Vatrozid: Zaštita informacijskog sustava

Levak, Dino

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

Dino Levak

Vatrozid: Zaštita informacijskog sustava
Firewall: Protection of information systems

Završni rad

Pula, 12.09.2024. godine

Sveučilište Jurja Dobrile u Puli
Fakultet informatike

Dino Levak

Vatrozid: Zaštita informacijskog sustava
Firewall: Protection of information systems

Završni rad

JMBAG: 0303082264, izvanredni student

Studijski smjer: Prijediplomski sveučilišni studij informatike

Kolegij: Operacijski sustavi

Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Mentor: doc. dr. sc. Ivan Lorencin

Pula, 12.09.2024. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Dino Levak, kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student
Dino Levak

U Puli, 12.09.2024. godine

IZJAVA
o korištenju autorskog djela

Ja, Dino Levak dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „VATROZID: ZAŠTITA INFORMACIJSKIH SUSTAVA“: koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.
Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 12.09.2024.

Potpis
Dino Levak

Sažetak

Cilj ovog završnog rada je opisati tehnologije i koncepte vatrozida koji se koriste za zaštitu informacijskih sustava. Detaljno su objašnjeni tradicionalni vatrozidi i vatrozidi nove generacije, njihove razlike, usporedbe u načinu rada te kako svaki tip vatrozida štiti informacijske sustave i prilagođava se suvremenim sigurnosnim prijetnjama.

Tradicionalni vatrozidi fokusiraju se na osnovno filtriranje mrežnog prometa koristeći sigurnosna pravila koja provjeravaju IP adrese, protokole i vrata (eng. port). S druge strane, vatrozidi nove generacije pružaju napredne značajke poput dubinske inspekcije paketa, kontrole aplikacija, inspekcije šifriranog prometa i prevencije upada.

U radu su detaljno prikazani načini obrane informacijskih sustava korištenjem obje vrste vatrozida te je objašnjeno kako pravilno posložiti sigurnosna pravila da bi se zaštitila mreža. Na kraju rada opisani su neki od najčešćih hakerskih napada.

Abstract

The goal of this bachelor's thesis is to describes the technologies and concepts of firewalls used to protect information systems. It provides a detailed explanation of traditional firewalls and next-generation firewalls, their differences, comparisons in operation and how each type of firewall protects information systems and adapts to modern security threats.

Traditional firewalls focus on basic network traffic filtering using security rules that check IP addresses, protocols and ports. On the other hand next-generation firewalls offer advanced features such as deep packet inspection, application control, encrypted traffic inspection and intrusion prevention.

This paper presents detailed methods of defending information systems using both types of firewalls and explains how to properly configure security rules to protect the network. At the end it describes some of the most common hacker attacks.

Sadržaj

1.Uvod

U ovom završnom radu detaljno je opisan i objašnjen pojam vatrozid, te vrste i načela rada vatrozida. Također opisan je doprinos sigurnosti informacijskih sustava s pomoću vatrozida. Opisana je povijest razvoja vatrozida i objašnjeni su njihovi načini primjene u zaštiti informacijskih sustava.

Prvi vatrozidi su razvijeni 1980-ih godina od strana američkih tehnoloških kompanija „Cisco Systems“ i „Digital Equipment Corporation“, to je bilo vrijeme kada je Internet još uvijek bio prilično nova tehnologija u smislu globalnog korištenja.[1]

S obzirom na to da se svaki dan događa veliki broj računalnih napada na određene poslužitelje, računala ili neki određeni uređaj postavlja se pitanje kako te site uređaje tj. Informacijske sustave zaštiti od napada. Vatrozid je tehnologija koja pomaže u zaštiti informacijskih sustava, stoga ga je potrebno implementirati u mrežnu infrastrukturu. U drugom poglavlju detaljno su objašnjene vrste vatrozida kroz povijest njihovog razvijanja i napredovanja mogućnost obrane s istima. Treće poglavlje uspoređuje tradicionalne vatrozide i vatrozide nove generacije uspoređujući njihov način rada te opcije i mogućnosti obrane koju nude. U četvrtom poglavlju opisuje se kako tradicionalni vatrozidi štite informacijske sustave filtriranjem mrežnog prometa temeljenog na sigurnosnim pravilima, uključujući IP adrese, protokole i vrata, te razmatra njihove funkcionalnosti i ograničenja. Peto poglavlje opisuje značajke vatrozida nove generacije kao što su dubinska inspekcije paketa, kontrola aplikacija i prevencije upada. Objašnjeno je kako vatrozidi poboljšavaju sigurnost pružajući sveobuhvatniju zaštitu od suvremenih prijetnji. Šesto poglavlje opsuje neke od najčešćih vrsta i tipova kibernetičkih napada.

[1] K.Ingham, S. Forrest - A History and Survey of Network Firewalls

2.Povijest Vatrozida

Ideja o zidu za zaštitu od uljeza postoji tisućama godina, na primjer prije više od dvije tisuće godina Kinezi su izgradili Kineski zid kao zaštitu od susjednih plemena. Primjerice drugi primjer je taj da su europski kraljevi koji su gradili dvorce s visokim zidinama i kanalima okolo dvorca kako bi zaštitili sebe i svoje podanike od napadačkih vojski i pljačkaških napadaća.

Izraz "vatrozid" prvi je koristio je Timothy Lightoler 1764. godine kako bi opisao zidove koji su odvajali dijelove zgrade koji su najvjerojatnije mogli zahvatiti požar (npr. kuhinju) od ostatka strukture. Ove fizičke barijere sprječavale su ili usporavale širenje požara kroz zgradu, spašavajući tako živote i imovinu.[2]

Iz ovih povijesnih primjera možemo vidjeti kako je izraz "vatrozid" počeo opisivati uređaj ili skup uređaja koji odvaja korisnike od potencijalno opasnih vanjskih okruženja, i napadača.

U ovom završnom radu ćemo se baviti vatrozidima u okruženju računalnih mreža. Prethodnici vatrozida za mrežnu sigurnost bili su usmjerivači (eng. router) korišteni krajem 1980-ih za odvajanje jedne od drugih mreža. Usmjerivači su omogućavali osnovnu kontrolu pristupa između različitih mrežnih segmenata, pružajući tako osnovnu razinu sigurnosti. Razvijanjem sofisticiranijih metoda za zaštitu mrežnog prometa, ovi su uređaji evoluirali u specijalizirane sustave poznate kao vatrozidi, koji su namijenjeni za precizniju kontrolu i zaštitu mrežnog prometa.

Vatrozidovi su sigurnosna mjera koju organizacije koriste kako bi zaštitile svoju mrežu ili više mreža od neovlaštenog pristupa. Vatrozid je sigurnosni sustavi temeljeni na hardveru ili softveru koji se nalazi između interne mreže organizacije i javnog interneta. Oni nadziru promet mreže kako bi osigurali da samo ovlašteni promet bude dopušten. Jedna od ključnih značajki vatrozida je uporaba sigurnosnih pravila kako bi se odredilo koji promet je dopušten u mreži organizacije, a koji je blokiran.

[2] Timothy Lightoler – The Gentlemand and Farmer's Arhitect (1757-1762)

2.1. Tradicionalni Vatrozid (“Stateless“)

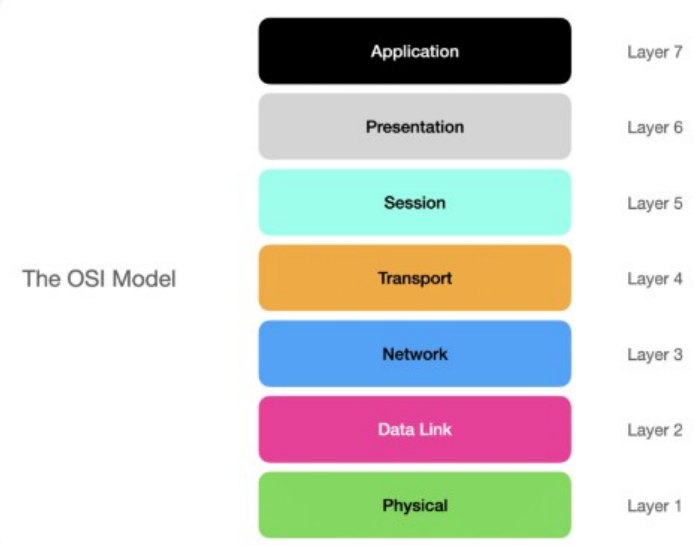
Tvrtka Digital Equipment Corporation razvila je prvi vatrozid 1988. godine [3]. To je bio jednostavan vatrozid za filtriranje paketa (eng. Packet filter). Vatrozidi za filtriranje paketa pregledavaju pakete dok prolaze između izvorišta (eng. Source) i odredišta (eng. Destination). Za pregled paketa se koriste sigurnosna pravila (eng. Security rule , Access control list). Ta sigurnosna pravila upravljaju protokom paketa provjeravajući izvorne i/ili odredišne IP adrese, protokole i vrata (eng. Port).

Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port
accept	forward	192.168.250.18	10.119.30.68	6 (tcp)		3389

Slika 1 - Primjer sigurnosnog pravila

Primjer sigurnosnog pravila (Slika 1) filtrira se promet s ishodišne IP adrese 192.168.250.18 te se dopušta samo promet po TCP protokolu i odredišnim vratima 3389 (Remote Desktop) prema odredišnoj IP adresi 10.119.30.68. Sigurnosno pravilo može se sastojati od samo jedne ishodišne ili odredišne adrese, ali može obuhvaćati i cijelu mrežu (eng. Subnet) koja uključuje više klijenata unutar te mreže.

Prvi tradicionalni vatrozidi, odnosno paketni filteri bili su bez stanja, što znači da nisu koristili nikakvu povijest prometa paketa ili kontekst za određivanje je li paket mogao biti zlonamjeran, dok filteri svjesni stanja to čine. Tradicionalni mrežni vatrozidi primarno rade na 3. i 4. sloju OSI modela fokusirajući se na filtriranje prometa s pomoću ranije navedenih sigurnosnih pravila.



Slika 2 - OSI Model Izvor: https://netbeez.net/wp-content/uploads/2021/05/osi-model-1024x802.png

[3] K.Ingham, S. Forrest - A History and Survey of Network Firewalls

OSI Model

3. Sloj – Mrežni sloj

- Upravlja usmjeravanjem (eng. Routing) i prijenosom podataka između različitih mreža.
- Paketni filteri na ovom sloju filtriraju promet na temelju IP adresa izvorišta i odredišta te vrste protokola (npr. ICMP, TCP, UDP).
- Filtriranje na ovom sloju omogućuje blokiranje ili dopuštanje prometa između određenih IP adresa ili mreža, što pruža osnovnu razinu kontrole i sigurnosti[4].

4. Sloj – Transportni sloj

- Transportni sloj upravlja prijenosom podataka između aplikacija na različitim uređajima, pružajući pouzdanost i kontrolu nad prijenosom podataka.
- Paketni filteri na ovom sloju filtriraju promet na temelju brojeva vrata izvorišta i odredišta te stanja veze (npr. SYN, ACK).
- Filtriranje na ovom sloju omogućuje precizniju kontrolu prometa, kao što je dopuštanje ili blokiranje specifičnih aplikacijskih protokola (npr. HTTP – vrata 80, FTP vrata 20 i 21), što poboljšava sigurnost mreže[5].

Svi paketni filteri dijele zajednički kriterij – povjerenje se temelji na IP adresama. Iako ovaj tip zaštite nije dovoljan za kompletnu mrežu ali prihvatljiv je na razini pojedine komponente. Većina IP paketnih filtera je bez stanja (eng. stateless), što znači da ne pamte ništa o paketima koji su prethodno prošli kroz njih.

Paketni filteri bez stanja su ranjivi na određene vrste napada koji iskorištavaju nedostatke konteksta ili povijesti u obradi paketa. Primjerice izvorna IP adresa u zaglavlju paketa može biti vrlo lako krivotvorena kako bi se maskirao pravi izvor paketa. Također ACK (acknowledgement) u zaglavlju TCP paketa koji se koristi za potvrdu primanja podataka može biti manipuliran kako bi se izbjegla detekcija tj. da se prevari sigurnosno pravilo paketnog filtera[6].

[4] James F. Kurose, Keith W. Ross - Computer Networking: A Top-Down Approach
[5] James F. Kurose, Keith W. Ross - Computer Networking: A Top-Down Approach
[6] William Stalings – Network Security Essentials:Applications and Standards

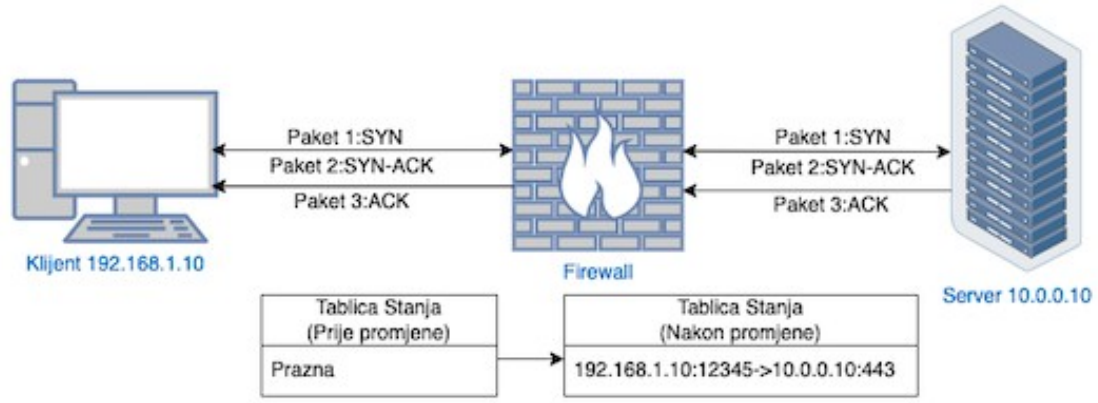
2.2. Tradicionalni Vatrozid (“Stateful“)

Početkom 2000-tih godina pojavili su se vatrozidi svjesni stanja (eng. Stateful), uvodeći drugu generaciju u tehnologiji vatrozida. Ovi sustavi su predstavljali značajnu evoluciju u odnosu na svoje prethodnike, jednostavne paketne filtere. Vatrozidi svjesni stanja (eng. Stateful) donijeli su promjenu paradigme u mrežnoj sigurnosti praćenjem stanja aktivnih veza i određivanjem konteksta mrežnog prometa [7]. Dizajnerski princip iza vatrozida svjesnog stanja bio je zasnovan na konceptu da nisu svi paketi neovisne jedinice tj. mnogi su dio veće komunikacije između mrežnih klijenata i poslužitelja. Održavajući svjesnost o kontekstu, vatrozidi svjesni stanja mogli su donositi informiranije odluke o tome koje pakete treba dopustiti ili odbiti. Procjenjivali su ne samo sam paket, već i njegov odnos prema prethodnim paketima u istoj sesiji. Ovo je bilo slično razumijevanju ne samo rečenica već cijelog razgovora u dijalogu[8].

