MEST Journal – FBIM Transactions SP
DOI 10.12709/mest.13.13.SP2.01

FIREWALL KAO PRVA LINIJA ODBRANE OD MITM NAPADA

FIREWALL AS THE FIRST LINE OF DEFENSE AGAINST MITM ATTACKS

Zoran Čekerevac
Independent researcher , Belgrade, Serbia
https://orcid.org/0000-0003-2972-2472

JEL Classification: **C88, D83, K24, L86, O33**

Apstrakt

Mrežni zaštitni zid (firewall) predstavlja prvu liniju odbrane protiv napada „čovek u sredini“ (MITM), koji ugrožavaju poverljivost, integritet i autentičnost komunikacije. Ovaj rad nudi sistematsku klasifikaciju osnovnih MITM tehnika – od ARP trovanja i DNS lažiranja, preko degradacije HTTPS-a (SSL stripping) i otmice sesija, do specijalizovanih varijanti usmerenih na cloud servise, pregledače, mobilne aplikacije i IoT uređaje. Posebno su razmatrane ranjivosti VPN infrastrukture, gde centralizovano dešifrovanje saobraćaja stvara visokovrednu metu, kao i slabosti IoT ekosistema usled nevalidiranih sertifikata i zastarelih fabričkih podešavanja. Analitičko-komparativna metodologija obuhvata pregled literature, statističku procenu ekonomskih troškova MITM incidenata i praktičnu demonstraciju naprednih firewall funkcija kroz Linux iptables/nftables konfigurisanje. Detaljno su prikazane osnovne i napredne sposobnosti modernih firewall rešenja – ACL pravila, stateful inspekcija, inspekcija aplikacionog sloja, DNS filtriranje, TLS inspekcija i integracija sa IDS/IPS sistemima. Ilustrativni primeri iz okruženja popularnih aplikacija ukazuju na prednosti i ograničenja ovih mera. Zaključci naglašavaju da firewall, iako neophodan, nije dovoljan sam po sebi. Efikasna odbrana zahteva višeslojnu arhitekturu koja kombinuje šifrovanje DNS zahteva, strogu validaciju TLS sertifikata, detekciju anomalija i kontinuiranu edukaciju korisnika kako bi se značajno smanjili rizici i ekonomske posledice MITM napada u savremenim digitalnim mrežama.

***Ključne reči**: firewall, MITM napadi, ARP trovanje, DNS spoofing, TLS inspekcija, IDS/IPS, VPN sigurnost, IoT ranjivosti*

Abstract

The network firewall represents the first line of defense against Man-in-the-Middle (MITM) attacks, which threaten the confidentiality, integrity, and authenticity of digital communications. This paper offers a systematic classification of core MITM techniques—ranging from ARP poisoning and DNS spoofing to HTTPS degradation (SSL stripping) and session hijacking—alongside specialized variants targeting cloud services, browsers, mobile applications, and IoT devices. Particular attention is given to vulnerabilities in VPN infrastructure, where

Address of the author:
Zoran Čekerevac
zoran@cekerevac.eu

centralized traffic decryption creates high-value targets, as well as weaknesses in IoT ecosystems due to unvalidated certificates and outdated factory settings. An analytical-comparative methodology is applied, encompassing a literature review, statistical assessment of the economic impact of MITM incidents, and a practical demonstration of advanced firewall capabilities via Linux iptables/nftables configuration. The paper details both fundamental and advanced features of modern firewall solutions, including ACL rules, stateful inspection, application-layer filtering, DNS filtering, TLS inspection, and integration with IDS/IPS systems. Illustrative examples from popular application environments highlight the strengths and limitations of these measures. The findings emphasize that while the firewall is essential, it is not sufficient on its own. Effective defense requires a multilayered architecture that combines encrypted DNS requests, strict TLS certificate validation, anomaly detection, and continuous user education to significantly reduce the risks and economic consequences of MITM attacks in contemporary digital networks.

Keywords: *firewall, MITM attacks, ARP poisoning, DNS spoofing, TLS inspection, IDS/IPS, VPN security, IoT vulnerabilities*

1 UVOD

Ovaj članak je razvijen na osnovu konceptualne strukture prethodno objavljene verzije na engleskom jeziku pod naslovom „Firewall-based defense strategies against man-in-the-middle attacks“ (Cekerevac Z. , 2025). Iako oba rada dele tematski okvir i metodološki pristup, srpska verzija je prilagođena domaćem akademskom kontekstu, uz dodatne terminološke, stilističke i sadržinske dopune. Rad ne predstavlja doslovan prevod, već samostalnu obradu iste istraživačke ideje.

1.1 Osnove hakovanja i motivacija hakera

Hakerisanje obuhvata sve neautorizovane metode interakcije sa informacionim sistemima, pri čemu akteri, poznati kao hakeri, ciljaju pristupanje, izmene ili krađu podataka izvan okvira dozvoljenih od strane vlasnika sistema. Hakeri se etički razvrstavaju u black-hat (zlonamerne), white-hat (etičke) i gray-hat (ambivalentne) grupe, koje dele alate i tehnike, ali se razlikuju po motivaciji i ciljevima. Nivoi njihovih veština se kreću od stručnjaka za kreiranje zlonamernog softvera do „skriptnih klinaca“ koji iskorišćavaju poznate ranjivosti bez dubokog razumevanja.

Razlozi za hakovanje uključuju prikupljanje podataka, lažno predstavljanje za prevarne aktivnosti poput DDoS napada, destruktivne namere za oštećenje sistema i hakovanje radi ličnog uzbuđenja ili izazova. Pravni okvir oko hakovanja je složen zbog pitanja poput vlasništva nad podacima u odnosu na vlasništvo nad sistemom, zabrinutosti za privatnost i dvosmislenih granica zakonitog ponašanja na mreži. Hakeri snose odgovornost za pravne posledice neovlašćenih radnji. Tehnike hakovanja kreću se od fizičke krađe uređaja do sofisticiranih mrežnih napada koji iskorišćavaju otvorene portove, zadnja vrata i taktike socijalnog inženjeringa kao što su phishing[1] i lažno predstavljanje radi dobijanja akreditiva. Softverska „uskršnja jaja“[2] koja su ostavili programeri se takođe mogu iskoristiti za napade. Jedan od značajnijih načina hakovanja je MITM napad koji je tema ovog rada i detaljnije izložen u sekciji 3.
Uspešno hakovanje zahteva pažljivo planiranje, uzimajući u obzir ciljeve napadača, profitabilnost, metode (masovni naspram ciljanih napada) i potencijalne posledice. Uspešni napadi zahtevaju značajan napor i nisu trenutni.

