema. Primarni vatrozid biti će smješten unutar Sobe1, dok će sekundarni biti smješten unutar Sobe2. Zahtjeva se dovoljno mjesta u mrežnim ormarima, potrebna mreža i strujni konektori kako bi oba vatrozida bili zadovoljavajuće instalirani. Po instalaciji vatrozida slijedi povezivanje istih na lokalnu mrežu. Svaki vatrozid povezan je s 1 x 10 GE SFP+ sučeljem na jezgreni preklopnik i to sučelje će bit korišteno za podatkovni promet. Obzirom da vatrozidi imaju samo dva 10 GE SFP+ neće biti korištena agregacija portova kako bi se smanjio trošak implementacije bez ugrožavanja redundancije, a preostalo 10 GE sučelje ostaje slobodno za buduću upotrebu. Kako bi se osigurao klaster u visokoj dostupnosti, vatrozidi koriste dedicirana HA sučelja koja su direktno povezana optikom, bez mrežnog uređaja među njima.



Slika 4.2 Stanje nakon fizičke implementacije – vlastiti rad autora

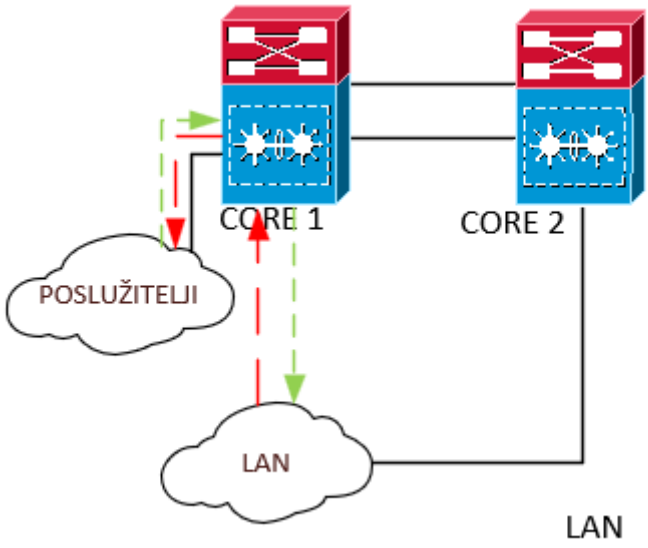
Po ispravnom fizičkom postavljanju vatrozida u server sobe, slijedi konfiguracija istog.

5. Koraci implementacije nultog povjerenja

Koraci provedeni, a u idućim poglavljima objašnjeni, kako bi migracija bila uspješna:

- Prijenos prometa s jezgrenog preklopnika na novi interni segmentacijski vatrozid
- Konfiguracija fizičkih i virtualnih sučelja na vatrozidu i provjera prvog koraka tj dolazi li sav potreban promet na vatrozid
- Konfiguracija pravila i servisa za implementaciju nultog povjerenja
- Praćenje stanja nakon migracije