Poput vatrozida bez stanja, vatrozidi svjesni stanja također rade na 3. i 4. sloju OSI modela. Važna značajka tradicionalnih vatrozida svjesnih stanja je sposobnost analize prometa u stvarnom vremenu i otkrivanje potencijalnih prijetnji. To se radi korištenjem tehnika poput inspekcije paketa, gdje se pojedinačni paketi podataka analiziraju radi sumnjivih aktivnosti. Tradicionalni vatrozidi također mogu biti konfigurirani za bilježenje događaja što se može koristiti u svrhe revizije i rješavanja problema u budućnosti.

Vatrozidi svjesni stanja koriste tablice stanja (eng. State tables) za praćenje svih aktivnih veza koje prolaze kroz vatrozid. Svaki unos u tablici stanja sadrži informacije kao što su IP adrese izvora i odredišta, brojevi portova, i trenutni status veze (npr. SYN, SYN-ACK, ACK). Ove informacije omogućuju vatrozidu da razlikuje legitimne pakete koji su dio postojeće sesije od sumnjivih ili nepoželjnih paketa koji pokušavaju započeti nove sesije bez odgovarajuće autorizacije[9].

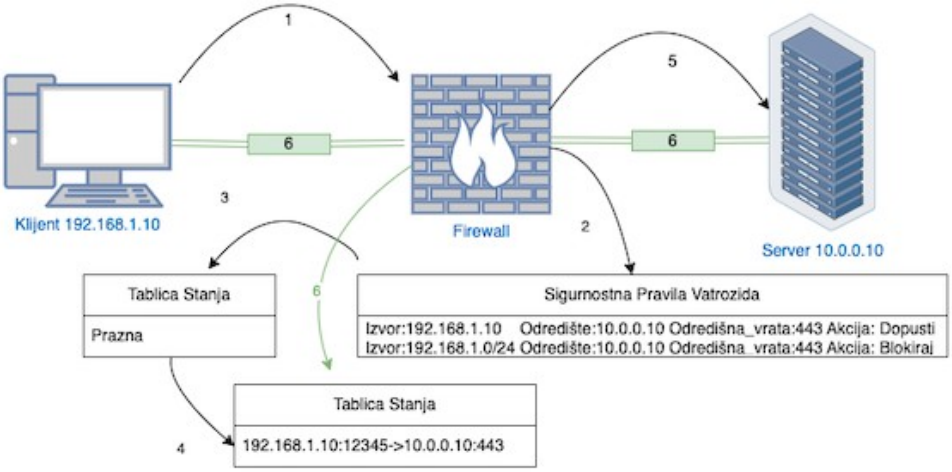
[7] paloaltonetworks.com/cyberpedia/history-of-firewalls
[8] paloaltonetworks.com/cyberpedia/history-of-firewalls
[9] James F. Kurose, Keith W. Ross - Computer Networking: A Top-Down Approach



Slika 3 - Dijagram tablice stanja

Na slici 3 vidimo da klijent s IP adresom 192.168.1.10 inicira TCP komunikaciju s poslužiteljem na IP adresi 10.0.0.10 koristeći vrata 443 slanjem SYN paketa. Vatrozid prima SYN paket i ažurira tablicu stanja te prosljeđuje paket poslužitelju. Poslužitelj odgovara SYN-ACK paketom koji vatrozid prosljeđuje klijentu nakon provjere stanja. Klijent završava rukovanje (eng. Handshake) slanjem ACK paketa koji vatrozid također prosljeđuje poslužitelju. Nakon toga vatrozid prati stanje svih paketa u uspostavljenoj sesiji.

Jedna od ključnih razlika između vatrozida bez stanja i vatrozida svjesnih stanja je da prvi paket koji uspješno odgovara nekom pravilu vatrozida rezultira unosom u tablicu stanja, koja se zatim provjerava za podudaranja prije baze pravila vatrozida. Kada postoji unos u tablici stanja, promet koji odgovara u bilo kojem smjeru više se ne provjerava s pravilima vatrozida. Ukratko nakon što je prvi paket komunikacije dopušten od strane pravila vatrozida, nema daljnje provjere sigurnosnih pravila vatrozida za preostale pakete koji čine tu komunikaciju[10].



Slika 4 - Komunikacija i Tablica Stanja

[10] William Stalings – Network Security Essentials:Applications and Standards

Cisco Adaptive Security Appliance (ASA) uređaji imaju mrežne utičnice koje omogućuju povezivanje uređaja s različitim mrežnim segmentima poput unutarnjih mreža (LAN), vanjskih mreža (WAN) i DMZ zona. Omogućujući kontrolu i filtriranje prometa između tih zona. Upravljačka utičnica (eng. Management interface) služi za administraciju uređaja. Omogućuje mrežnim administratorima pristup konfiguraciji i upravljanju putem sigurnih protokola kao što su SSH, telnet ili web baziranih sučelja poput Cisco ASDM[11].

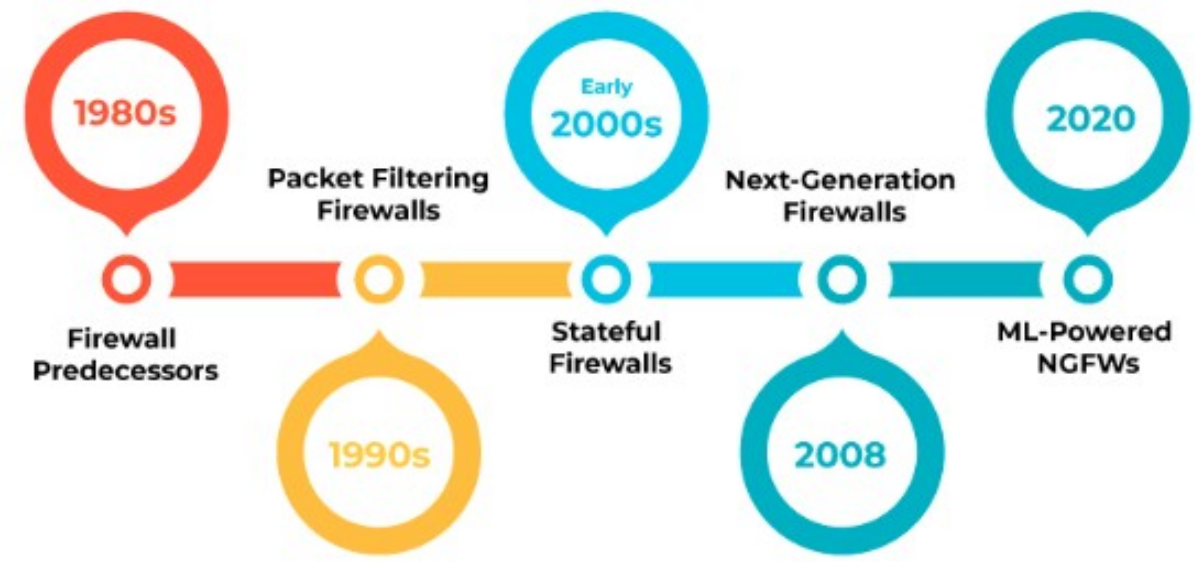
Slika 5 - Cisco ASA (Adaptive Security Appliance) 5510
Izvor: https://www.cisco.com/web/ANZ/cpp/refguide/hview/security/asa.html

Iako su tradicionalni vatrozidi učinkovita sigurnosna mjera, imaju neka ograničenja. Jedno od glavnih ograničenja je da su dizajnirani za zaštitu od poznatih prijetnji te možda nisu učinkoviti protiv novih ili nepoznatih prijetnji. Nadalje, tradicionalni vatrozidi mogu postati usko grlo za promet mreže, usporavajući rad mreže dok se promet preusmjerava kroz vatrozid. Unatoč tim ograničenjima, tradicionalni vatrozidi i dalje ostaju važna sigurnosna mjera za mnoge organizacije. Pružaju osnovnu razinu zaštite od neovlaštenog pristupa i mogu biti djelotvorni u sprječavanju mnogih uobičajenih vrsta napada. Ekonomično rješenje za male i srednje organizacije koje možda nemaju resurse za provedbu naprednijih sigurnosnih mjera. Zaključno tradicionalni vatrozidi su važna komponenta sigurnosti mreže. Iako imaju neka ograničenja i dalje ostaju učinkovita sigurnosna mjera za mnoge organizacije. Pružaju osnovnu zaštitu i analiziraju promet u stvarnom vremenu.

[11] Cisco ASA 5500 Series Configuration Guide

2.3. Vatrozid Nove Generacije

Vatrozidi nove generacije (eng. Next Generation Firewalls - NGFW) pojavili su se 2008. godine kao odgovor na rastuće prijetnje i složenije mrežne okoline. NGFW-ovi predstavljaju značajan napredak u odnosu na tradicionalne vatrozide svjesne stanja jer kombiniraju klasične značajke vatrozida s dodatnim funkcionalnostima, uključujući dubinsku inspekciju paketa (eng. Deep Packet Inspection - DPI), integriranu prevenciju upada (eng. Intrusion Prevention System - IPS) i mogućnosti aplikacijske svijesti[12].



Slika6-Povijest Vatrozida od 1980-ih do 2020.
Izvor:https://www.paloaltonetworks.com/content/dam/pan/en_US/images/cyberpedia/history-of-firewalls/history-of-firewalls.png?imwidth=1920

Vatrozidi novije generacije osim na 3. i 4. sloju OSI modela rade i na 7. sloju tj. aplikativnom sloju.

- 3. i 4. Sloj (Mrežni i Transportni slojevi)

  Kao i tradicionalni vatrozidi, vatrozidi nove generacije pregledavaju promet na ovim slojevima, dopuštajući ili blokirajući pakete na temelju IP adresa, vrata i protokola.

- 7. Sloj (Aplikacijski sloj)

  Vatrozidi nove generacije idu korak dalje analizirajući aplikacijski sloj. Ova analiza omogućuje prepoznavanje i kontrolu aplikacija koje prolaze kroz mrežu, bez obzira na korištena vrata ili protokol. To je ključna prednost jer omogućuje

[12] Computer Security Principles and practice – William Stallings

bolju zaštitu od prijetnji koje se skrivaju unutar legitimnog prometa.

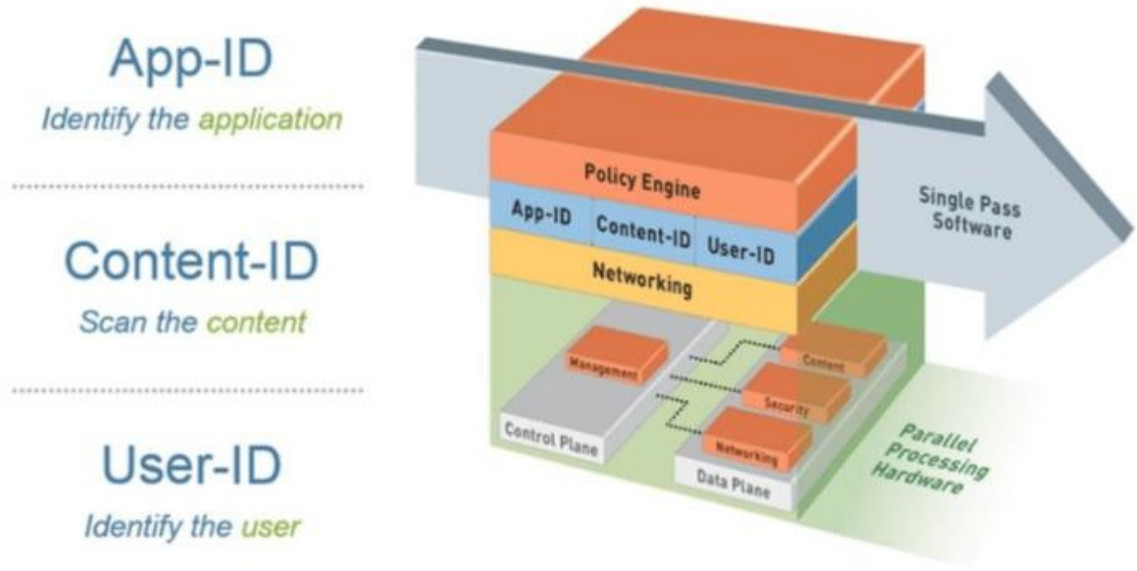
Važne značajke vatrozida nove generacije:

- Dubinska inspekcija paketa (DPI): Vatrozidi provode detaljnu analizu sadržaja paketa kako bi identificirali i blokirali napredne prijetnje kao što su zlonamjerni softver (eng. Malware), iskorištavanje ranjivosti (eng. Exploit) i druge vrste napada. Proučavanjem sadržaja i konteksta svakog paketa, ovi vatrozidi mogu identificirati ne samo poznate prijetnje već i prijetnje koje do sada nisu viđene ili 0-dan (eng. 0-day) napade, pružajući proaktivnu obranu protiv novih kibernetičkih prijetnji[13].
- Integrirana prevencija upada (IPS): Ugrađeni IPS sustavi omogućuju vatrozidu da otkrije i spriječi poznate i nepoznate napade u stvarnom vremenu. Proučavanjem prometa na mreži u stvarnom vremenu i usporedbom s poznatim obrascima napada, ovi sustavi mogu otkriti i blokirati zlonamjerne aktivnosti prije nego što prouzroče štetu[14].
- Aplikacijska svijest: Vatrozidi mogu prepoznati specifične aplikacije koje se koriste unutar mreže, što omogućuje granularnu kontrolu i politiku primjene, poboljšavajući sigurnost i performanse mreže.

Vatrozidi ove generacije de korak dalje u inspekciji prometa, omogućujući dubinsku analizu i klasifikaciju aplikacija (App-ID), sadržaja (Content-ID) i korisnika (User-ID).

Tehnologija za identifikaciju aplikacija (App-ID) im omogućava identifikaciju aplikacija koje se koriste unutar mreže, bez obzira na vrata ili protokole koji su u upotrebi. Ova identifikacija omogućava mrežnim administratorima da precizno kontroliraju promet temeljen na specifičnim aplikacijama, čak i ako se aplikacija pokušava sakriti ili promijeniti vrata kako bi izbjegla detekciju. Aplikacije i funkcije aplikacija identificiraju se putem više tehnika kao što su aplikacijski potpisi (eng. Application signatures), dešifriranje (eng. Decryption), dekodiranje protokola (eng. Protocol decoding) i heuristiku[15].

[13] Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare – Thomas A. Johnson
[14] Cybersecurity Essentials - Charles J. Brooks
[15] Palo Alto Official Documentation



Slika 7 – Palo Alto funkcije vatrozida nove generacije
Izvor: https://www.orangecyberdefense.com/fileadmin/be/Blog/NGFW.png

Tehnologija za identifikaciju sadržaja (Content-ID) omogućuje inspekciju prometa kako bi se otkrio potencijalno opasan sadržaj poput zlonamjernog softvera, virusa ili neželjenih aplikacija. Identifikacija sadržaja također pruža mogućnost filtriranja sadržaja na temelju nekih politika tvrtke blokirajući pristup određenim web stranicama ili tipovima datoteka. Ograničava neovlašteni prijenos datoteka i osjetljivih podataka poput brojeva kreditnih kartica ili matičnih brojeva [16].