[1] "Phishing" se odnosi na pokušaj krađe osetljivih informacija, obično u obliku korisničkih imena, lozinki, brojeva kreditnih kartica, informacija o bankovnom računu ili drugih važnih podataka za korišćenje ili prodaju ukradenih informacija. Maskirajući se kao ugledni izvor sa primamljivim zahtevom, napadač mami žrtve da ih prevari, slično kao što ribar koristi mamac da uhvati ribu.

[2] Softverska 'uskršnja jaja' (engl. *software Easter eggs*) su skriveni sadržaji, funkcije ili poruke koje su programeri namerno ubacili u softver, a koji nisu deo zvanične funkcionalnosti. Oni su često zabavni, duhoviti ili nostalgični, i otkrivaju se samo ako korisnik zna tačan niz koraka ili komandi. Primeri:

- Google Search: Ukucajte "do a barrel roll" i stranica će se okrenuti.
- Mozilla Firefox: Ukucajte `about:robots` u adresnu traku i dobićete šaljivu poruku o robotima.

1.2 Motivacija kroz finansijski interes

Sajber napadi uzrokuju značajne finansijske gubitke, uključujući direktnu krađu, troškove čišćenja i tekuće troškove zaštite. Još u 2011. godini, hakeri su zaradili 12,5 milijardi dolara, a zabeleženi su i značajni korporativni gubici (Stanescu, 2012). U novije vreme i pored svih mera zaštite, štete su daleko veće. Tako, npr:

- Prosečna cena jednog data breach-a u 2024. iznosila je 4,88 miliona USD, što je za oko 10 % više u odnosu na 2023. kada je iznosila 4,45 miliona USD po organizaciji, ali je u 2025. godini opala za 9 %, na 4,44 miliona USD. (IBM, 2025). To može da znači da se organizacije bolje štite, ali i da napadači učestalije napadaju i male organizacije.
- Prema izveštaju Verizona (2025) ističu se sledeći nalazi:
  - 30% kršenja bezbednosti uključuje treće strane, što je dvostruko više nego prethodne godine; uzroci uključuju ranjivosti i prekide poslovanja.
  - Broj napadača koji koriste ranjivosti za početni pristup porastao je za 34% u odnosu na prošlu godinu.
  - Organizacije su otklonile 54% ranjivosti na perimetru uređaja, dok je gotovo polovina ostala nerešena.
  - 44% analiziranih incidenata uključuje ransomware, što predstavlja značajan porast u odnosu na prethodni izveštaj.

Pojava AI alata poput ChatGPT-a krajem 2022. dovela je do eksplozije phishing kampanja, pri čemu je njihov broj u narednih šest meseci porastao za više od 40 puta u odnosu na prethodni period (SOCRadar, 2024). Pre pojave AI modela, phishing i-mejlovi su često bili gramatički loši, sa očiglednim greškama. ChatGPT je omogućio generisanje gramatički ispravnih, stilistički uverljivih i-mejlova. Napadači su to iskoristili za pisanje personalizovanih poruka koje deluju kao da dolaze od kolege, banke, IT podrške, itd. Rezultat: Veća stopa uspešnosti napada. Pored toga, AI može generisati stotine varijacija phishing poruka u sekundi. Napadači mogu da koriste skripte koje kombinuju ChatGPT sa i-mejl automatima.

Tokom 2021. godine, prosečni trošak sajber incidenta iznosio je preko 670 hiljada evra za svaki sat aktivnog trajanja napada, dok je broj kompromitovanih naloga premašio milijardu (AAG, 2025).

Prema podacima sa sajta CVEdetails.com, koji prati javno objavljene CVE identifikatore, tokom 2024. godine otkriveno je preko 40.000 ranjivosti, dok je u prvih sedam meseci 2025. već registrovano više od 30.000 (CVEdetails, 2025). Na osnovu analize alata poput CVEmap i podataka iz GitHub zajednice, procenjuje se da je između 35–45% tih ranjivosti imalo dostupni proof-of-concept (PoC) exploit kod — što ih čini tehnički dostupnim za eksploataciju. Takve ranjivosti su ili su mogle biti iskorišćene u različitim vrstama sajber napada: ransomware, phishing, supply chain attacks, privilege escalation, remote code execution, zero-day exploitation. Prema izveštaju Hackmanac Cyber Threat Report 2024 (2024), prosečna šteta po sajber napadu tokom te godine iznosila je oko 5 miliona USD. Ova cifra obuhvata ukupne troškove — od otkupa i tehničke sanacije, do gubitka reputacije i prekida poslovanja. Ipak, važno je napomenuti da prosek značajno odstupa u zavisnosti od cilja napada: dok velike organizacije beleže višemilionske gubitke, pojedinci i mali biznisi često trpe štetu koja je znatno manja, ali i za njih veoma značajna. Prema izveštaju NETSCOUT Threat Intelligence Report, samo u prvih šest meseci 2024. godine zabeleženo je u proseku oko 41.000 DDoS napada dnevno ili približno 7,5 miliona DDoS napada što predstavlja povećanje od 30 % u odnosu na isti period prethodne godine (NETSCOUT, 2024).

2 METODOLOGIJA

U skladu sa ciljevima istraživanja, postavljena su sledeća istraživačka pitanja:

RQ1: Da li je firewall uopšte upotrebljiv za zaštitu od MITM napada?

RQ2: Ako jeste, kako pravilno konfigurisani firewall, u kombinaciji sa višeslojnom bezbednosnom arhitekturom, može efikasno ublažiti rizik od MITM napada u savremenim digitalnim okruženjima?

Istraživanje je sprovedeno primenom analitičko-komparativne metodologije, uz kombinaciju teorijske analize, studija slučaja i tehničke demonstracije. Sledeće komponente činile su osnovu metodološkog okvira:

- Analiza tehnika MITM napada i njihovih varijacija
- Komparacija klasičnih i naprednih funkcionalnosti firewall sistema
- Studije slučaja MITM scenarija u okruženju aplikacija Viber i WhatsApp
- Uporedna analiza VPN i Tor[3] infrastrukture u kontekstu bezbednosne otpornosti
- Statistički pregled finansijskog uticaja MITM incidenata
- Demonstracija `iptables` pravila u Linux okruženju kao praktičnog primera konfiguracije

Pregled literature je obuhvatio akademske baze podataka kao što su Google Scholar**,** IEEE Xplore**,** SpringerLink i MDPI**,** uz dopunsko korišćenje specijalizovanih tehničkih izvora fokusiranih na konfiguraciju firewall sistema. Zbog kompleksnosti teme, u procesu pretrage i selekcije korišćeni su alati veštačke inteligencije radi optimizacije formulacije upita, apstraktnog skrininga i preliminarnog izbora relevantnih publikacija.