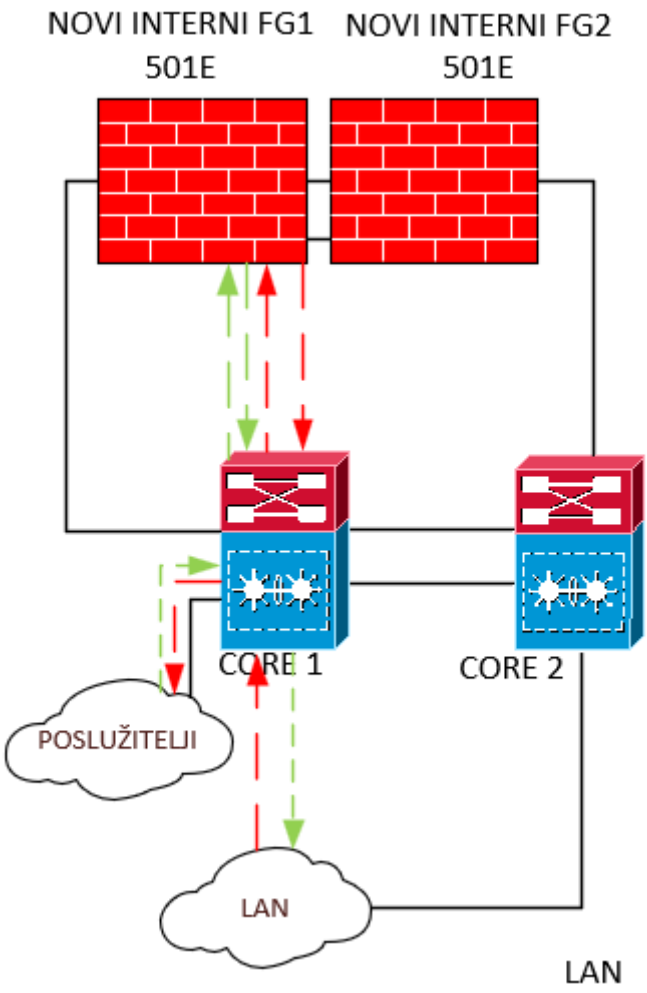
Prije same migracije potrebno je podesiti konfiguraciju vatrozida kako bi migracija mrežnog prometa s jezgrenih preklopnika (engl *core*) na interni segmentacijski vatrozid prošla bez prekida istog. Stanje prije migracije je takvo da sav promet ide preko sučelja trećeg sloja na jezgrenom preklopniku (na slici crveni promet je prema poslužitelju, a zeleni označava povratni promet s poslužitelja prema klijentu).



Slika 5.1 Tok internog prometa prije migracije – vlastiti rad autora

Migracija sučelja trećeg sloja (engl *Switch Virtual Interface*, kasnije u tekstu SVI) s jezgrenog preklopnika na vatrozid provjereno je da je na vatrozidu sve podešeno za prihvaćanje prometa. Migracija je odrađena tako da je administrativno ugašeno SVI sučelje i podešeno usmjeravanje kako bi se i dalje propuštao promet koji dolazi iz mreža koje još nisu migrirane. Nakon što se zabilježilo da nema komunikacijskih poteškoća, SVI sučelje je trajno obrisano.

Novi tok prometa prikazan na slici jest Klijent -> Jezgreni usmjernik-> FortiGate-> Jezgreni usmjernik -> Poslužitelj (crvena linija na slici), a također i promet s poslužitelja prema klijentu prolazi filtriranje na vatrozidu.



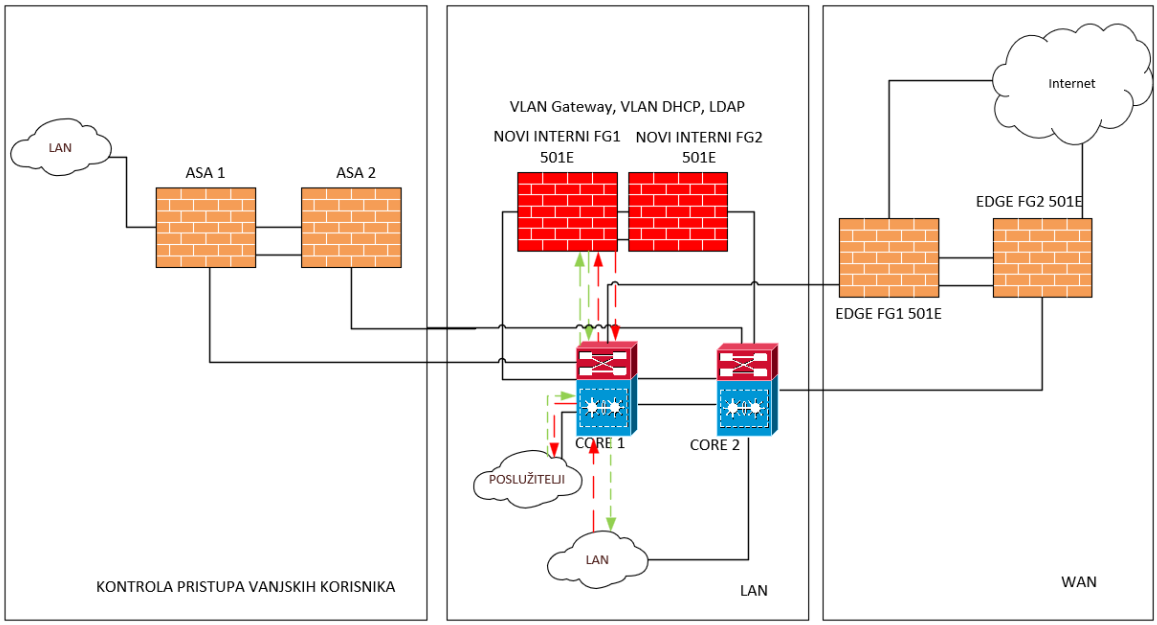
Slika 5.2 Tok internog prometa nakon implementacije internog vatrozida – vlastiti rad autora