Tehnologija za identifikaciju korisnika (User-ID) integrira se s raznim sustavima koji služe kao baza korisnika, poput Microsoft Active Directorya kako bi omogućila praćenje i kontrolu prometa temeljenog na specifičnim korisnicima ili korisničkim grupama, umjesto da se oslanja samo na IP adrese. Pomoću identifikacije korisnika se zna tko koristi aplikacije na mreži ili tko je možda prenio nekakvu prijetnju, ili koje datoteke prenosi koji korisnik. Ova također tehnologija omogućava administratorima da definiraju politike i pravila koje se primjenjuju na određene korisnike bez obzira na to gdje se nalaze u mreži ili koje uređaje koriste [17].

[16] Palo Alto Official Documentation
[17] Palo Alto Official Documentation

3. Usporedba Tradicionalnog Vatrozida i Vatrozida Nove Genracije

Tradicionalni stateful vatrozidi pružaju osnovnu zaštitu mrežnog prometa, i njihova ograničenja u prepoznavanju i zaustavljanju složenih prijetnji čine ih manje efikasnim u suvremenom okruženju. Nasuprot tome vatrozidi nove generacije, zahvaljujući naprednim tehnologijama poput DPI-a i IPS-a, omogućuju detaljniju analizu i zaštitu, čineći ih ključnim mrežnim uređajima u modernim sigurnosnim strategijama za zaštitu informacijskih sustava.

Značajke	Tradicionalni Vatrozid	Vatrozid Nove Generacije
Analiza Prometa	Zaglavlje paketa	Cjeli Paket (zaglavlje i sadržaj)
Praćenje stanja	IP adresa i broj vrata	IP adresa i broj vrata, sadržaj paketa, aplikacija
Dubinska inspekcija paketa	Ne	Da
Prevencija Upada (IPS)	Ne	Da
Aplikacijska svjesnost	Ne	Da
Dodatne Sigurnosne Funkcije	Ograničeno	Antivirus, URL filtriranje, kontrola aplikacija

Tablica 1- Usporedba Vatrozida

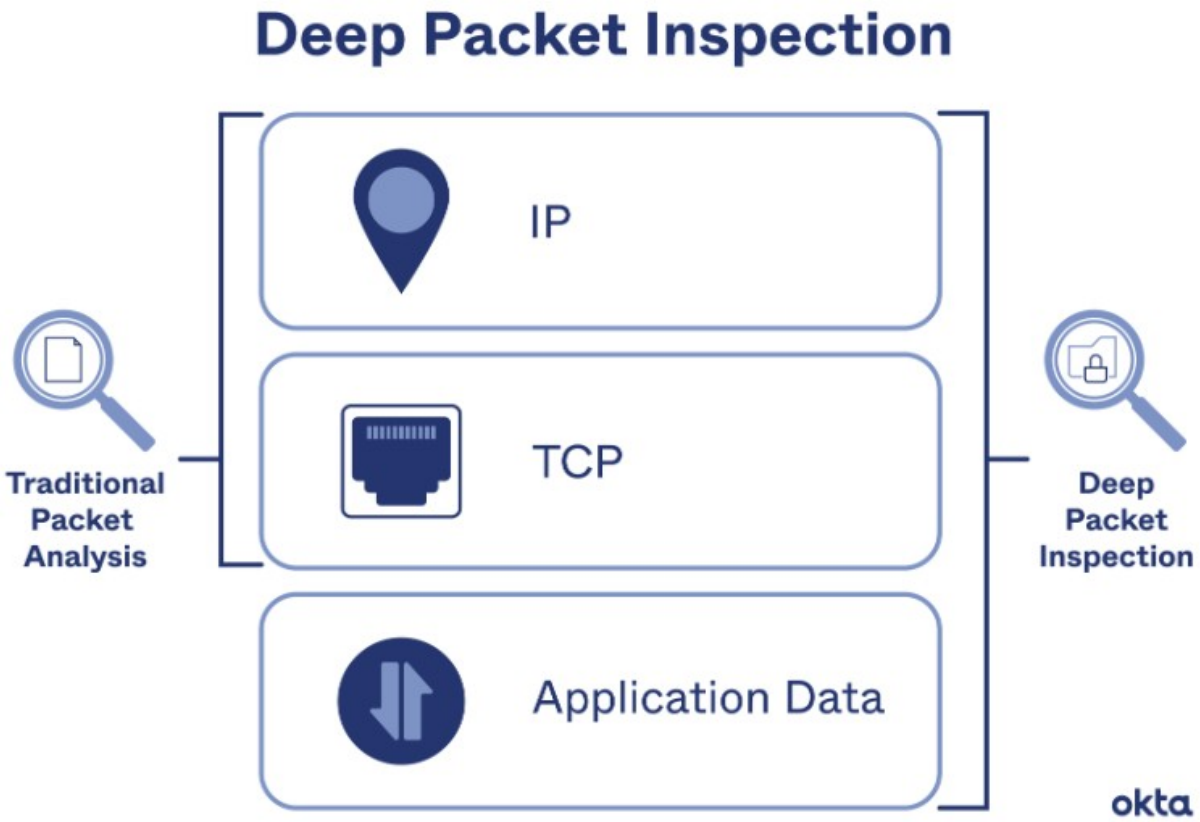
3.1 Usporedba analize prometa i praćenja stanja

Tradicionalni vatrozidi analiziraju samo zaglavlja IP paketa, fokusirajući se na IP adrese, brojeve portova i protokole kako bi donijeli odluke o propuštanju ili blokiranju prometa[18]. Ovaj pristup omogućuje osnovnu kontrolu ali ne otkriva zlonamjerni sadržaj unutar paketa. Vatrozidi novije generacije (NGFW) koriste dubinsku inspekciju paketa (DPI) za analizu cijelog paketa što uključuje zaglavlje i sadržaj paketa. To omogućava prepoznavanje i zaustavljanje složenih prijetnji unutar legitimnog prometa [19]. Ovakva dublja analiza uključuje i aplikacijski sloj, omogućujući precizniju detekciju zlonamjernih aktivnosti na mreži.

[18] William Stalings – Network Security Essentials:Applications and Standards
[19] Eirc Malwald – Network Security: A Beginner's Guide

3.2 Dubinska inspekcija Paketa

Dubinska inspekcija paketa omogućuje pregledavanje sadržaja unutar paketa, analizirajući podatke paketa na svim razinama OSI modela kako bi identificirala potencijalno zlonamjerne aktivnosti. Radi se prepoznavanje obrasca u sadržaju paketa kako bi se otkrili poznati napadi i anomalije koje mogu ukazivati na nove prijetnje čime se omogućuje identifikacija i blokiranje ne samo zlonamjernog softvera već i neželjenih aplikacija te neovlaštenih komunikacija unutar mreže.



Slika 8 - Dubinska Inspekcija Paketa
Izvor: https://www.okta.com/sites/default/files/media/image/2022-08/DEEPPACKETINSPECTION_GRAPHIC_1.png

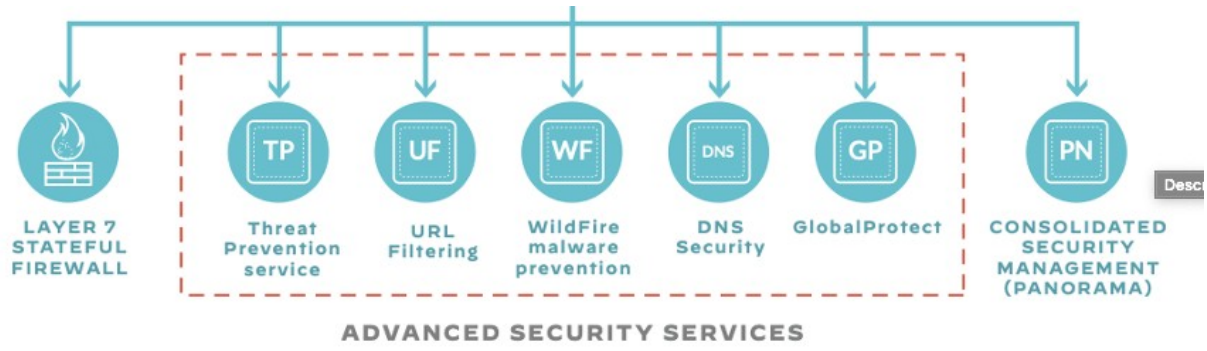
Kao što je vidljivo na slici 8, IP paket se sastoji od zaglavlja i podatkovnog dijela (sadržaja). U zaglavlju paketa se nalaze informacije kao što su izvorna i odredišna IP adresa, broj vrata i protokoli. Tradicionalni vatrozidi provjeravaju samo taj dio paketa. Podatkovni dio sadrži stvarne korisničke podatke koji se prenose putem mreže kao što su informacije o aplikaciji (obrasci), datoteke koje se prenose itd[20].

[20] William Stalings – Network Security Essentials:Applications and Standards

3.3 Dodatne Sigurnosne Funkcije

Za opisivanje dodatnih sigurnosnih funkcija firewalla nove generacije uzet ćemo vatrozid nove generacije proizvođača Palo Alto. Dodatne funkcije koje Palo Alto nudi u svojim vatrozidovima su antivirusna zaštita, URL filtriranje, identifikacija aplikacija, identifikacija prijetnji.

- Antivirusna zaštita provjerava dolazni i odlazni promet kako bi identificirala i blokirala zlonamjerne datoteke i programe prije nego što dospiju na ciljane uređaje.
- URL filtriranje omogućuje kontrolu pristupa web stranicama na temelju URL-a blokirajući pristup nepoželjnim i zlonamjernim stranicama ili web stranicama za koje sami odlučimo da ćemo blokirati pristup
- Identifikacija aplikacija omogućuje vatrozidu prepoznavanje i upravljanje specifičnim aplikacijama koje generiraju promet na mreži.
- Dentifikacija prijetnji omogućuje vatrozidu prepoznavanje poznatih i nepoznatih prijetnji kao i 0-day napada, te aktivno sprječavanje tih prijetnji prije nego što prouzroče štetu.[21]



Slika 9 - Portfolio Palo Alto Naprednih Sigurnosnih Funkcija
Izvor: https://docs.oracle.com/en/solutions/secure-app-palo-alto-firewall/img/pan-advanced-security.png

[21] Official Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide

4.Zaštita informacijskih sustava tradicionalnim vatrozidom

Primjer korporativne mreže neke kompanije s javnim servisima. Kompanija ima vezu prema internetu s fiksnim javnim IP adresama. Jednu javnu adresu ima vatrozid, a ostali servisi su javno dostupni, tj. servisu su dostupni s interneta. Na jednoj strani vatrozida se nalazi korporativna mreža podijeljena na zone. Zone su kreirane tako da podijele unutarnju privatnu IP mrežu na VPN zonu (eng. Virtual Private Network), unutarnju zonu (eng. Inside zone), vanjsku zonu (eng. Outside/Internet zone) i DMZ (eng. Demilitarized zone) zonu. DMZ zona ili Demilitarizirana zona je zona u kojoj se nalaze javno dostupni servisi na korporativnim poslužiteljima (eng. Server). Između tih zona nalaze se usmjernici (eng. switch) na kojima je mreža dodatno segmentirana u VLAN-ove.

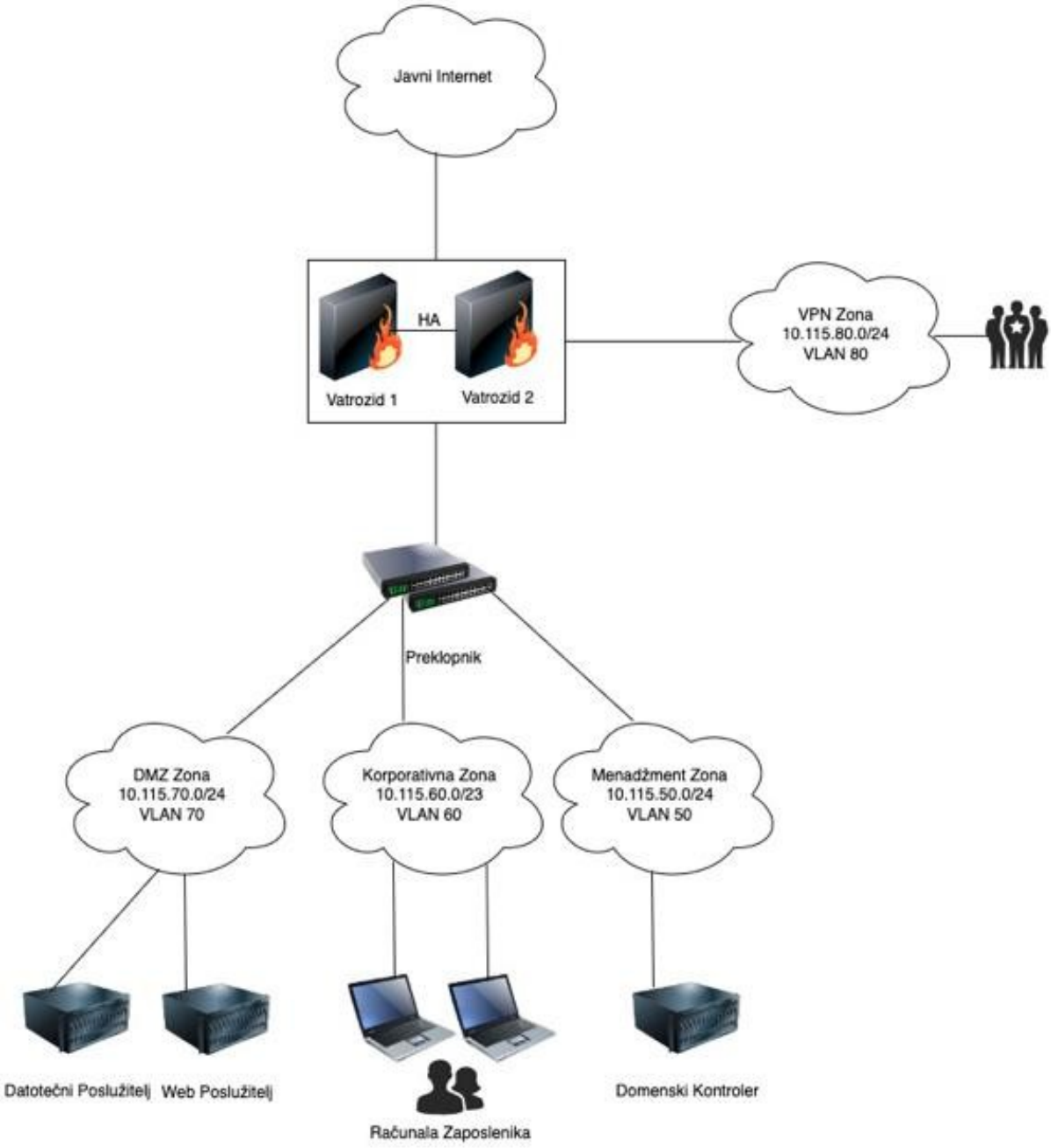
Primjeri vanjskih poslužitelja (eng. servera):

- Poslužitelj s web sadržajem (eng. Web server)
- Datotečni poslužitelj (eng. File server)
- Poslužitelj elektroničke pošte (eng. Mail server)

Svaka od zona, pa tako i DMZ zona, nalazi se u vlastitom subnetu i VLAN-u. Kako su sve zone u zasebnim podmrežama (eng. subnet) i VLAN-ovima, komunikacija između njih može se filtrirati i/ili blokirati prema potrebi na vatrozidu. Također, na vatrozidu se vrši filtriranje prometa iz unutarnje mreže prema vanjskoj, tj. prema internetu, i u suprotnom smjeru.