Kriterijumi za uključivanje izvora obuhvatali su tematsku relevantnost, metodološki kvalitet i datum objavljivanja. Većina analiziranih radova potiče iz poslednjih pet godina, uz dodatak prethodnih publikacija autora u oblasti MITM napada.

Prikupljeni materijal je podvrgnut kritičkoj analizi, uz primenu akademskih standarda za validaciju izvora, procenu pouzdanosti nalaza i njihovu relevantnost za definisani istraživački problem. Informacije su organizovane kroz tematsku analizu, kojom su identifikovani ključni bezbednosni domeni, ponavljajući obrasci i konceptualni okvir koji integriše postojeće znanje.

Radi preglednosti i lakšeg poređenja, pojedini nalazi su predstavljeni u tabelarnom formatu. Na osnovu sprovedene analize, identifikovani su nedostaci u postojećoj literaturi, što je poslužilo kao osnova za formulisanje zaključaka i preporuka.

3 MITM NAPADI

3.1 Uvod u MITM napade

Napadi tipa „čovek u sredini“ (Man-in-the-Middle – MITM) predstavljaju specifičnu klasu sajber upada u kojima se napadač neprimetno pozicionira između dve komunikacione strane, sa ciljem presretanja, preusmeravanja ili izmene prenesenih podataka. Ovakvi napadi direktno ugrožavaju poverljivost, integritet i autentičnost komunikacije, kako u korporativnim, tako i u krajnjim korisničkim okruženjima.

Uobičajeni pravci napada u MITM scenarijima obuhvataju nesigurne Wi-Fi mreže, lažiranje DNS zapisa (*DNS spoofing*, poznat i kao *DNS cache poisoning*), uklanjanje sloja bezbednosti u TLS/SSL protokolima (SSL stripping[4]), kao i otmicu sesija (session hijacking). Sa razvojem cloud tehnologija, Interneta stvari (IoT) i koncepta „donesi sopstvenu tehnologiju“ (Bring Your Own Technology – BYOT[5]), MITM napadi postaju sve prisutniji, jer napadači koriste slabosti u enkripciji, autentifikaciji i mrežnim protokolima.

3.2 Tehnološka osnova MITM napada

MITM napadi su zabeleženi davno pre pojave računara i mogu se uporediti sa zlonamernim poštarom koji presreće pisma. Današnji MITM napadi se oslanjaju na sofisticirane tehnike koje eksploatišu ranjivosti u bezbednosnim protokolima. Posebno su problematične implementacije SSL/TLS protokola, gde složenost administracije često dovodi do jednostrane autentifikacije, ostavljajući prostor za napadače da se predstave kao legitimni entiteti.

Napadač u MITM scenariju može da presretne komunikaciju, da se infiltrira između komunikacionih strana kao posrednik, i da manipuliše sadržajem poruka — na primer, izmenom podataka o uplati na fakturi radi preusmeravanja sredstava ka sopstvenom računu.

[3] Tor (The Onion Router) je decentralizovana mreža i softverski paket koji omogućava anonimnu komunikaciju putem interneta. Tor koristi višeslojno šifrovanje i rutiranje saobraćaja kroz niz nasumično odabranih čvorova (relay servera), čime se identitet korisnika i njegova lokacija efikasno prikrivaju. (Dingledine, Mathewson, & Syverson, 2004)

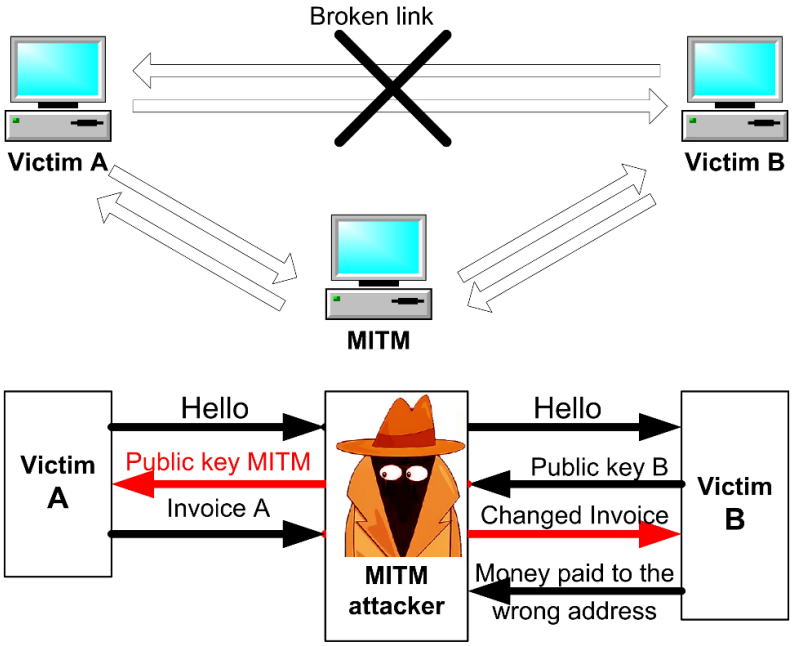
[4] SSL stripping predstavlja tehniku u kojoj napadač presreće HTTPS zahteve i preusmerava ih ka HTTP verziji sajta, čime se uklanja enkripcija i omogućava krađa podataka.

[5] Bring Your Own Technology (BYOT) je strategija ili praksa koja omogućava zaposlenima, studentima ili saradnicima da koriste svoje lične uređaje i tehnologije (laptopove, pametne telefone, aplikacije, cloud servise itd.) za pristup organizacionim resursima, mrežama i podacima.

Najčešće tehnike MITM napada uključuju (OWASP, 2025):

- Trovanje ARP keša (ARP cache poisoning[6])
- Lažiranje DNS zapisa (DNS spoofing)
- Otmicu sesija (session hijacking), uključujući side-jacking“, „evil twin“ i „sniffing“
- Otmicu SSL sesije (SSL hijacking)

Tehnologija MITM napada detaljno je predstavljena u radu Čekerevac et al. (2017a), pa se u ovom tekstu prikazuje samo šematski tok jednog napada, sa jasno označenim informacijskim pravcima. Šema prikazana slikom 1 ilustruje kako napadač, pozicioniran između dve žrtve, presreće i menja komunikaciju, čime kompromituje integritet prenesenih podataka.