Niti jedan dinamički usmjernički protokol nije odabran nego se svo usmjeravanje prometa radi statički. Idućim koracima vatrozid je inicijalno podešen kako bi se moglo nastaviti s implementacijom nultog povjerenja:

- Konfiguracija trunk sučelja prema jezgrenom preklopniku
- Konfiguracija menadžment sučelja
- Podešavanje menadžment pristupa
- Konfiguracija korisničke autentifikacije pomoću ACS servera i RADIUS protokola
- Podešavanje NTP servera i sinkronizacije s istim
- Konfiguracija FSSO (Fortinet Single Sign On) i podešavanje agenata
- Konfiguracija usmjeravanja
- Nadogradnja softvera vatrozida

5.1. Odabir VLAN-ova za migraciju na interni vatrozid

Korisnik ima oko trideset korisničkih VLAN-ova te deset serverskih VLAN-ova koji su migrirani na FortiGate 501E. Po dogovoru s korisnikom migrirana je velika većina traženih VLAN-ova, pojedni su ostali terminirani na jezgrenom preklopniku. Migracija je odrađena tako da su ta sučelja prvo administrativno ugašena na prvotnoj lokaciji te potom i trajno obrisana jer je vatrozid preuzeo ulogu gatewaya i DHCP servera za njih.



Slika 5.3 VLAN konfiguracija na internom vatrozidu – vlastiti rad

Svi VLAN-ovi kreirani su pod istim fizičkim sučeljem.

5.2. Kreiranje sigurnosnih pravila i profila na internom vatrozidu

Prvotno su kreirana dva pravila na internom segmentacijskom vatrozidu, jedno koje propušta sav promet prema internetu te drugo koje propušta sav promet i sve servise od privatnih izvorišnih IP adresa prema privatnim odredišnim IP adresama, te je osiguran pristup svima i prema Internetu i prema lokalnoj mreži. Kako bi se pratio mrežni model nulto-povjerenje, jednom tjedno izvezeni su logovi prometa s FortiGate 501E uređaja i temeljitom analizom i u dogovoru s Korisnikom kreirana su nova vatrozid pravila iznad postojećih definirana na određenim korisnicima, grupama, uređajima i aplikacijama. Poprilično zahtjevan posao koji traje mjesecima i zahtjeva izuzetno dobro poznavanje ostale korisničke infrastrukture pa čak

i pozicije zaposlenika. Izazov je bio otkriti promet koji se ne događa često i možda još niti ne postoji u bazi vatrozida no ipak je nužan i bitan korisniku. Takvih je bilo poprilično, jer su zaposlenici određenim aplikacijama morali pristupati jednom mjesečno samo i s nekim gornjim, VLAN definiranim pravilom, im je to bilo onemogućeno. Cilj je bio kreirati specifična pravila tako da se zadnje pravilo više ne koristi u lokalnoj mreži i da je sav promet potpuno kontroliran. Neka pravila su kreirana privremeno kako bi se njihov status preispitao na kraju i definirani su precizniji uvjeti prolaska kroz mrežu. Pravila na vatrozidu definirana su dugotrajnom i opsežnom analizom prometa te vođeni korisnikovim uputama i informacijama o pravima pristupa.