Primjer jedne korporativne mreže koja ima zakupljen javni adresni prostor IP adresa, jedan vatrozid ili dva ako je potrebna visoka dostupnost (eng. High availability), te nekoliko mrežnih preklopnika (eng. Switch). Privatna mreža tj. privatni adresni prostor, podijeljen je u više manjih podmreža (eng. Subnet), te svaka podmreža pripada jednom VLAN-u. Iste te podmreže su dio određenih zona, tako da primjerice web poslužitelj koji se nalazi u DMZ zoni ima privatnu adresu iz podmreže 10.115.70.0/24, dok klijentsko računalo iz unutarnje zone (eng. Inside zona) ima adresu iz 10.115.60.0/23. U menadžment zoni nalaze se privatne adrese mrežnih uređaja, internih poslužitelja koji nisu u DMZ zoni (npr. Domain Controller - DC) i služe samo za unutarnje potrebe, tj. nije potrebno da su javno dostupni s interneta. Imamo

još VPN (eng. Virtual Private Network) zonu u kojoj se nalaze klijenti koji su spojeni na VPN. Sve što dolazi s interneta je vanjska zona (eng. Outside).

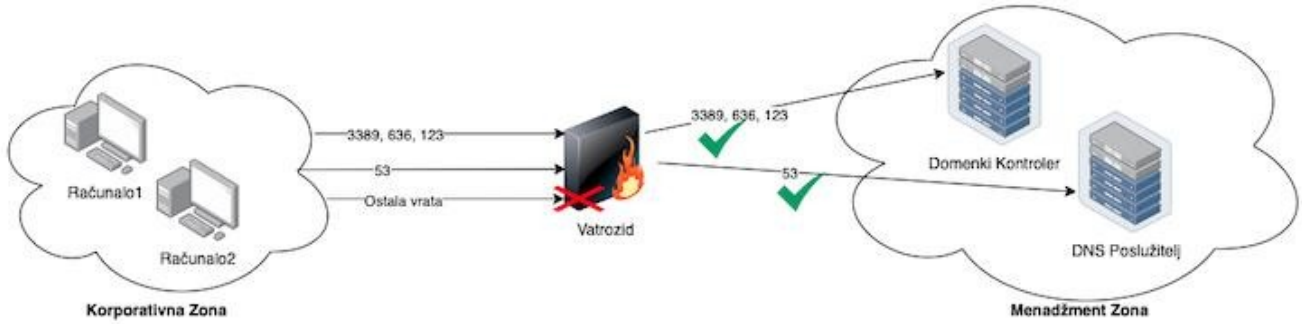


Slika 10 - Korporativna Mreža – Tradicionalni Vatrozid

4.1 Sigurnosna Pravila Vatrozida Za Zaštitu Informacijskih Sustava

Pristup iz korporativne zone prema menadžment zoni

Dopušten je pristup računalima koja se nalaze u korporativnoj zoni prema određenim IP adresama u menadžment zoni isključivo kroz dopuštena vrata. Računala zaposlenika mogu komunicirati s domenskim kontrolerom putem vrata 389 (LDAP - The Lightweight Directory Access Protocol), 636 (LDAPS - The Lightweight Directory Access Protocol Secure), 123 (NTP) i s DNS poslužiteljem putem vrata 53 (DNS). LDAP i LDAPS koriste se za autentifikaciju i pristup informacijama o korisnicima u Active Directoryju, NTP se koristi za sinkronizaciju vremena odnosno postavki sata, a DNS za prevođenje domena u IP adrese. Sva ostala komunikacija je strogo zabranjene, čime se osigurava sigurnost mreže i sprječava neovlašteni pristup.

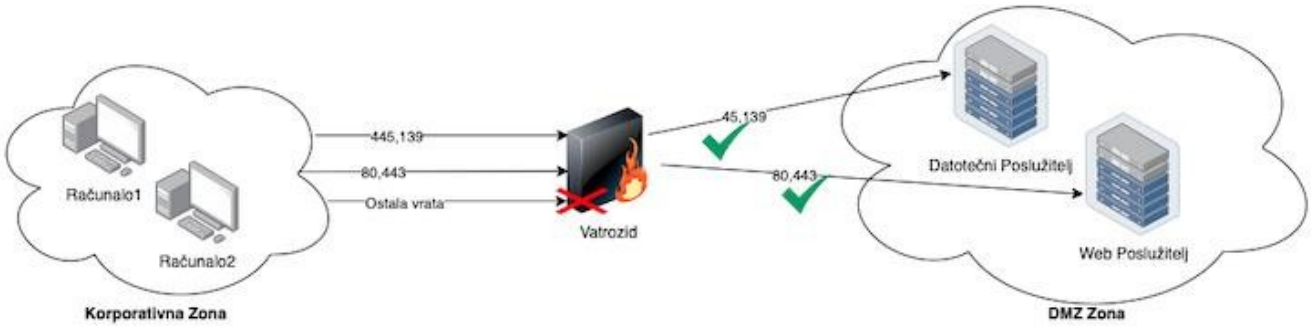


Slika 11 - Grafički prikaz pristupa iz korporativne zone prema menadžment zoni

Pristup iz korporativne zone prema DMZ zoni

Pristup iz korporativne zone prema DMZ zoni strogo je kontroliran i dopušten je samo prema određenim IP adresama unutar DMZ-a, i to kroz specifična mrežna vrata. Konkretno dopušten je promet putem vrata 445 i 139 na kojem radi SMB (eng. Server Message Block) protokol. SMB protokol omogućuje razmjenu datoteka i resursa unutar mreže. Dopušten je pristup web poslužiteljima u DMZ zoni kroz vrata 80 koja služe za nešifriranu HTTP (eng. Hypertext Transfer Protocol) komunikaciju, te vrata 443 koja

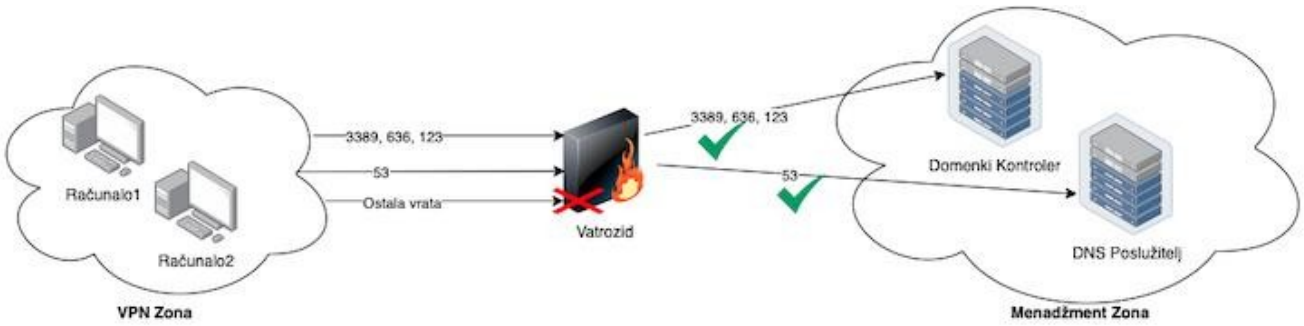
omogućuju sigurnu HTTPS (eng. Hypertext Transfer Protocol Secure) komunikaciju, osiguravajući enkripciju podataka tijekom prijenosa.



Slika 12 - Grafički prikaz pristupa iz korporativne zone prema DMZ zoni

Pristup iz VPN zone prema menadžment zoni

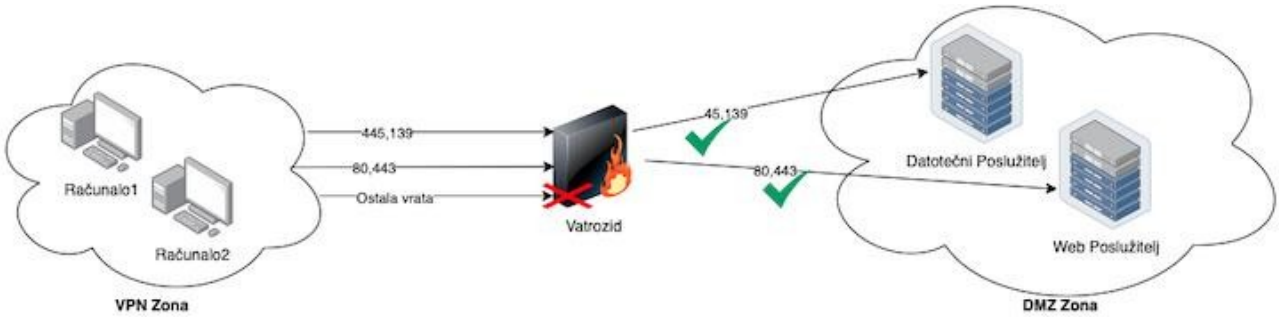
Pristup iz VPN zone prema menadžment zoni strogo je ograničen i dopušten samo za određene IP adrese i specifična vrata, kako bi se osigurala sigurnost mreže. Korisnici koji su spojeni putem VPN-a mogu komunicirati s domenskim kontrolerom kroz vrata 389 i 636, kao i putem vrata 123 te putem vrata 53 za pristup DNS poslužitelju. Sva ostala vrsta pristupa koja nije izričito dopuštena ovim pravilima strogo je zabranjena. Ovakav način postavljanja pravila vatrozida za pristup s VPN-a prema internim servisima pomaže u preciznom kontroliranju koji korisnici i uređaji mogu pristupiti kritičnim resursima, smanjujući rizik od neovlaštenih upada. Time se dodatno osigurava sigurnost mreže i zaštita osjetljivih podataka unutar organizacije.



Slika 13 - Grafički prikaz pristupa iz VPN zone prema menadžment zoni

Pristup iz VPN zone prema DMZ zoni

Dopuštanje pristupa računalima spojenim putem VPN-a prema IP adresama u DMZ zoni na specifičnim vratima predstavlja važan sigurnosni korak u zaštiti mreže. Omogućena je komunikacija isključivo kroz vrata 445 i 139 za SMB protokol, te kroz vrata 80 i 443 za komunikaciju s web poslužiteljima. Na ovaj način se može precizno kontrolirati koji se podaci i usluge mogu koristiti iz VPN mreže prema DMZ-u. Ovako posložena sigurnosna pravila vatrozida sprječavaju neovlašteni pristup drugim uslugama ili resursima unutar DMZ zone, smanjujući rizik od napada koji bi mogli kompromitirati sigurnost mreže. Također, postavljanjem ovih specifičnih pravila, osigurava se da VPN korisnici imaju samo onoliko pristupa koliko im je potrebno za obavljanje zadataka, dok se istovremeno minimizira površina potencijalnog napada i štiti osjetljive informacije.

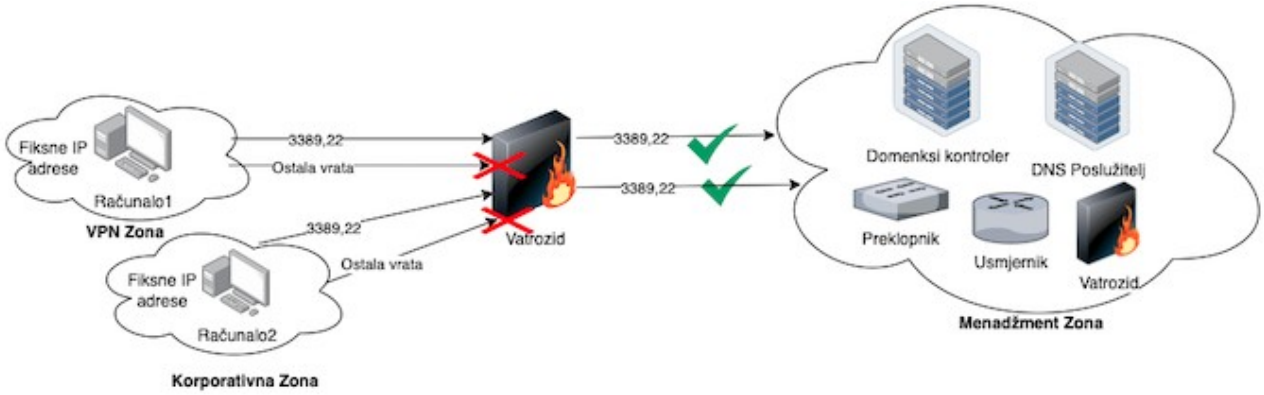


Slika 14 - Grafički prikaz pristupa iz VPN zone prema DMZ zoni

Poseban pristup za Mrežne i Serverske Administratore

Dopušten je pristup mrežnim i serverskim administratorima s fiksnim IP adresama na LAN-u i VPN-u prema svim resursima u menadžment zoni. Ovo predstavlja jednu od ključnih sigurnosnih mjera zato što ova pravila omogućuju kontroliran i ograničen pristup osjetljivim područjima mreže. Dopuštanje pristupa samo s fiksnih IP adresa pomaže u sprječavanju napadača koji koriste dinamičke IP adrese za pristup mreži. Fiksne IP adrese omogućuju lakšu identifikaciju i praćenje aktivnosti administrativnih korisnika, čime se povećava sigurnost i olakšava detekcija neovlaštenih pokušaja pristupa. Osim toga ograničavanje pristupa samo na vrata 3389 (eng. RDP - Remote Desktop Protocol) i 22 (eng. SSH - Secure Shell) dodatno

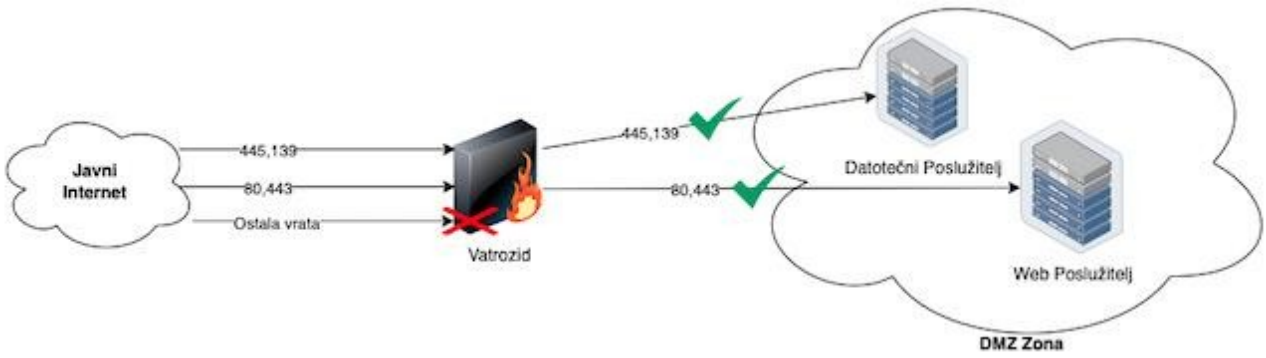
smanjuje površinu napada. RDP omogućuje udaljeni grafički pristup računalima, dok SSH osigurava sigurno povezivanje i upravljanje putem komandne linije. Ova sigurnosna pravila osiguravaju da samo ovlašteni administratori mogu pristupiti ključnim resursima, minimizirajući rizike.