Slika 1 Shema MITM napada: presretanje i manipulacija poruka između dve žrtve

Izvor: (Cekerevac et al., 2017a)

Na slici 1 prikazan je tipičan MITM scenario:

- **Žrtva A** (Victim A) inicira komunikaciju porukom „*Hello“*, koju napadač presreće i prosleđuje **Žrtvi B** bez izmena, čime se stvara lažni osećaj direktne veze.
- **Žrtva B** (Victim B) odgovara slanjem svog javnog ključa („*Public key B*“), koji napadač presreće i zamenjuje sopstvenim ključem („*Public key MITM*“) u povratnoj poruci ka **Žrtvi A**.
- Kada **Žrtva A** pošalje fakturu („*Invoice A*“), napadač je menja i prosleđuje izmenjenu verziju („*Changed invoice*“) **Žrtvi B**.
- Na kraju, **Žrtva B** vrši uplatu na pogrešnu adresu („*Money paid to the wrong address*“), verujući da komunicira sa legitimnim partnerom.

Ova šema prikazuje osnovne korake MITM napada: presretanje, manipulaciju i zloupotrebu komunikacije, uz korišćenje lažnih kriptografskih ključeva i modifikovanih poruka. Napadač se neprimetno integriše u komunikacioni kanal, ostavljajući obe strane u uverenju da međusobno komuniciraju direktno

Jedan od ilustrativnih primera je presretanje FTP akreditiva pomoću alata kao što je *dsniff*, koji omogućava napadaču da uhvati korisnička imena i lozinke u otvorenom tekstu, čime se otvara mogućnost za dalju kompromitaciju mreže.

3.3 Evolucija MITM napada

Sa razvojem tehnologije, MITM napadi su evoluirali u više specijalizovanih oblika:

[6] ARP cache poisoning, poznato i kao ARP spoofing, je vrsta sajber napada koji cilja slabosti u Address Resolution Protocol (ARP) — protokolu koji povezuje IP adrese sa MAC adresama unutar lokalne mreže (LAN). Najčešće korišćeni alati u ovu svrhu su *Ettercap, Scapy, Cain & Abel, Bettercap* i *MITMf.*

- *MIT-cloud (MITC):* Eksploatacija sesijskih tokena u cloud servisima radi neovlašćenog pristupa.
- *MIT-mobile (MITMO):* Presretanje mobilnih autentifikacionih kodova (mTAN) putem SMS poruka.
- *MIT-app (MITA):* Umetanje samopotpisanih sertifikata radi presretanja podataka iz aplikacija.
- *MIT-IoT:* Ciljanje IoT uređaja koji ne validiraju SSL sertifikate, čime se omogućava krađa akreditiva.

Napomena: Iako slični po nazivu, MITB (Man-in-the-Browser) napadi se tehnički ne klasifikuju kao MITM, jer se izvode lokalno unutar internet pregledača putem malvera, bez presretanja mrežnog saobraćaja između klijenta i servera

3.4 MITM napadi u kontekstu IoT uređaja

IoT uređaji su posebno ranjivi na MITM napade zbog ograničenih resursa, nedostatka ažuriranja i slabe enkripcije. Napadi se izvode lokalno putem Ethernet ili Wi-Fi mreža, koristeći ARP trovanje, DNS modifikaciju i presretanje HTTPS saobraćaja pomoću samopotpisanih sertifikata ili alata poput SSLstrip.

Mnogi pametni uređaji i dalje ne validiraju TLS/SSL sertifikate, što napadačima omogućava presretanje i krađu lozinki te kompromitaciju konekcija uz pomoć alata kao što su Ettercap, Evilgrade, dsniff i Cain & Abel (Vahab, 2025).. Prema OWASP-u, “Insecure Data Transfer and Storage” ostaje jedna od najraširenijih IoT ranjivosti, budući da veliki broj uređaja ne proverava lanac poverenja sertifikata i često koristi zastarele kriptografske biblioteke. Bluetooth Low Energy (BLE), prisutan u pametnim bravama, termostatima i sigurnosnim kamerama, pokazuje visoku stopu ranjivosti — Hlapisi (2023) dokumentuje da je 70–80 % ispitivanih BLE modela podložno kloniranju, pasivnom presretanju podataka i neautorizovanom preuzimanju kontrole nad uređajima. Ovi noviji nalazi potvrđuju i proširuju ranija zapažanja Springa (2016) i ukazuju na hitnu potrebu za implementacijom strožih mehanizama verifikacije sertifikata i redovnim ažuriranjima firmware-a (Watlecorp, 2025; Hlapisi, 2023).

DDoS i srodni DoS napadi činili su oko 60–64% napada na IoT uređaje u 2016. godini, prema izveštajima McAfee-a i OWASP-a (McAfee, 2016). Milijarde IoT uređaja neprekidno su povezane na nedovoljno nadgledane mreže, što ih čini pogodnim metama za uključivanje u botnet infrastrukture, izvođenje DDoS napada, distribuciju spama i krađu akreditiva. Primeri uključuju napade na pametne habove i frižidere koji često šalju nešifrovane podatke.

IoT uređaji se često isporučuju sa nesigurnim fabričkim podešavanjima — lozinkama, otvorenim interfejsima, zastarelim kodom i bez ažuriranja — što ih čini lakom metom. Povezana vozila su takođe ranjiva, kao u slučaju Jeep Cherokee iz 2015 (Cekerevac et al., 2017), kada je daljinsko hakovanje dovelo do povlačenja 1,4 miliona vozila.

3.5 VPN infrastruktura kao potencijalna tačka MITM napada

Hot-spot mreže, naročito one otvorene i nezaštićene, predstavljaju klasičan ambijent za izvođenje MITM napada. Međutim, zbog ograničenog dometa i fizičke dostupnosti, ovakvi napadi su uglavnom usmereni ka lokalnim i ciljanim grupama korisnika. Nasuprot tome, VPN infrastruktura — kao centralizovana tačka kroz koju prolazi šifrovani saobraćaj velikog broja korisnika — poseduje daleko širi potencijal za kompromitaciju. Iako se VPN servisi uobičajeno percipiraju kao bezbednosni mehanizmi koji štite privatnost, sama arhitektura podrazumeva da sav saobraćaj bude dešifrovan na serverskoj strani pre prosleđivanja ka krajnjoj destinaciji. Ukoliko bi VPN provajder bio zlonameran ili kompromitovan, otvorila bi se mogućnost za presretanje, modifikaciju i analizu saobraćaja — čime bi se stvorili uslovi za sofisticirani MITM napad. Posebno su ranjivi nešifrovani protokoli, nevalidirani sertifikati i neprovereni DNS zahtevi. Imajući u vidu poverenje koje korisnici poklanjaju ovim servisima, od suštinskog je značaja da se biraju rešenja sa transparentnim politikama, otvorenim kodom, nezavisnim bezbednosnim revizijama i tehničkim mehanizmima koji minimizuju rizik od zloupotrebe, bilo od strane samih provajdera, bilo u slučaju njihove kompromitacije. Povoljno je kada bezbednost VPN proveravaju spoljne nezavisne organizacije. Jedan od takvih primera je provera koju je uradila

Mobile Application Security Assessment (MASA) kod VPN provajdera Mullvad (Mullvad, 2025).