Nakon kreiranja svih željenih pravila za korisničke VLAN-ove, kreirana su nova pravila netom iznad zadnjeg koja brane svakom pojedinačnom VLAN-u pristup privatnim IP adresama. Tada je zabilježen manji broj prijava korisnika kako ne mogu pristupiti nekom od servisa i to je promptno, u suradnji s AD timom i Korisnikom riješeno na način da je određeni korisnik dodan u ispravnu domensku grupu. Nakon potpunog pročišćavanja prometa za korisničke VLAN-ove, isti pristup, samo s mnogo više opreza, rađen je i za serverske VLAN-ove, što je rezultiralo s nula prijava nakon pravila koja zabranjuju svakom pojedinačnom serverskom VLAN-u pristup privatnim mrežama. U konačnici, zadnje pravilo koje je propuštalo sav promet iz privatnih mreža prema privatnim IP adresama je onemogućeno, te nakon nekog vremena i potpuno obrisano s vatrozida. Migracija je uvela red mrežnim pristupom nulto povjerenje.

5.3. Stanje nakon migracije

Pri analizi logova u fazama migracije, zabilježen je mrežni promet za koji nitko s korisničke strane nije znao zašto se generira, počevši od konstantnog pinga između pojedinih mrežnih uređaja, koji su rezultat prethodno pogrešno konfiguriranih uređaja ili nebilježenja evidencije o gašenju pojedinih uređaja. Također je zabilježen korisnički promet koji nije nužan za poslovanje nego je korišten više jer je u danom trenutnu bio dostupan, te su pristup gotovo svim podacima imali svi zaposlenici. Po migraciji definirano je precizno tko i zašto smije pristupati određenim dokumentima. Prije gašenja pravila koje dopušta pristup svima po svim servisima i dalje je bio vidljiv neobjašnjiv promet, no nakon završetka migracije, to je pravilo obrisano i pokazalo se kako taj promet nije niti bio potreban. Korisniku je pročišćen mrežni promet i samim time isti i akceleriran, no najbitnije od svega omogućena

je kompletna kontrola pristupa i korisnicima i uređajima u mreži korištenjem prava danih putem domenskih organizacijskih jedinica. Postignuto je stanje u kojem je korisnik ne samo u mogućnosti potpuno pratiti sav mrežni promet, nego i biti siguran da svaki zaposlenik, uređaj ili aplikacija imaju minimalan potreban pristup svim podacima kompanije.

6. Izazovi implementacije mrežnog modela nulto povjerenje

Mrežni model nulto povjerenje nije još zaživio svoje pune benefite u većini organizacija, a razlozi vjerojatno leže u idućim izazovima s kojima se suočavaju organizacije:

Kompleksnost implementacije – većina organizacija danas nije u stanju sažeti pristup svih svojih zaposlenika prema svim svojim osjetljivim podacima, pogotovo ako se radi o organizacijama preko 1000 zaposlenih i širokom spektru zanimanja. U tu svrhu je idealno rješenje partnerstvo s nekim od pružatelja nultog povjerenja mrežnog modela. Tu se onda nameće pitanje troška i svijesti vodećih osoba u organizaciji i važnosti informacijske sigurnosti. Rečenica „ Ako sigurnost ne stavljaš na prvo mjesto, stavljaš na zadnje.“ (*„ If you don't put security first, you are putting it last“*) možda još nije dovoljno ozbiljno shvaćena.

Promjena razmišljanja – mrežni model nulto povjerenje uklanja korisnika s vodećeg mjesta u sigurnosti i stavlja podatke kao glavnu metu zaštite, jer su podaci većinom i glavna meta napada. Također, zaštita se seli s perimetra mreže i potrebna je prvo edukacija informacijskog tima kako pristupiti kvalitetnoj nulto povjerenje zaštiti, što opet zahtjeva određene ljudske i novčane resurse.

Usporavanje aplikacija – Obzirom da svaki korisnik, uređaj ili aplikacija mora biti autentificiran i autoriziran kako bi se ostvario pristup podacima ili aplikaciji. Najbolji način prilagodbe na ovaj izazov jest korištenje kontrole adaptivnog pristupa, koji omogućava dinamičko dodjeljivanje pristupa temeljeno na profilu rizika korisnika, uređaja ili aplikacije.