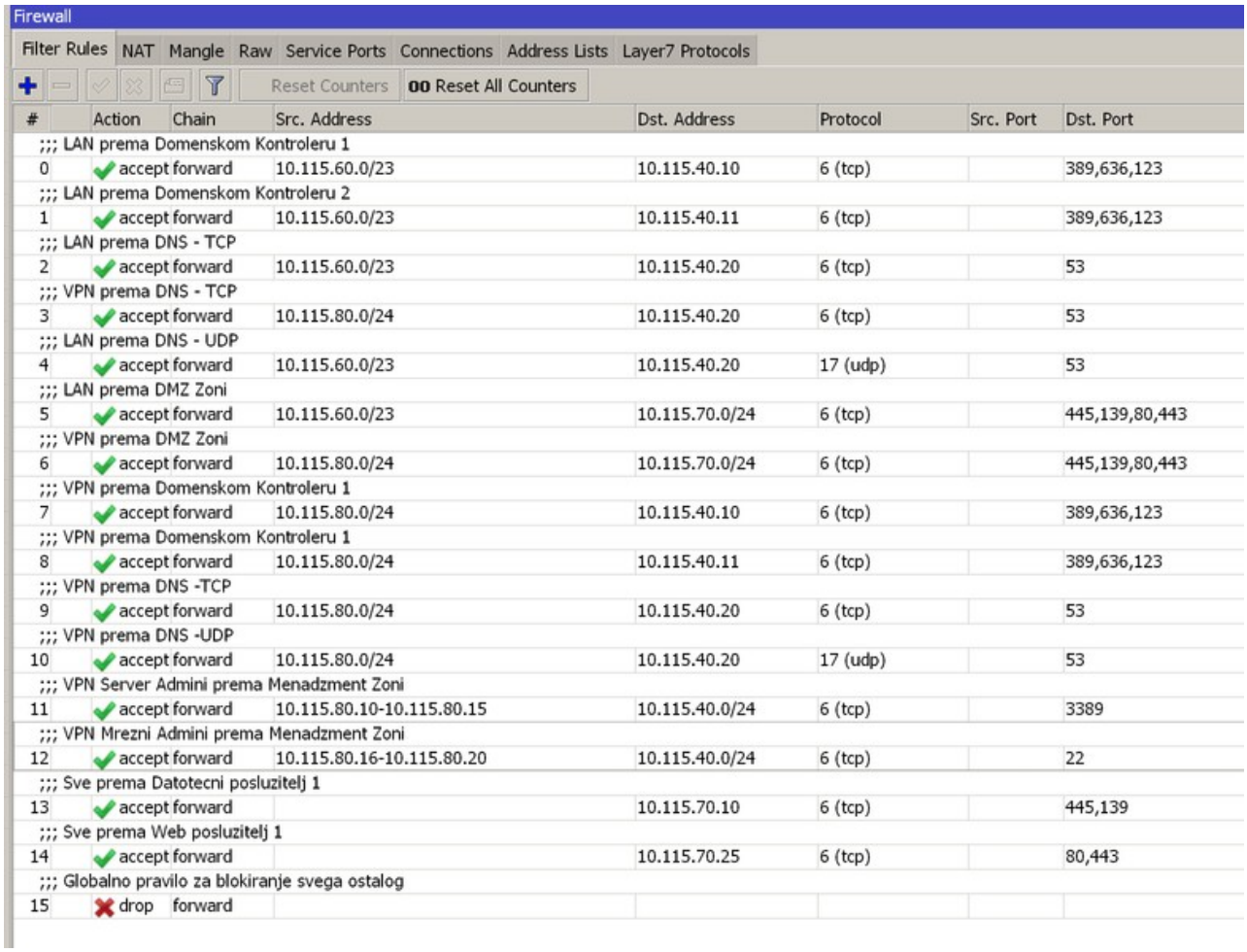
Slika 15 - Grafički prikaz pristupa za Mrežne i Serverske Administratore

Pristup s javnog interneta prema DMZ zoni tj. prema javno dostupnim poslužiteljima

Dopušten je pristup s bilo koje javne IP adrese prema datotečnom poslužitelju u DMZ zoni putem specifičnih vrata. To uključuje vrata 445 i 139 za pristup datotekama te vrata 80 i 443 za pristup web poslužitelju. Ovakve postavke sigurnosnih pravila omogućuju korisnicima izvan mreže da pristupe javno dostupnim resursima i uslugama, kao što su web stranice i javno dostupne datoteke, dok istovremeno održava sigurnost unutarnjih sustava.



Slika 16 - - Grafički prikaz pristupa s javnog interneta prema DMZ Zoni



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port
;;; LAN prema Domenskom Kontroleru 1							
0	accept	forward	10.115.60.0/23	10.115.40.10	6 (tcp)		389,636,123
;;; LAN prema Domenskom Kontroleru 2							
1	accept	forward	10.115.60.0/23	10.115.40.11	6 (tcp)		389,636,123
;;; LAN prema DNS - TCP							
2	accept	forward	10.115.60.0/23	10.115.40.20	6 (tcp)		53
;;; VPN prema DNS - TCP							
3	accept	forward	10.115.80.0/24	10.115.40.20	6 (tcp)		53
;;; LAN prema DNS - UDP							
4	accept	forward	10.115.60.0/23	10.115.40.20	17 (udp)		53
;;; LAN prema DMZ Zoni							
5	accept	forward	10.115.60.0/23	10.115.70.0/24	6 (tcp)		445,139,80,443
;;; VPN prema DMZ Zoni							
6	accept	forward	10.115.80.0/24	10.115.70.0/24	6 (tcp)		445,139,80,443
;;; VPN prema Domenskom Kontroleru 1							
7	accept	forward	10.115.80.0/24	10.115.40.10	6 (tcp)		389,636,123
;;; VPN prema Domenskom Kontroleru 1							
8	accept	forward	10.115.80.0/24	10.115.40.11	6 (tcp)		389,636,123
;;; VPN prema DNS -TCP							
9	accept	forward	10.115.80.0/24	10.115.40.20	6 (tcp)		53
;;; VPN prema DNS -UDP							
10	accept	forward	10.115.80.0/24	10.115.40.20	17 (udp)		53
;;; VPN Server Admini prema Menadzment Zoni							
11	accept	forward	10.115.80.10-10.115.80.15	10.115.40.0/24	6 (tcp)		3389
;;; VPN Mrezni Admini prema Menadzment Zoni							
12	accept	forward	10.115.80.16-10.115.80.20	10.115.40.0/24	6 (tcp)		22
;;; Sve prema Datotecni posluzitelj 1							
13	accept	forward		10.115.70.10	6 (tcp)		445,139
;;; Sve prema Web posluzitelj 1							
14	accept	forward		10.115.70.25	6 (tcp)		80,443
;;; Globalno pravilo za blokiranje svega ostalog							
15	drop	forward					

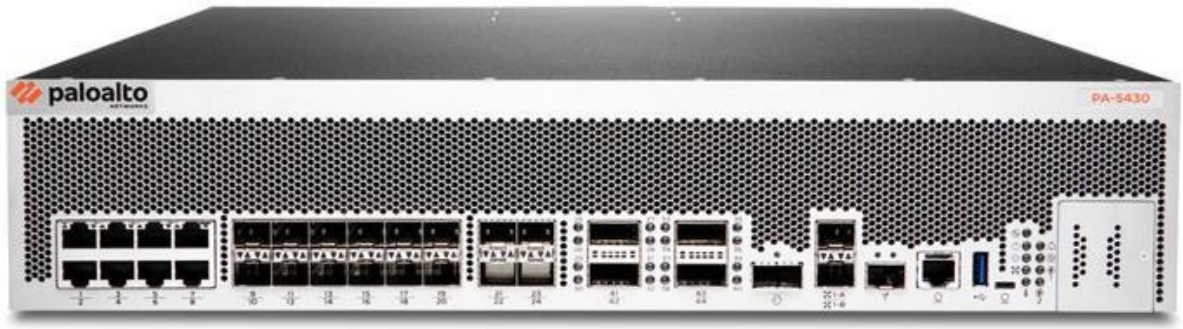
Slika 17 - Lista sigurnosnih pravila (Mikrotik)

Kao što je vidljivo na slici 11, na vrhu su navedena sigurnosna pravila koja dopuštaju specifičnu komunikaciju preko određenih vrata, dok je na dnu globalno pravilo zabrane (eng. Global Deny) koje blokira svu ostalu komunikaciju. Ova struktura osigurava da se samo unaprijed definirani promet može odvijati, dok se svi ostali pokušaji komunikacije automatski blokiraju. Kada vatrozid analizira paket koji je stigao do njega, koristi pravilo provjere od vrha prema dnu što znači da najprije razmatra pravila na vrhu popisa. Ako paket zadovoljava uvjete prvog pravila koje se podudara vatrozid primjenjuje to pravilo i zanemaruje sva daljnja pravila. Čak i ako kasnije postoji pravilo koje bi bolje odgovaralo paketnom prometu, ono se ne uzima u obzir ako je prvi odgovarajući uvjet već zadovoljen. Ovaj pristup omogućuje jasnu i učinkovitu filtraciju prometa osiguravajući da se pravila primjenjuju prema unaprijed definiranim prioritetima.

5.Zaštita Informacijskih Sustava Vatrozidom Nove Generacije

Kako tehnologija napreduje IT timovi moraju voditi brigu o rastućem broju uređaja, aplikacija i podataka, ali i o povećanom broju sigurnosnih napada tj. sigurnosnih izazova. Neovisno radi li se o sigurnosnim rupama u samoj organizaciji, probojima u sustav ili izazovima koje donese udaljeni zaposlenici i razni cloud servisi, sigurnosnim je timovima teško pravovremeno reagirati na napade.
Zaštitu informatičkih sustava vatrozidovima nove generacije se fokusira na zaštitu korisnika na lokaciji (eng. On-site) i korisnika koji rade izvan ureda npr. od kuće (eng. Remote users). Kao i na osiguravanje vidljivosti i kontrole nad svim uređajima spojenima na mrežu.

Jedna od trenutno najpoznatijih i vodećih tvrtki za kibernetičku sigurnost koja je poznata po proizvodnji i prodaji vatrozida nove generacije je Palo Alto Networks. Portofolio proizvoda tvrtke uključuje fizičke vatrozide, virtualne vatrozide, vatrozide u oblaku itd. Njihova rješenja pomažu organizacijama da zaštite svoje mreže od sve sofisticiranijih kibernetičkih prijetnji, pružajući potpunu vidljivost i kontrolu nad mrežnim prometom u stvarnom vremenu[22]. Palo Alto Networks je vodeća tvrtka u području kibernetičke sigurnosti koja je prepoznata kao lider u Gartnerovom magičnom kvadrantu za mrežne firewalle deset godina zaredom uključujući i 2024. godinu.[23]



Slika 18 - Palo Alto 5430 model vatrozida
Izvor https://mma.prnewswire.com/media/1743027/PA5430_FrontWtop.jpg

[22] Meghdeep Mukherjee – The Ohio State university – Palo Alto Networks Analysis

[23] Insider - Palo Alto Networks named a Ten-Time Leader in Gartner Magic Quadrant

5.1 Inspekcija Prometa – Šifriranog i ne šifriranog (eng. SSL decryption)

S obzirom na da je više od 90% poslovnog mrežnog prometa danas šifrirano, vatrozidi nove generacije mogu vidjeti i zaštiti šifrirani (eng. Encrypted) promet, tj. mogu vršiti inspekciju šifriranog prometa tako da ga dešifriraju (eng. Decrypt), provjere i zatim opet šifriraju. Kod Palo Alto vatrozida nove generacije radi analizu cjelokupnog mrežnog prometa (bez obzira na portove, protokole ili enkripciju) s ciljem automatskog prepoznavanja i blokade poznatih prijetnji, malwarea i špijunskih softvera.

Prednosti SSL dekripcije:

- Sprječavanje povrede podataka pronalaženjem skrivenog zlonamjernog softvera i sprječavanje hakera da se provuku kroz obranu nezapaženo.
- Vidljivost onog što zaposlenici šalju izvan organizacije bilo to namjerno ili slučajno (osiguravanje da zaposlenici ne izlažu povjerljive podatke riziku)[24].

5.2 Ulazno SSL dešifriranje (eng. Inbound SSL Decryption)

Kada se certifikat SSL poslužitelja učita na vatrozid i konfigurira se pravilo SSL dešifriranja za ulazni promet, vatrozid dekriptira i čita promet dok se prosljeđuje. Ne mijenjaju se paketni podaci, a sigurni kanal (eng. Secure channel) je od klijentskog sustava do internog poslužitelja. Vatrozid tada može otkriti zlonamjerni sadržaj i kontrolirati aplikacije koje rade preko ovog sigurnog kanala.

5.3 Odlazno SSL dešifriranje (eng. Outbound SSL Decryption)

U ovom slučaju vatrozid proksira izlazne SSL veze presretanjem izlaznih SSL zahtjeva i generiranjem certifikata u hodu za stranicu koju korisnik želi posjetiti. Datum valjanosti na generiranom certifikatu preuzet je iz datuma valjanosti na pravom poslužiteljskom certifikatu. Kod Palo Alto vatrozida druge generacije, tijelo (eng. Certificate Authority - CA) koje izdaje taj certifikat je vatrozid Palo Alto. Ako certifikat

[24] Official Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide

vatrozida nije dio postojeće hijerarhije ili nije dodan u predmemoriju preglednika klijenta, tada klijent prima upozorenje prilikom pregledavanja sigurne web stranice. Ako je certifikat pravog poslužitelja izdalo tijelo kojem vatrozid Palo Alto ne vjeruje, tada certifikat za dešifriranje koristi drugi "nepouzdani" ključ tijela za izdavanje certifikata (eng. Certificate Authority - CA) kako bi se osiguralo da je korisnik upozoren na bilo kakve naknadne napade kao što su središnji napadi.
Upozorenje kakvo vidi korisnik ako ne vjeruje izdavaču certifikata:

5.4 Filtriranje URL-ova (eng. URL Filtering)

URL je akronim za eng. pojam Uniform Resource Locator, u prijevodu - ujednačeni ili usklađeni lokator sadržaja (resursa)**.** Vatrozidovi nove generacije imaju opciju URL filtriranja, a to je tehnologija koja uspoređuje mrežni promet na internetu sa bazom podataka koja se sastoji od URL filtera[25].