U kontekstu zaštite komunikacije, ključno je razlikovati dva koncepta:

- *Poverenje u infrastrukturu*: VPN servisi funkcionišu na osnovu pretpostavke da je provajder pouzdan, da ne vodi logove, da ne sarađuje sa trećim stranama, i da je tehnički sposoban da zaštiti korisnički saobraćaj. Međutim, korisnik nema direktnu kontrolu nad tim aspektima — poverenje je eksterno i često neproverljivo.
- *Tehnička garancija bezbednosti*: Tor mreža, iako sporija, zasniva se na decentralizovanom modelu sa višeslojnim enkripcijama (*onion routing*), gde nijedan čvor ne zna celu putanju. Bezbednost se ne oslanja na poverenje u pojedinačne entitete, već na arhitekturu sistema. Iako izlazni čvor može biti tačka nadzora, prethodni slojevi štite identitet korisnika.

U tabeli 1 je dat uporedni prikaz VPN i Tor-a.

Tabela 1. VPN vs. Tor — Bezbednosna razmatranja

Aspekt	VPN	Tor
Brzina	Brži, pogodan za streaming i rad	Sporiji, zbog višeslojnog rutiranja
Privatnost	Zavisi od provajdera	Ugrađena u samu strukturu sistema
Otpornost na MITM	Ranjiv ako provajder sarađuje sa trećima ili ako je kompromitovan	Veća otpornost, ali izlazni čvor je slab
Uvid i upravljanje komunikacijom*	Ograničena	Veća anonimnost, ali manje kontrole
Pogodnost za svakodnevnu upotrebu	Visoka	Niža, ali korisna za specifične potrebe

** U ovom kontekstu, „uvid i upravljanje komunikacijom " označavaju mogućnost korisnika da utiče na bezbednosne parametre komunikacije, da razume arhitekturu mreže i da upravlja sopstvenim nivoom privatnosti i anonimnosti. Kod VPN-a, ta autonomija je ograničena poverenjem u provajdera, dok Tor omogućava veću tehničku nezavisnost.*

Izvor: Autor

3.6 Strategije u MITM napadima: napadači vs. žrtve

U okviru MITM napada, strategije nisu rezervisane samo za branioca — i napadači razvijaju sofisticirane pristupe za izbegavanje detekcije i povećanje efikasnosti. Razumevanje napada kod obe strane omogućava preciznije definisanje bezbednosnih zahteva i efikasniju odbranu.

3.6.1 Strategije samoočuvanja napadača

Napadači obično preduzimaju niz mera kako bi minimizovali mogućnost otkrivanja:

- Operišu daljinski, često menjajući fizičke lokacije.
- Koriste javno dostupne ili jednokratne uređaje.
- Finansijske transakcije obavljaju gotovinom ili putem prepaid instrumenata, čime smanjuju tragove.
- Primenjuju anonimizacione alate (VPN, Tor) i automatizovane skripte koje otežavaju atribuciju.

3.6.2 Strategije odbrane žrtava

Potpuna eliminacija MITM napada je izazovna, ali se rizik može značajno smanjiti primenom sledećih mera:

- Projektovanje mrežnih arhitektura sa bezbednošću kao temeljnim principom
- Implementacija sigurnosno-orijentisanih mrežnih topologija
- Redovno ažuriranje operativnih sistema i softvera
- Korišćenje firewall-a i snažne enkripcije (npr. SSL/TLS sertifikata)
- Implementacija statičkih ARP unosa radi sprečavanja ARP trovanja
- Izbegavanje povezivanja na nesigurne Wi-Fi mreže i korišćenje alata kao što je *HTTPS Everywhere*
- Primena DNSSEC i sistema za detekciju upada radi ublažavanja DNS spoofing napada
- Podizanje digitalne pismenosti i razvoj bezbednosne kulture među korisnicima

Organizacije, posebno manje sa ograničenim resursima, često moraju da revidiraju

bezbednosne prakse ili da angažuju eksternu zaštitu. Ključni izazovi ostaju svest o pretnjama i pravovremeno otkrivanje napad.

Upotreba kriptografije sa javnim ključem (PKC) i digitalnih sertifikata koje izdaju pouzdani sertifikacioni autoriteti (CA) od suštinskog je značaja za pouzdanu identifikaciju uređaja i bezbednu komunikaciju. Međutim, kompromitacija *root* ključeva (tzv. ključeva poverenja na najvišem nivou) može ugroziti celokupan sistem, što naglašava značaj koncepta '*korena poverenja*'[7] u okviru modula za pouzdano računanje. Iako kriptografske metode pružaju osnovnu zaštitu, njihova efikasnost se značajno povećava kada se kombinuju sa pravilno konfigurisanim firewall sistemima, što će biti detaljnije razmotreno u narednoj sekciji.

Korisnicima se savetuje da onemoguće automatsko povezivanje na mreže, da ne otvaraju sumnjive linkove i priloge, kao i da izbegavaju „*jailbreak*“ ili „*root*“ modifikacije uređaja, kako bi se smanjio rizik od MITM napada.

S obzirom na sve veću povezanost uređaja i kompleksnost mrežnih okruženja, MITM napadi ne predstavljaju samo tehnički izazov, već i ozbiljan bezbednosni i ekonomski rizik, naročito u kontekstu digitalne transformacije poslovanja.

Zbog svoje učestalosti i sposobnosti da kompromituju kritične komunikacione tokove, MITM napadi zauzimaju zavidno mesto među sajber pretnjama. Sledeća podsekcija prikazuje njihove finansijske posledice kroz statističke pokazatelje u poslednjih pet godina.