Usporavanje rada organizacije – Krajnji korisnici će poprilično osjetiti implementaciju mrežnog modela nulto povjerenje jer zbog dodatnih faktora autentifikacije možda čak i izgubiti pristup na određene dokumente, čekanje na davanje pristupa istima. Ukoliko se dobro implementira nulto povjerenje, moguće je, korištenjem adaptivnog pristupa, login bez lozinke ili biometrike, ubrzati proces i ostati siguran.

Svi navedeni izazovi nisu nepremostivi i u slučaju težeg sigurnosnog propusta i gubitka podataka niti jedna financijska ušteda na sigurnosti nije vrijedna toga.[8]

Zaključak

Izazovi koje svakodnevno donosi briga o informacijskoj sigurnosti kompanija diljem svijeta glavna je problematika svih zaduženih za zaštitu podataka jer i najmanji propust može imati katastrofalne posljedice za poslovanje. Tradicionalni načini zaštite postali su nedostatni jer su se oslanjali na mogućnost zaokruživanja lokalne mreže kompanije iza rubnih vatrozida i u potpunosti su predefinirano vjerovali korisniku ili uređaju unutar lokalne mreže. Za prijetnje je smatrano da dolaze isključivo izvana. U razdoblju dok je i bilo tako, tradicionalni pristup je služio svrsi. Međutim, po promjeni načina poslovanja, posebice u doba korona virusa, kad su zaposlenici bili primorani raditi od doma, promijenio se pogled na naziv koji stoji iza imena lokalna mreža. Postao je izazov kako svakog korisnika, od ulaska u lokalnu mrežu, držati u šinama tj kako dozvoliti samo kretanje po mreži sa minimalnim pravima po korsiniku, uređaju ili aplikaciji. Posebice ako se radi o poduzeću koje ima hibridni način poslovanja.

Rad prati implementaciju internog segmentacijskog vatrozida u okruženje koje ima fizičku opremu i tek pojedine aplikacije u oblaku. No, zbog poslovanja je bitno da svaki zakupac ima svoj zaseban pristup servisima koji su potrebni za njihovo poslovanje. Cisco ASA vatrozid je zadužen za taj dio komunikacije i propuštanje definiranih korisnika kroz konifguraciju virutalnog usmjeravanja i proslijeđivanja. Za zaštitu mreže izvana korisnik posjeduje rubni FortiGate 501E vatrozid preko kojega je moguć udaljeni pristup u lokalnu mrežu. Korisnik uz razna antivirusna rješenja i konstantan monitoring stanja ima dovoljnu sigurnosnu razinu od eventualnih prijetnji izvana, no jednom kad se pojedinac uspješno autentificira dozovljeno mu je apsolutno lateralno kretanje po mreži bez nadzora. Kako korisnik nije bio svjestan tog stanja u svojoj mreži, zahtjevano je hitno rješavanje navedenog stanja. Ponuđena je implementacija internog segmentacijskog vatrozida koji bi granularnim pravilima i konstantnim provjeravanjem identiteta korisnika i uređaja doveo kompaniju u nulto povjerenje mrežni model.

Prije same implementacije bilo je potrebno odabrati uređaj koji će biti u stanju podržati trenutni, ali i budući korisnički mrežni promet. Ideja o virtualnom uređaju je odbačena zbog veličine kompanije, te su rađene usporedbe između Palo Alto, Fortinet, Cisco i Checkpoint proizvoda. Donesena je odluka o implementaciji FortiGate 501E uređaja u visoko dostupnom načinu rada. Po odrađenoj fizičkoj implementaciji i početnoj konfiguraciji

vatrozida, kreće se sa migracijom prometa sa jezgrenog preklopnika preko novih uređaja. Migracija je omogućila sakupljanje logova o korisničkom prometu. Većina implementacije mrežnog modela nulto povjerenje sastojalo se od postepenog filtriranja prometa i kreiranja pravila po dogovoru sa korisnikom. Za svaki od korisničkih VLAN-ova bilo je potrebno oko tjedan dana kako bi se odredilo koji promet će biti propušten, a koji zabranjen. Izazov je bio i zapaziti da se neki mreženi promet pojavljuje samo jednom u mjesecu ili samo na određene datume, te je bilo potrebno pažljivo filtrirati promet. Višemjesečni rad doveo je potpuno filtriranog prometa po korisniku, uređaju i aplikaciji. Korisnik je mogao u svakom trenutku provjeriti promet, znati da nema nepotrebnog prometa u mreži i biti siguran da napadač samim ulaskom u lokalnu mrežu nema dozvolu lateralnog kretanja po istom, nego će vrlo vjerojatno biti brzo zaustavljen radi granularne segmentacije mreže i nepovjerenja unutar lokalne mreže.