Svaki URL koji je definiran u bazi podataka ima dodijeljenu URL kategoriju i/ili grupu koja se može iskoristiti na dva načina:

1. Da blokira ili dozvoli promet na osnovu URL kategorije. Kreira se profil za URL filtriranje koji određuje akciju za svaku URL kategoriju i onda se taj prodil dodaje pravilu na vatrozidu.

2. Da upari promet prema nekoj URL kategoriji kako bi se primijenilo pravilo na vatrozidu. Ako je cilj da se točno određeno pravilo primjeni na točno određene kategorije prometa, onda se treba dodati kategoriju kao kriterij za uparivanje kada se kreira pravilo.

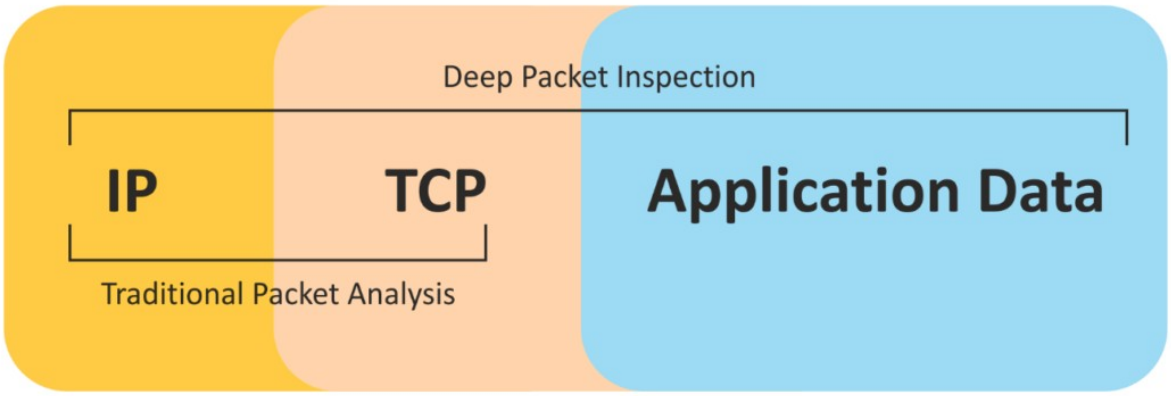
Usluga u cloudu za filtriranja URL-ova Palo Alto vatrozida nove generacije skenira web stranice i analizira njihov sadržaj pomoću strojnog učenja (eng. Machine learning), sa statičkom i dinamičkom analizom, kako bi se točno odredile kategorije i ocjene rizika. URL-ovi se klasificiraju u benigne ili zlonamjerne kategorije, koje se lako mogu ugraditi u sigurnosna pravila vatrozida za potpunu kontrolu web prometa. Novo

[25] Official Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide

kategorizirani zlonamjerni URL-ovi odmah se blokiraju nakon otkrivanja, ne zahtijevajući intervenciju administratora.

5.5 Deep Packet Inspection (DPI)

Palo Alto vatrozid omogućava detaljnu analizu mrežnog prometa na svim razinama OSI modela. DPI tehnologija omogućuje prepoznavanje i inspekciju ne samo zaglavlja paketa, već i njihovog sadržaja čime se otkrivaju prijetnje koje se skrivaju unutar legitimnog prometa. Palo Alto koristi DPI za identifikaciju aplikacija (eng. Application ID) što omogućuje prepoznavanje specifičnih aplikacija bez obzira na vrata ili protokol koji aplikacija koristi. DPI se također koristi za otkrivanje i blokiranje zlonamjernog softvera, virusa te neovlaštenih aktivnosti unutar mreže putem naprednih sigurnosnih funkcija kao što su Antivirus, URL filtriranje i identifikacija prijetnji (eng. Threat ID). Ove napredne funkcije čine Palo Alto moćnim alatom za osiguranje i upravljanje mrežnim prometom u realnom vremenu[26].



Slika 19 - Dubinska inspekcija paketa DPI
Izvor: https://smex.org/wp-content/uploads/2019/02/DPI-App-data-1024x426.png

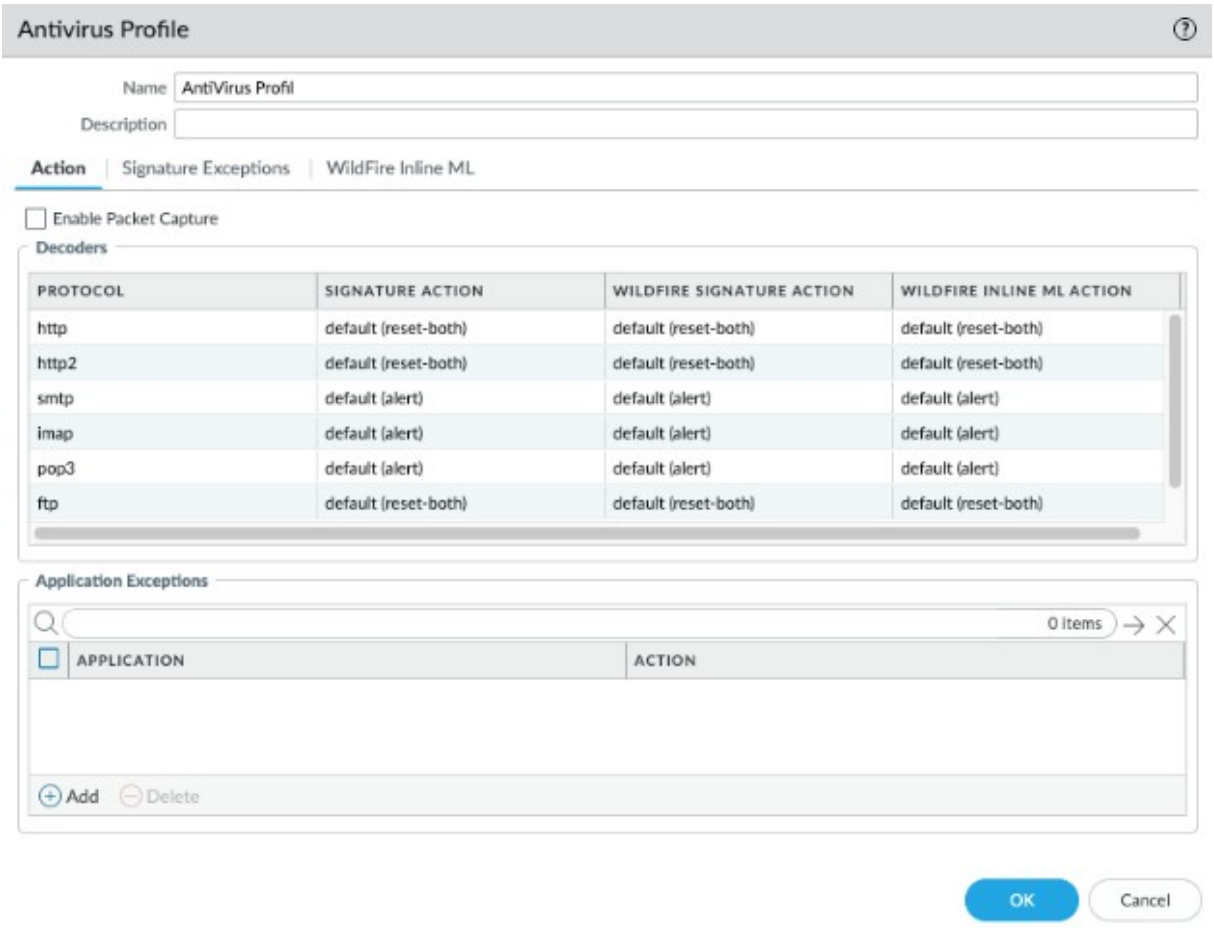
Slika 19 prikazuje razliku između tradicionalne analize paketa i dubinske inspekcije paketa. Tradicionalna analiza paketa obuhvaća samo IP i TCP slojeve, dok dubinska inspekcija paketa uključuje i analizu podataka aplikacije.

[26] Palo Alto Official Documentation

5.6 Palo Alto vatrozid - Sigurnosni Profili

Antivirusni Profili

Antivirusni profili skeniraju promet kako bi otkrili i blokirali poznate viruse, trojane i druge maliciozne datoteke koje mogu ugroziti sigurnost mreže. Palo Alto antivirusni profili koriste ažurirane antivirusne potpise na dnevnoj bazi kako bi osigurali da su najnovije prijetnje pravovremeno prepoznate i blokirane.



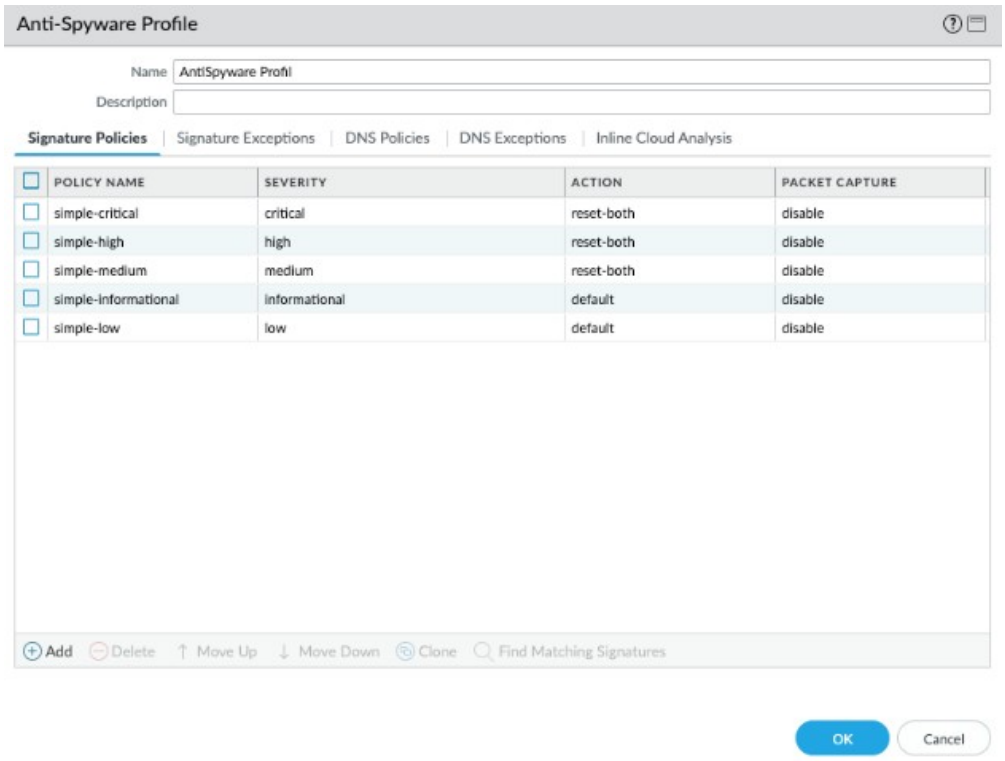
Slika 20 - Palo Alto AntiVirus Profil

Osim skeniranja web prometa (HTTP/HTTPS), antivirusni profil može skenirati i druge protokole kao što su SMTP (e-pošta), IMAP (e-pošta), POP3(e-pošta) i FTP (mrežni transfer podataka). Na profilu se podese akcije koje će se odraditi kad se prepozna virusni potpis u prometu. Akcije poput dopuštanje prometa, generiranje upozorenja,

odbacivanje prometa ili resetiranje veze između klijenta i servera[27].

Protušpijunski (eng. Anti-Spyware) Profil:

Protušpijunski profili identificiraju i sprječavaju širenje špijunskih i drugih zlonamjernih softvera koji prikupljaju osjetljive podatke bez korisnikovog znanja. Korist metode prepoznavanja uzoraka i analizu ponašanja za otkrivanje prijetnji. Palo Alto koristi metode prepoznavanja uzoraka (eng. Signature-based detection) i analizu ponašanja kako bi identificirao i spriječio širenje špijunskih softvera unutar mreže.



Slika 21 - Palo Alto Anti-Spyware Profil

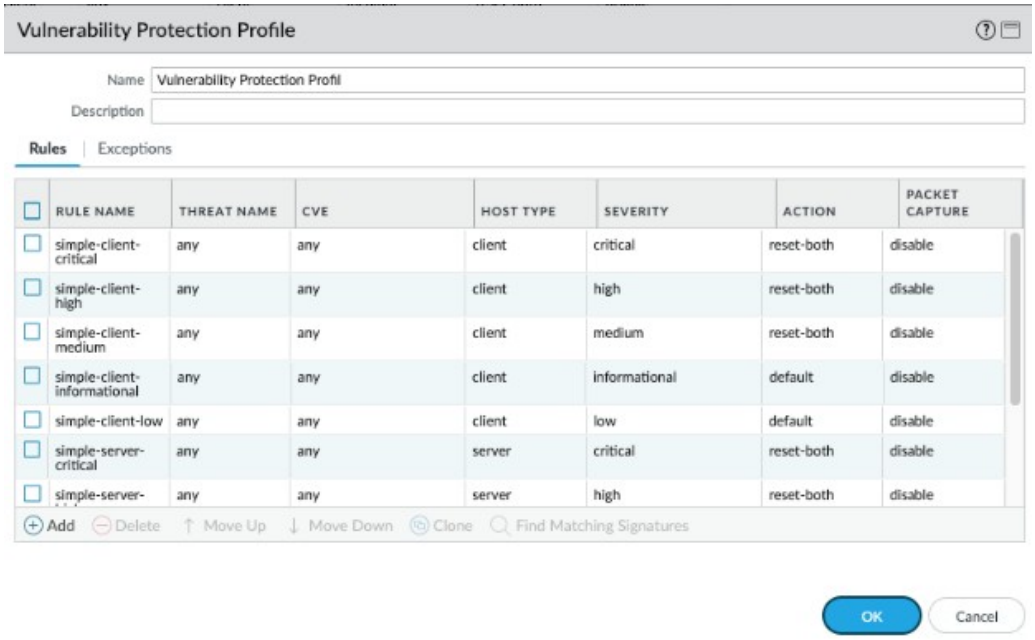
Nudi mogućnost postavljanja akcija koje će se odraditi kad se u prometu detektira špijunski softver kao što su generiranje upozorenja, odbacivanje prometa ili resetiranje veze između klijenta i servera. Uz sve to, protušpijunski profil nudi funkcionalnosti poput prepoznavanja botnet mreža (eng. *Botnet Detection*) što radi prepoznavanje i blokiranje zlonamjernih botova koji mogu komunicirati s udaljenim serverima (eng. Command & Control), te DNS preusmjeravanja (eng. *DNS sinkhole*) koji se koristi za preusmjeravanje zaraženih uređaja na lažnu IP adresu kako bi se

[27] Palo Alto Official Documentation

identificirali zaraženi uređaji unutar mreže[28].

Profili za zaštitu ranjivosti (eng Vulnerability Protection):

Ovi profili štite mrežu od poznatih ranjivosti i eksploatacijskih napada tako što otkrivaju i blokiraju pokušaje iskorištavanja sigurnosnih propusta. Redovito se ažuriraju potpisima koji prepoznaju pokušaje iskorištavanja ranjivosti kako bi pružili zaštitu od novih i postojećih prijetnji čime osiguravaju sigurnost mreže.