3.7 Procena ekonomskih posledica MITM napada

MITM napadi predstavljaju tehnički sofisticiran oblik sajber pretnji, sa sposobnošću da neprimetno presreću komunikaciju, kradu akreditive i manipulišu sesijama i transakcijama. Njihova destruktivnost se ne ogleda samo u direktnoj šteti, već i u sistemskom narušavanju poverenja u digitalne infrastrukture.

U okviru ukupnog spektra sajber napada, MITM zauzima zapaženo mesto — kako po učestalosti, tako i po ekonomskom uticaju. Prema dostupnim podacima, MITM čini oko 19% uspešnih online napada, sa procenjenim godišnjim troškom od 2,4 milijarde USD (Astra Security, 2023). U domenu Wi-Fi eksploatacije, MITM tehnike učestvuju sa čak 35%, što ih svrstava među najzastupljenije vektore napada u bežičnom okruženju. Dodatno, 50% MITM incidenata rezultira krađom korisničkih kredencijala, a mesečno se kompromituje preko milion lozinki — što ukazuje na ozbiljan rizik za identitete korisnika i sigurnost poslovnih sistema.

Proizvodna preduzeća su najranjivija, zbog široke upotrebe IoT uređaja, automatizovanih sistema i često nedovoljno zaštićenih mrežnih konfiguracija. MITM napadi se sve češće kombinuju sa automatizacijom i veštačkom inteligencijom, čime se povećava njihova efikasnost i smanjuje potreba za direktnim angažovanjem napadača.

Radi sveobuhvatnijeg uvida, u nastavku je prikazana Tabela 2 koja objedinjuje karakteristike MITM i drugih dominantnih sajber napada u periodu 2021–2025.

Tabela 2. Vrste sajber napada: karakteristike, učestalost i finansijski uticaj (2021–2025)

Vrsta napada	Tipični cilj	Učestalost (2021–2025)	Godišnji trošak	Dominantni vektor	Udeo u krađi podataka	Izvor(i)
MITM	Komunikacija, lozinke, sesije	Visoka (19% online napada)	2,4 milijarde USD	AI, phishing, Wi-Fi	50% MITM uključuje krađu kredencijala	(Wabuge, 2023)
Phishing	Korisnički podaci, kredencijali	Veoma visoka (3,4 milijarde phishing imejlova na dan)	3,1 milijarda USD (procena)	i-mejl, linkovi	41% incidenata započinje phishingom	(Palatty, 2025), (SSL Insights, 2025), (APWG, 2025)
Ransom-ware	Sistemi, baze podataka	Opala sa 66 % u 2023. na 59 % u 2024. godini, uz	20 milijardi USD u 2021. godini	Enkripcija, ucena	Srednji (60% uključuje	(Okoruwa & Chapman, 2025),

[7] „Koreni poverenja“ (engl. roots of trust) predstavljaju osnovne komponente hardverske ili softverske infrastrukture koje se smatraju inherentno pouzdanim. U kontekstu TPM-a (Trusted Platform Module), to su ključevi i mehanizmi koji inicijalizuju bezbednosne operacije, kao što su verifikacija firmware-a, enkripcija podataka i autentifikacija sistema.

Vrsta napada	Tipični cilj	Učestalost (2021–2025)	Godišnji trošak	Dominantni vektor	Udeo u krađi podataka	Izvor(i)
		ponovni rast krajem 2024. godine	57 milijardi USD u 2025. godini (3,9 miliona USD u proseku po incidentu)		gubitak podataka)	(Morgan, 2025) (Threat Hunter Team, 2025)
DDoS	Dostupnost servisa	Srednja, ali ubrzano rastuća. 4 puta više napada u Q4 2022 u odnosu na Q4 2021	1,6 milijardi USD	Botneti	Nizak	(StormWall, 2025), (Smith, 2025)
Supply-chain	Softverski lanci, update sistemi	Rastuća (431% rast)	Teško procenljivo	Kompromito-vani update	Varijabilan	(Morgan, 2023), (Snape, 2025)
SQL Injection	Baze podataka	Srednja	Lokalizovana šteta	Automatizovani kod	Nizak	(Jackson, 2024), (Citakovic, 2023)

Izvor: Autor

Podaci ukazuju da MITM napadi, iako često zanemareni u javnim diskusijama, imaju visok strateški značaj. Njihova sposobnost da se integrišu sa drugim vektorima (npr. phishing) i da ciljaju komunikacione tokove čini ih posebno opasnim u kontekstu digitalne transformacije **i** industrijske automatizacije.

U poređenju sa ransomware napadima koji generišu direktnu finansijsku štetu, MITM napadi deluju tiše, ali sistemski — narušavajući autentifikaciju**,** integritet podataka i poverenje korisnika. Zbog toga je neophodno razviti slojevite strategije zaštite, uključujući end-to-end (E2E)[8] enkripciju**,** segmentaciju mreže**,** detekciju anomalija i edukaciju korisnika.

4 FIREWALL

Implementacija robusnih mera mrežne bezbednosti predstavlja osnovu zaštite od MITM napada, pri čemu mrežni zaštitni zid (u daljem tekstu firewall) ima ulogu prve linije odbrane između korisničke mreže i spoljnih pretnji. Da bi se sagledala njegova funkcionalna vrednost u kontekstu MITM scenarija, neophodno je prethodno razmotriti tehnike napada, analizirati osnovne i napredne sposobnosti savremenih firewall rešenja, te kroz studije slučaja demonstrirati primenu preporučenih bezbednosnih mera.

Firewall-i zasnovani na klasičnoj filtraciji portova, IP adresa i protokola na nivou paketa često nisu efikasni u otkrivanju kompromitovanih sesija kada napadač koristi dozvoljene i enkriptovane komunikacione kanale. Standardni L3/L4[9] firewall bez uključene TLS inspekcije vidi samo metapodatke (IP/port/SNI[10]), ali ne i validnost sertifikata; validaciju radi klijent u okviru aplikacije ili operativnog sistema. Za više detalja pogledajte 4.2.2.