Popis kratica

CIA	*Confidentiality, Integrity, Availability*	povjerljivost, integritet, dostupnost
URL	*Uniform Resource Locator*	jedinstveno mjesto resursa
TCP	*Transmission Control Protocol*	protokol kontrole transmisije
IP	*Internet Protocol*	internet protokol
OSI	*Open System Interconnection*	interkonekcije otvorenih sustava
ACK	*Acknowledge*	prihvaćanje
OTP	*One Time Password*	jednovremenska lozinka
LDAP	*Lightweight Directory Access Protocol*	pristupni protokol direktoriju
SAML	*Security Assertion Markup Language*	jezik oznake sigurnosnih tvrdnji
IEEE	*Institute of Electrical and Electronics Engineers*	institut inženjera elektrike i elektronike
IEEE802.1X	*Network Access Control*	kontrola pristupa mreži
API	*Application Programming Interface*	sučelje za programiranje aplikacija
VPN	*Virtual Private Network*	virtulna privatna mreža
CLI	*Command Line Interface*	sučelje komandne linije
LAN	*Local Area Network*	lokalna mreža
VRF	*Virtual Routing and Forwarding*	virtualno usmjeravanje i prosljeđivanje
ASA	*Adaptive Security Appliance*	prilagodljivi sigurnosni uređaj
NAT	*Network Address Translation*	prevoditelj mrežnih adresa
CPE	*Customer-premises Equipement*	korisnička oprema
VLAN	*Vitrual Local Area Network*	virtualna lokalna mreža
MAC	*Media Access Control*	fizička adresa uređaja
FTP	*File Transfer Protocol*	protokol za transfer podataka
ACS	*Access Control Server*	server za kontrolu pristupa
DNS	*Domain Name System*	sustav za pretvaranje IP adresa u tekst
IPS	*Intrusion Prevention System*	sustav za sprječavanje ugroze
GE	*Gigabit Ethernet*	gigabitno sučelje
SFP	*Small Form-factor Pluggable*	optički adapter
NTP	*Network Time Protocol*	mrežni protocol za vrijeme
HA	*High Availability*	visoka dostupnost

Popis slika

Popis tablica

Literatura

[1] http://ibm.biz/threat-intel-report, veljača 2023.

[2] http://ibm.biz/zero-trust-solutions, veljača 2023.

[3] http://ibm.biz/zero-trust-assessment, veljača 2023.

[4] Scott W. Rose, Oliver Borchert, Stuart Mitchell, Sean Connelly – Zero Trust Architecture (Research Gate)

[5] Evan Gilman, Doug Barth – Zero Trust Networks (Research Gate)

[6] Ramesh Sivaraman – Zero Trust Model (Research Gate)

[7] A. Shaji George - A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall

[8] Definitive Guide to Zero Trust Data Security – Global IT Research, prosinac 2022.

[9] What Is the Zero Trust Security Model? | Fortinet, lipanj 2022.

[10] Next Generation Firewall (NGFW) - See Top Products (fortinet.com), prosinac 2021.

[11] EMS Administration Guide | FortiClient 7.0.7 | Fortinet Documentation Library, prosinac 2022

[12] What is Network Segmentation? | Fortinet, prosinac 2022.

[13] Best Practices | FortiGate / FortiOS 7.2.0 | Fortinet Documentation Library, prosinac 2022.

[14] Zero Trust Access For Dummies (fortinet.com), veljača 2023

[15] Compare Next-Generation Firewalls - Palo Alto Networks, prosinac 2022

[16] Zero Trust Network Access (ZTNA): A Complete Guide (privacyaffairs.com), veljača 2023