Slika 22 - Palo Alto Vulnerability Protection Profil

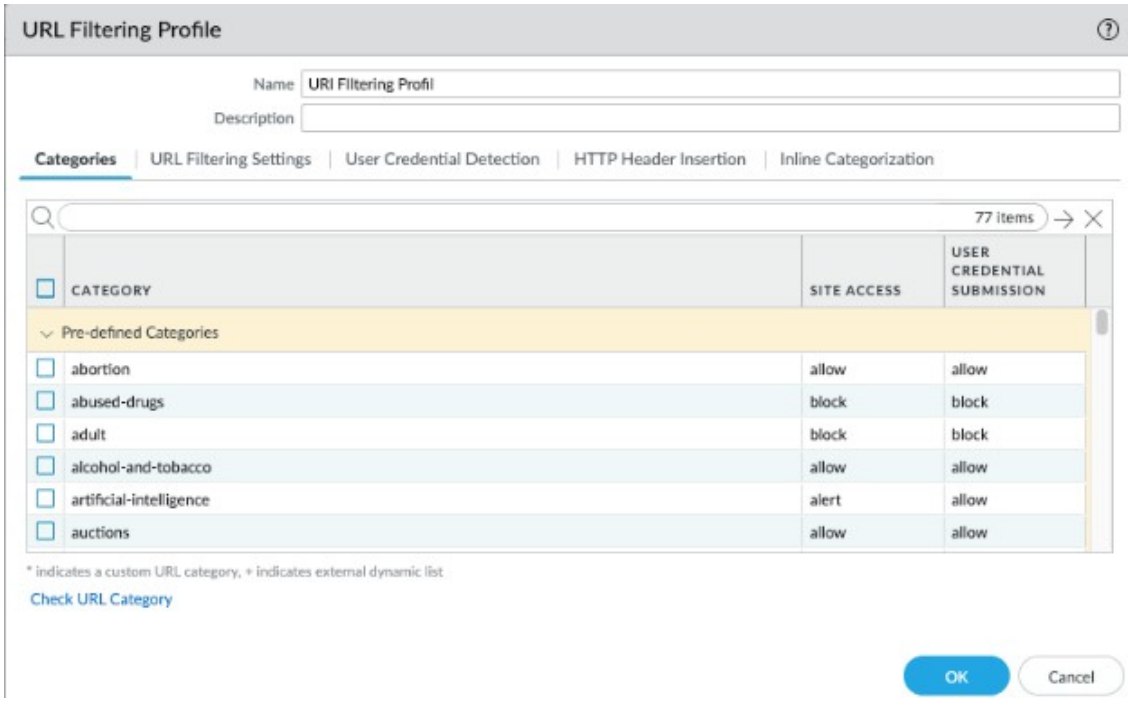
Kada se u mrežnom prometu moguća prijetnja detektira ovisno o postavljenoj akciji dogodit će se generiranje upozorenja, odbacivanje prometa ili resetiranje veze između klijenta i servera. Ovaj profil pomaže zaštiti kao što su prekoračenje međuspremnika (eng. Buffer overflows) i nezakonitog izvršavanja koda (eng. Illegal code execution)[29].

Profil za filtriranje URL-ova (URL Filtering):

Profili za filtriranje URL-ova kontroliraju pristup web stranicama na temelju njihovih kategorija ili specifičnih URL-ova čime se sprječava pristup zlonamjernim, phishing i neprimjerenim web stranicama. Pomažu u provođenju sigurnosnih politika i povećanju produktivnosti. Administratori također mogu definirati vlastite kategorije

[28] Palo Alto Official Documentation
[29] Palo Alto Official Documentation

URL-ova kako bi prilagodili filtriranje specifičnim potrebama organizacije.



Slika 23 - Palo Alto URL Filtering Profil

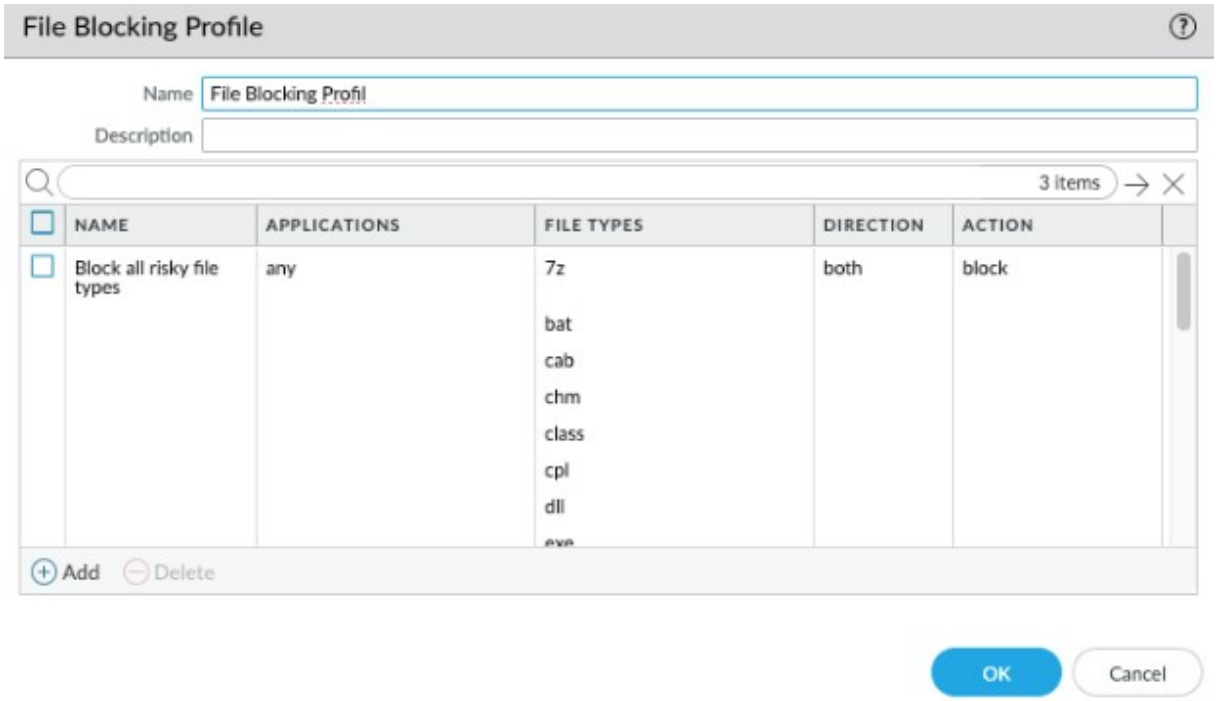
Palo Alto nudi napredno filtriranje URL-ova (eng. *Advanced URL Filtering*) koje štiti od zlonamjernih URL-ova koji su ažurirani ili uvedeni prije nego što ih je Palo Alto baza analizirala i dodala u bazu podataka te se ista baza sinkronizirala s lokalnom bazom na Palo Alto uređaju. Napredno filtriranje i analiza provode se pomoću Palo Alto modula u oblaku (eng. *cloud-based*) pri čemu mehanizam temeljen na strojnome učenju otkriva i blokira zlonamjerne web stranice provodeći inspekciju za phishing i zlonamjerni JavaScript kod koji se može nalaziti na web mjestu tj. web stranici.

Akcije se postavljaju na bazi URL kategorije i mogu uključivati upozorenje (eng. Alert), dopusti (eng. Allow), blokiraj (eng. Block), nastavi (eng. Continue), nadjačaj (eng. Override) ili ne poduzimaj nikakvu akciju (eng. None). Upozorenje generira zapis (eng. Log), dopusti ne generira zapis te dopušta pristup URL-u, dok blokiranje i nastavljanje također generiraju zapis samo što „nastavljanje“ upozorava korisnika da pristupa sumnjivoj stranici. Akcija nadjačaj omogućuje privremeni pristup uz unos lozinke, a akcija "None" ne poduzima nikakvu radnju[30].

[30] Palo Alto Official Documentation

Profil za blokiranje datoteka (eng. File Blocking):

Ovi profili omogućuju blokiranje prijenosa specifičnih vrsta datoteka putem mreže čime se sprječava distribucija potencijalno opasnih datoteka. Ovo je posebno korisno za sprječavanje širenja malvera kroz ekstenzije datoteka koje su poznate po tome što sadrže zlonamjerni kod [31].



Slika 24 - Palo Alto File Blocking Profil

Pomoću ovog profila administratori mogu definirati koje vrste datoteka će se blokirati, poput „.exe“, „.bat“, „.pdf“ i sličnih. Također kao i drugi sigurnosni profili, i ovaj nudi različite akcije koje se poduzimaju kada se otkrije navedena vrsta datoteke. Te akcije uključuju obavijest (eng. Alert) korisniku, blokiranje (eng. Block) datoteke, te mogućnost nastavljanja (engl. Continue) gdje će korisniku biti prikazana stranica s na kojoj korisnik može kliknuti kako bi nastavio odnosno preuzeo datoteku. Također je moguće konfigurirati smjer na koji će se primijeniti određena akcija, bilo da se radi o komunikaciji između klijenta i servera ili obrnuto[32].

[31] Official Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide
[32] Palo Alto Official Documentation

Sigurnosna Pravila Vatrozida Nove Generacije Za Zaštitu Informacijskih Sustava

Pristup iz korporativne zone prema menadžment zoni:

Računala koja se nalaze u korporativnoj zoni mogu komunicirati samo s određenim IP adresama odnosno poslužiteljima u menadžment zoni, i to samo koristeći specifične aplikacije umjesto brojeva vrata. Konkretno, pristup domenskom kontroleru omogućen je putem aplikacija LDAP, LDAPS i NTP, dok je pristup DNS poslužitelju dopušten isključivo preko aplikacije DNS. Sva ostala komunikacija između ove dvije zone je strogo zabranjena. Za identifikaciju korisnika koristi se Palo Alto funkcionalnost User-ID koja koristi Active Directory grupu u kojoj se nalaze korisnički računi svih zaposlenika. Dodatno na sav dozvoljeni promet primijenit će se dekripcija kako bi se omogućila inspekcija šifriranog prometa čime se osigurava dodatna razina sigurnosti mrežnog prometa

Pristup iz korporativne zone prema DMZ zoni:

Računala koja se nalaze u korporativnoj zoni mogu komunicirati s određenim IP adresama unutar DMZ zone samo putem specifičnih aplikacija. Dopušten je pristup datotečnom poslužitelju za promet koji koristi aplikaciju SMB, dok je pristup web poslužitelju omogućen preko aplikacije WEB-BROWSING. Sva ostala komunikacija između ove dvije zone je strogo zabranjena. Za identifikaciju korisnika koristi se Palo Alto funkcionalnost User-ID, koja se oslanja na Active Directory grupu u kojoj se nalaze korisnički računi svih zaposlenika. Također na sav dozvoljeni promet primijenit će se dekripcija, čime se omogućava inspekcija šifriranog prometa i dodatna sigurnost mrežnog prometa.

Pristup iz VPN zone prema menadžment zoni:

Računala odnosno korisnici koji su spojeni putem VPN-a nalaze se u VPN zoni te je iz te zone moguće pristupiti određenim IP adresama u menadžment zoni isključivo putem određenih aplikacija. Pristup domenskom kontroleru omogućen je kroz aplikacije

LDAP, LDAPS i NTP, dok je pristup DNS poslužitelju dopušten samo putem aplikacije DNS. Sva ostala komunikacija je zabranjena. Funkcionalnost User-ID koristi se za identifikaciju korisnika kroz Active Directory grupu koja sadrži račune svih zaposlenika. Dodatno, dekripcija se primjenjuje na dozvoljeni promet kako bi se omogućila inspekcija šifriranog prometa, osiguravajući dodatnu sigurnost.

Pristup iz VPN zone prema DMZ zoni:

Korisnici odnosno računala spojena putem VPN-a mogu pristupiti određenim IP adresama u DMZ zoni samo preko određenih aplikacija kao što je SMB za pristup datotečnom poslužitelju i aplikacija WEB-BROWSING za pristup web poslužitelju. Sve ostale vrste komunikacije su zabranjene. Također se koristi User-ID funkcionalnost za identifikaciju korisnika pomoću Active Directory grupe. Kako bi se osigurala inspekcija šifriranog prometa na sav dozvoljeni promet primijenjena je dekripcija mrežnog prometa.

Poseban pristup za mrežne i serverske administratore:

Mrežnim i serverskim administratorima dopušten je pristup svim potrebnim resursima prema menadžment zoni. Svi serverski administratori mogu pristupiti poslužiteljima putem aplikacije MS-RDP, dok se identifikacija korisnika se radi pomoću Active Directory grupe Server_Administratori u kojoj se nalaze samo korisnički računi serverskih administratora.

Server Administratori VPN prema Mena...	none	universal	VPN	10.115.80.0/23	Server_Administratori	any	Menadzment	10.115.40.0/24	any	ms-rdp
Mrezni Administratori VPN prema Men...	none	universal	VPN	10.115.80.0/23	Mrezni_Administratori	any	Menadzment	10.115.40.0/24	any	ssh

Slika 25 - Sigurnosno pravilo za mrežne i serverske administratore

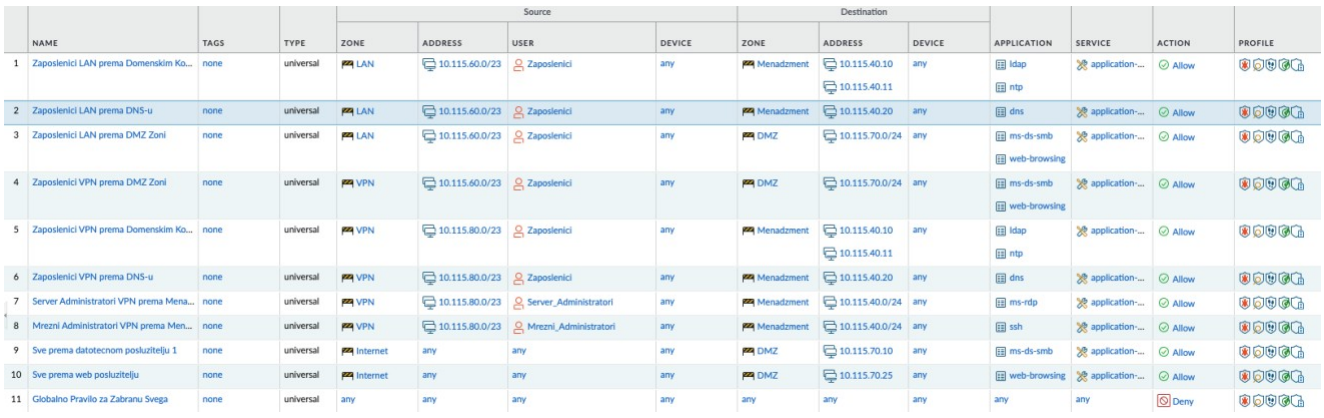
Mrežni administratori imaju pristup svim mrežnim uređajima kroz aplikaciju SSH unutar menadžment zone. identifikacija korisnika se radi pomoću Active Directory grupe Server_Administratori u kojoj se nalaze samo korisnički računi serverskih administratora. Također, i na ovaj promet se primjenjuje inspekcija šifriranog prometa.