Pravilno konfigurisan firewall ne predstavlja samo nominalnu bezbednosnu meru, već ključnu razliku između formalne zaštite i stvarne otpornosti sistema. U nastavku se razmatraju konkretne konfiguracione strategije koje omogućavaju identifikaciju i blokiranje sumnjivih aktivnosti karakterističnih za MITM napade. Pravilna konfiguracija obuhvata sledeće korake:

1. Definisanje pravila pristupa (Access Control Lists – ACLs)
   - Precizno određuje ko može da pristupi kojim resursima, kada i kako.
   - Blokira sve što nije eksplicitno dozvoljeno — tzv. default-deny pristup.
2. Praćenje stanja konekcije (Stateful Inspection)

[8] Skraćenica E2E označava End-to-End, odnosno od-kraja-do-kraja komunikaciju ili zaštitu.
[9] L3 i L4 označavaju mrežni i transportni sloj OSI modela, respektivno, i često su osnova za filtriranje saobraćaja u standardnim firewall-ima.
[10] SNI označava Server Name Indication — ekstenziju TLS protokola koja omogućava klijentu da u toku TLS handshaka serveru saopšti ime domena kojem želi da pristupi

- Firewall ne analizira pakete izolovano, već prati celokupnu sesiju.
- Prepoznaje neautorizovane pokušaje ubacivanja paketa u aktivnu sesiju — što je tipično za MITM.

3. Filtriranje po aplikacionom sloju (Layer 7 filtering)
   - Omogućava dubinsku inspekciju HTTP, DNS, FTP i drugih protokola.
   - Blokira modifikovane zahteve, neautentične odgovore i neobične obrasce ponašanja.
4. Zaštita od spoofinga i ARP manipulacije
   - Sprečava lažno predstavljanje IP adresa i manipulaciju ARP tabelama — česte MITM vektore.
   - Uključuje *anti-spoofing* pravila i ARP monitoring.
5. Logovanje i alarmiranje
   - Pravilno konfigurisan firewall beleži pokušaje pristupa, neuspele konekcije, i sumnjive obrasce.
   - Može da šalje real-time alarme administratoru ili SIEM[11] sistemu.
6. Redovno ažuriranje pravila i firmware-a
   - Pravila se prilagođavaju novim pretnjama, a firewall softver se ažurira radi zaštite od poznatih ranjivosti.

4.1 Funkcionisanje firewall-a

Pre nego što se pristupi analizi funkcije firewall-a, važno je razumeti da port, u kontekstu mreže, predstavlja logički identifikator koji omogućava da više aplikacija na istom računaru istovremeno komunicira sa mrežom. Port nije fizički ulaz, već softverski kanal koji operativni sistem koristi za usmeravanje dolaznih podataka ka odgovarajućoj aplikaciji. Aplikacija koristi sistemske resurse — procesor, memoriju i druge komponente — da obradi primljene podatke.

Postupak obrade izgleda ovako:

- Mrežni paket stiže do mrežnog interfejsa (npr. Ethernet kartice).
- Paket se prosleđuje TCP/IP steku operativnog sistema.
- Operativni sistem koristi transportni sloj da identifikuje odredišni port i prosledi podatke aplikaciji registrovanoj za taj port.
- Aplikacija obrađuje podatke i, po potrebi, koristi procesor za izvršavanje zadataka.

Da bi mogla da prima podatke, aplikacija mora biti pokrenuta, konfigurisana za mrežnu komunikaciju i autorizovana od strane operativnog sistema. U tom procesu, firewall može blokirati ili dozvoliti pristup portu u skladu sa bezbednosnim pravilima. Aplikacija se registruje na određeni port i počinje da prihvata dolazne konekcije.

Neke karakteristične situacije prikazane su u Tabeli 3.

Tabela 3. Neki primeri pristupa portovima

Aplikacija	Port koji obično koristi	Da li stalno sluša?
Web server (npr. Apache)	80 (HTTP), 443 (HTTPS)	Da, ako je pokrenut
I-mejl server (npr. Postfix)	25 (SMTP)	Da, ako je aktivan
Web browser (npr. Chrome)	Dinamički portovi	Ne sluša — on inicira konekcije
Torrent klijent	6881–6889 (nekada); dinamički portovi (sada)	Da, ako je pokrenut

Izvor: Autor

Tabela 4. Podela portova

Tip portova	Opseg	Namena
Dobro poznati portovi	0–1023	Standardne usluge (HTTP, HTTPS, FTP, SSH, DNS...)
Registrovani portovi	1024–49151	Aplikacije koje nisu deo OS-a, ali su poznate
Dinamički/privatni	49152–65535	Privremeni portovi za klijentske konekcije (ephemeral)

Izvor: Autor

[11] SIEM (Security Information and Event Management) sistem je centralizovana platforma za upravljanje bezbednosnim informacijama i događajima u IT okruženju. Njegova osnovna funkcija je da prikuplja, analizira i korelira podatke iz različitih izvora — kao što su mrežni uređaji, serveri, aplikacije i korisnički nalozi — kako bi se pravovremeno otkrile pretnje, anomalije i bezbednosni incidenti.

TCP/IP podržava ukupno 65536 portova koji su podeljeni u tri grupe (v. tabelu 4).

Međutim, u praksi se koristi relativno mali broj portova.

- Serveri koriste poznate portove za usluge: 80 (HTTP), 443 (HTTPS), 21 (FTP), 22 (SSH), 25 (SMTP), 53 (DNS), itd. (v. tabelu 4)
- Klijenti koriste dinamičke portove za uspostavljanje konekcije. Npr. kada klijent otvori sajt, njegov računar koristi neki port iz opsega 49152–65535 da komunicira sa serverom na portu 443.

U proseku, aktivno se koristi manje od 100 portova na većini sistema — ostali su zatvoreni ili neaktivni.

U bezbednosnim praksama se preporučuje:

- Zatvoriti sve nepoznate portove
- Logovati pokušaje pristupa
- Koristiti intrusion detection sistem (IDS[12]) da prati neobične aktivnost

Može se postaviti pitanje: *šta se dešava kada paket stigne na neki drugi port, npr. 54321?*

Port *54321* pripada IANA opsegu za dinamičke i privatne portove i nije standardizovan za neku poznatu uslugu (npr. 80 za HTTP ili 443 za HTTPS). U praksi se može koristiti za prilagođene aplikacije, zlonamerni softver (npr. backdoor kanali) ili eksperimentalne servise.

Mogući ishodi pri pristupu portu *54321*:

1. Port nije otvoren (nije dozvoljen u firewall pravilima):
   - Firewall automatski *odbacuje paket* (*drop*) ili *odgovara ICMP[13] porukom* da je port nedostupan (*reject*).
   - Paket ne stiže do operativnog sistema — firewall je presekao pokušaj.
2. Port je otvoren, ali nijedna aplikacija ne „sluša“:
   - Operativni sistem može da *ignorše zahtev* ili *vrati grešku* (npr. TCP RST).
   - Ako je firewall pasivan, napadač može da zaključi da je port otvoren — što je *potencijalni bezbednosni rizik*.
3. Port je otvoren i aplikacija aktivna, ali nije zaštićena:
   - Napadač može da pokuša *eksploataciju ranjivosti* aplikacije.
   - Ako firewall ne filtrira sadržaj, može doći do *buffer overflow, remote code execution*, ili čak *MITM napada* ako aplikacija koristi nesigurnu autentifikaciju.