Pristup s javnog interneta prema DMZ zoni:

Dopušten je pristup sa bilo koje javne IP adrese prema datotečnom i web poslužitelju unutar DMZ zone, i to samo putem specifičnih aplikacija. Pristup datotečnom poslužitelju dopušten je samo za promet koji koristi aplikaciju SMB, dok je pristup web poslužitelju omogućen preko aplikacije WEB-BROWSING.

Sigurnosni profili kao dodatna zaštita na sigurnosnim pravilima

- Antivirusni profil: Sav ulazni i izlazni promet bit će pregledan na prisutnost zlonamjernih datoteka i softvera.
- Protušpijunski profil: Promet će biti pregledan kako bi se identificirali i blokirali špijunski softveri.
- Profil za zaštitu od ranjivosti: Prepoznat će se i blokirati eksploatacije poznatih ranjivosti u mrežnim aplikacijama i sustavima.
- Profil za blokiranje datoteka: Blokiranje ekstenzija određenih datoteka koje se često koriste za širenje zlonamjernog softvera.[33]



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	Zaposlenici LAN prema Domenskim Ko...	none	universal	LAN	10.115.60.0/23	Zaposlenici	any	Menadzment	10.115.40.10 10.115.40.11	any	ldap ntp	application-...	Allow	
2	Zaposlenici LAN prema DNS-u	none	universal	LAN	10.115.60.0/23	Zaposlenici	any	Menadzment	10.115.40.20	any	dns	application-...	Allow	
3	Zaposlenici LAN prema DMZ Zoni	none	universal	LAN	10.115.60.0/23	Zaposlenici	any	DMZ	10.115.70.0/24	any	ms-ds-smb web-browsing	application-...	Allow	
4	Zaposlenici VPN prema DMZ Zoni	none	universal	VPN	10.115.60.0/23	Zaposlenici	any	DMZ	10.115.70.0/24	any	ms-ds-smb web-browsing	application-...	Allow	
5	Zaposlenici VPN prema Domenskim Ko...	none	universal	VPN	10.115.80.0/23	Zaposlenici	any	Menadzment	10.115.40.10 10.115.40.11	any	ldap ntp	application-...	Allow	
6	Zaposlenici VPN prema DNS-u	none	universal	VPN	10.115.80.0/23	Zaposlenici	any	Menadzment	10.115.40.20	any	dns	application-...	Allow	
7	Server Administratori VPN prema Mena...	none	universal	VPN	10.115.80.0/23	Server_Administratori	any	Menadzment	10.115.40.0/24	any	ms-rdp	application-...	Allow	
8	Mrezni Administratori VPN prema Men...	none	universal	VPN	10.115.80.0/23	Mrezni_Administratori	any	Menadzment	10.115.40.0/24	any	ssh	application-...	Allow	
9	Sve prema datotecnom posluzitelju 1	none	universal	Internet	any	any	any	DMZ	10.115.70.10	any	ms-ds-smb	application-...	Allow	
10	Sve prema web posluzitelju	none	universal	Internet	any	any	any	DMZ	10.115.70.25	any	web-browsing	application-...	Allow	
11	Globalno Pravilo za Zabranu Svega	none	universal	any	any	any	any	any	any	any	any	any	Deny	

Slika 26 - Sigurnosna Pravila na Vatrozidu Nove Generacije (Palo Alto)

Kao što je vidljivo na slici 26 na vrhu su sigurnosna pravila koja dopuštaju ranije navedenu komunikaciju po određenim aplikacijama, dok je na dnu globalno pravilo

[33] Palo Alto Službena Dokumentacija

koje blokira sav ostali promet. Vatrozid nove generacije također uspoređuje pakete sa sigurnosnim pravilima od vrha prema dnu (eng. *Top-down*) i primjenjuje politiku prvog pravila koje se podudara, ignorirajući sva sljedeća pravila.

6.Moguće Vrste i Tipovi Napada

Da bi zaštitili informacijske sustave od hakerskih napada potrebno je poznavati i same napade. Napade možemo podijeliti na pasivne i aktivne napade. Aktivni napadi su oni kada napadač tijekom napada odrađuje i izvršava neke akcije koje utječu direktno na sustav te ga mijenjaju prema vlastitim potrebama. Dok kod pasivnih napada napadači pokušavaju do povjerljivih informacija ali bez mijenjanja sustava s ciljem da ostanu neotkriveni.

6.1 Čovjek u sredini (eng. Man in the middle – MITM) Napad

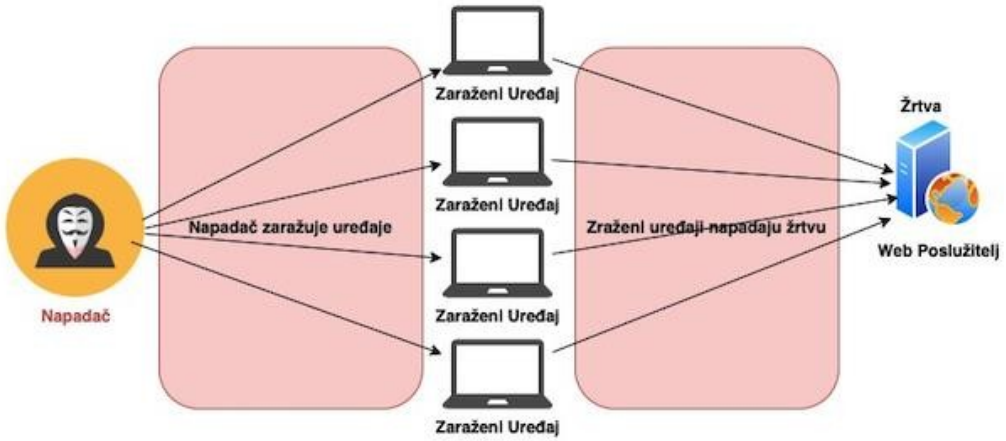
Ovim napadom napadač upada u sredinu između komunikacije dviju strana što mu omogućuje prisluškivanje podataka koji se šalju između tih dviju strana. Uz prisluškivanje napadač može mijenjati te podatke, što može dovesti do krađe osjetljivih i povjerljivih informacija ili unošenja lažnih podataka i informacija u komunikaciju[34].

Slika 27 - Napad čovjeka u sredini

[34] William Stallings & Lawrie Brown – Computer Security: Principles and Practice

6.2 Distribuirani napad uskraćivanja usluge (eng. Distributed Denial of Service)

Jedan on najčešće korištenih napada je Denial of service (DoS) odnosno Distributed Denial od Service (DdoS) a oni imaju cilj da opterete uređaj koji je meta napada do te mjere da više nije u mogućnosti odgovoriti na valjane upite odnosno s DdoS napadam se čini ista stvar samo je napad organiziran od strane više uređaja koji su prethodno zaraženi zlonamjernim softverom te se taj napad izvodi puno brže nego DoS[35].



Slika 28 - DDoS Napad

6.3 Napad Iznuđivanja (eng. Ransomware)

U današnje vrijeme ovi napadi su sve češći. Metama napada podaci budu zaključani, tj. zakriptirani, te dobiju ultimatum da plate određenu svotu za dekripcijski ključ ili će ostati bez podataka. Najčešće napadači dođu do resursa nekog računala preko zaražene datoteke koju meta napada preuzme. Nakon preuzimanja datoteke, zlonamjerni softver iz datoteke šifrira sve podatke kojima može pristupiti[36].

Slika 29 – Napad iznuđivanja

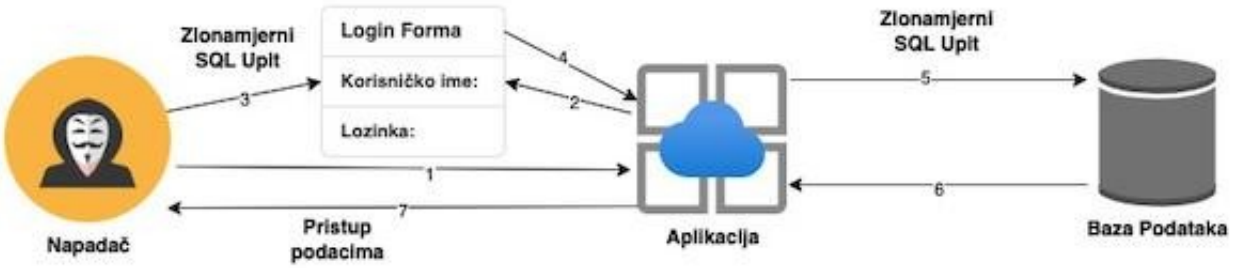
[35] William Stallings – Network Security Essentials: Applications and Standrads
[36] Allan Liska & Timothy Gallo - Ransomware: Defending Against Digital Extortion

6.4 Iskorištavanje 0-dan ranjivosti (eng. 0-day Exploit)

Napad iskorištavanja ranjivost nultog-dana (eng. *zero-day vulnerability*) predstavlja sigurnosni propust u softveru koji napadači otkriju prije nego što programeri postanu svjesni njenog postojanja. Ova vrsta ranjivosti omogućava napadačima da iskoriste propust odnosnu „rupu“ u sistemu za napade, krađu podataka, preuzimanje kontrole nad sistemom i druge aktivnosti prije nego što bilo kakva zaštita bude dostupna. Zbog toga što nema dostupnih zakrpa (eng. Patch) ili zaštite u trenutku napada, ovakve ranjivosti predstavljaju ozbiljnu prijetnju korisnicima[37].

6.5 SQL Injekcija (eng. SQL Injection)

Ovim napadom napadači iskorištavaju sigurnosne ranjivosti u aplikacijama koje komuniciraju s bazama podataka manipulirajući SQL upitima koji se šalju bazi podataka. Napadač ubacuje zlonamjerni SQL kod u polje za unos podataka što može dovesti do neovlaštenog pristupa, modifikacije podataka ili čak brisanja podataka iz baze. To je jedan od najčešćih i najopasnijih oblika kibernetičkih napada jer može imati katastrofalne posljedice za sigurnost podataka[38]. Da bi se zaštitili od ovakvih napada, preporučuje se koristiti vatrozid nove generacije koji kontrolom mrežnog prometa može prepoznati i blokirati pokušaje napada u stvarnom vremenu osiguravajući da zlonamjerni SQL upiti ne dođu do baze podataka.



Slika 30 - Napad SQL Injekcije

[37] Yurong Chen - Zero-day Defense: Discovering and Removing Vulnerabilities through Program Customization and Fuzzing
[38] Halfond, W. G., Viegas, J., & Orso -A Classification of SQL-Injection Attacks and Countermeasures

7.Zaključak

Sigurnost informacijskih sustava danas predstavlja jedan od najvećih izazova zbog stalnog razvoja novih zlonamjernih softvera koji ciljaju osjetljive informacije. Smatram da je ključno posvetiti se sigurnosti vlastite mreže i vlastitih informacijskih sustava uvođenjem ne samo vatrozida kao sigurnosne komponente nego i antivirusne zaštite na računalima i poslužiteljima. Primjenom vatrozida ne samo da se zaustavljaju razni pokušaji napada na informacijski sustav već i omogućuje mrežnim administratoru i timovima za kibernetičku sigurnost kontinuirano nadgledanje mreže, praćenje i analizu pokušaja napada čime se mogu pripremite za buduće prijetnje.

Tradicionalni vatrozidi štite mreže filtriranjem prometa na osnovi IP adresa, protokola i vrata, dok s druge strane vatrozidi nove generacije nude napredne funkcije poput dubinske inspekcije paketa, kontrole aplikacija i prevencije upada, pružajući bolju zaštitu informacijskih sustava.

Svim kompanijama i ustanovama bi preporučio korištenje vatrozida nove generacije za obranu informacijskih sustava jer pružaju napredniju zaštitu protiv suvremenih prijetnji. Iako u startu koštaju više od tradicionalnih vatrozida radi svojih naprednih dodatnih sigurnosnih funkcija, smatram da će se kroz godine to višestruko isplatiti jer će informacijski sustav biti zaštićeniji i otporniji na razne pokušaje napada.

8. Literatura

1. Timothy Lightoler – *The Gentlemand and Farmer's Architect* (1757-1762) - Izvor: https://www.betterworldbooks.com/product/detail/the-gentleman-and-farmer-s-architect-9783337102982
2. Kenneth Ingham and Stephanie Forrest – *A History and Survey of Network Firewalls*, Kenneth Ingham Consulting and University of New Mexico (2002) - Izvor: https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf
3. William Stallings - *Network Security Essentials: Applications and Standards* (2011 4th Edition) - Izvor: https://elhacker.info/manuales/Redes/3._Network-security-essentials-4th-edition-william-stallings.pdf
4. William Stallings – *Computer Security Principles and Practice* (2017 4th Edition) - Izvor: https://www.mcu.edu.ng/home/wp-content/uploads/2023/11/Computer-Security-Principles-and-Practice-by-William-Stallings-Lawrie-Brown-z-lib.org_.pdf
5. Thomas A. Johnson - *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (2020) - Izvor: https://www.routledge.com/Cybersecurity-Protecting-Critical-Infrastructures-from-Cyber-Attack-and-Cyber-Warfare/Johnson/p/book/9780367599362
6. Charles J. Brooks - *Cybersecurity Essentials* (2018) - Izvor: https://a.co/d/3Qi8veX
7. Eric Maiwald – *Network Security: A Beginner's Guide* (2012 3rd Edition)
8. Official Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide - Izvor: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnsa-study-guide.pdf
9. Službena dokumentacija Palo Alto - Izvor: https://docs.paloaltonetworks.com/resources
10. Allan Liska & Timothy Gallo - *Ransomware: Defending Against Digital Extortion* (2017 1st Edition) - Izvor: https://www.amazon.com/_/dp/1491967889?smid=ATVPDKIKX0DER&_encoding=UTF8&tag=oreilly20-20
11. Cisco ASA 5500 Series Configuration Guide - Izvor: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/about.html

12. Meghdeep Mukherjee – *The Ohio State University – Palo Alto Networks Analysis* - Izvor: https://files.fisher.osu.edu/department-finance/public/2020-12/mukherjeemeghdeep_475546_21846342_Palo%20Alto%20Networks%20Report%20-%20Meghdeep%20%281%29.pdf?AFvLA5_qvGlp_duXDD4PfYl8CTuNlJSB
13. Insider - *Palo Alto Networks named a Ten-Time Leader in Gartner Magic Quadrant* - Izvor: https://insider.govtech.com/california/sponsored/palo-alto-networks-named-a-ten-time-leader-in-gartner-magic-quadrant-for-networks-firewalls
14. Yurong Chen - Zero-day Defense: Discovering and Removing Vulnerabilities through Program Customization and Fuzzing – Izvor: https://scholarspace.library.gwu.edu/downloads/tq57nr84m?disposition=inline&locale=en

9. Popis Slika i Tablica