Firewall (ili njegova OS-integrisana komponenta) predstavlja prvi sloj zaštite. Nakon njega nastupa operativni sistem, koji vodi internu tabelu aktivnih portova i aplikacija koje su ih rezervisale. Kada stigne mrežni paket:

1. OS analizira port broj u paketu.
2. Proverava da li neka aplikacija „sluša“ na tom portu.
3. Ako postoji aktivna aplikacija — prosleđuje podatke.
4. Ako ne — odbacuje paket ili pošalje poruku da port nije dostupan.

Pravilno konfigurisan firewall može da:

- Blokira paket pre nego što stigne do OS-a (*drop*)
- Ignoriše paket bez ikakvog odgovora
- Odbije paket uz ICMP poruku (*reject*).

Primer iz prakse

Grafikon na slici 2 prikazuje algoritam odlučivanja o mrežnom paketu prispelom na port, npr. 54321, uz interakciju firewall-a i operativnog sistema (OS).

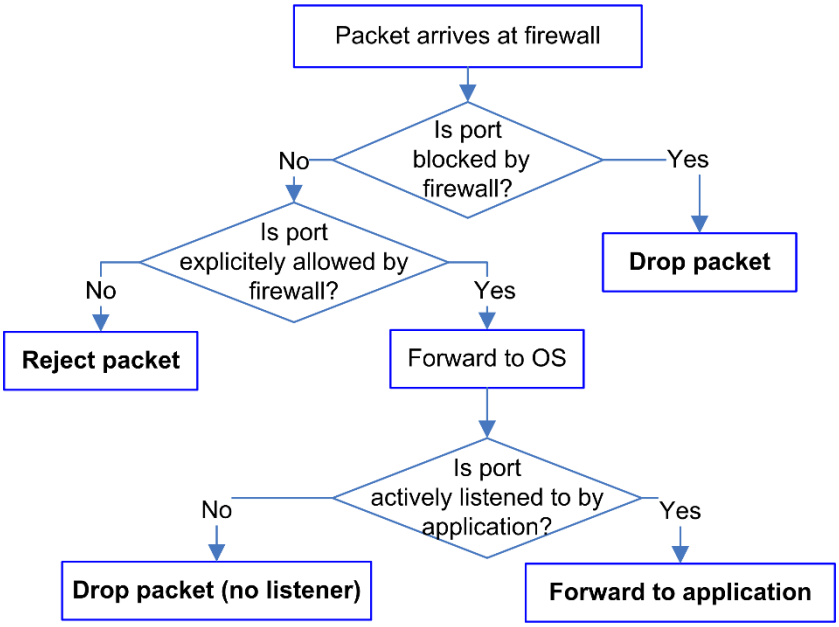
U vezi sa firewall-om, dve su opcije moguće:

- Ako je port otvoren na firewallu, ali nijedna aplikacija ne sluša:
  - Firewall dozvoljava paket.
  - OS ga odbacuje jer nema aplikacije na tom portu.
  - OS može poslati ICMP poruku „port unreachable“ (UDP) ili TCP segment sa RST zastavicom (TCP)
- Ako je port blokiran na firewallu:
  - Paket ne stiže do OS-a.
  - Firewall ga može tiho odbaciti (*drop*) ili eksplicitno odgovoriti (*reject*).

Odluka zavisi od konfiguracije oba sloja — firewall je prvi čuvar, OS je drugi.

[12] IDS (Intrusion Detection System) i IPS (Intrusion Prevention System) su bezbednosni sistemi dizajnirani za identifikaciju, analizu i reagovanje na sumnjive aktivnosti u mrežnom saobraćaju.

[13] ICMP poruka (Internet Control Message Protocol) označava kontrolnu mrežnu poruku koja se koristi za signalizaciju problema u komunikaciji između uređaja na IP mreži.



Slika 2 Obrada mrežnih paketa

Izvor: Autor

Grafikon vizuelizuje tok obrade paketa kroz sledeće faze odlučivanja:

- Firewall odluke: *dozvoli, blokiraj* ili *odbij*
- OS odluke: zavise od toga da li aplikacija sluša na ciljanom portu
- Rezultat: *odbaci (drop), odbij (reject)* ili *prosledi aplikaciji (forward to application).*

Poređenje ponašanja TCP i UDP protokola u odnosu na primljeni paket prikazano je Tabelom 5.

Tabela 5. Uporedna analiza TCP vs UDP

Osobina	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Tip protokola	Povezan (connection-oriented)	Nepovezan (connectionless)
Pouzdanost	Visoka — potvrda prijema, retransmisija	Niska — bez potvrde
Kontrola toka i grešaka	Da	Ne
Kada niko ne sluša port	OS šalje TCP RST (reset)	OS šalje ICMP Port Unreachable
Firewall ponašanje (*drop*)	Paket se tiho odbacuje, bez odgovora	Isto — tiho odbacivanje
Firewall ponašanje (*reject*)	Može poslati TCP RST	Može poslati ICMP poruku
Tip aplikacija	Web serveri, i-mejl, SSH, FTP	DNS, VoIP, video streaming
Brzina	Sporiji zbog kontrole	Brži, ali manje pouzdan
Ranjivost na MITM	Veća ako se koristi bez enkripcije	Veća zbog nedostatka kontrole

Izvor: Autor

U slučaju da napadač pokuša da ispita dostupnost portova, ponašanje sistema zavisi od korišćenog protokola:

- TCP: Ako se pokušaj konekcije izvrši ka portu 22 (SSH), a nijedna aplikacija ne sluša, operativni sistem šalje TCP RST — što napadaču može signalizirati da port postoji, ali nije aktivan.
- UDP: Ako se pošalje paket ka portu 53 (DNS), a nema aktivne aplikacije, OS može poslati ICMP Port Unreachable — ukoliko firewall to dozvoljava.

Ovakvi odgovori mogu imati bezbednosne implikacije. TCP RST i ICMP poruke omogućavaju napadaču da mapira mrežu pomoću alata kao što je *nmap*. Zbog toga se često primenjuje firewall

drop politika — tiho odbacivanje paketa bez odgovora, čime se smanjuje mogućnost otkrivanja mrežnih servisa.

U zavisnosti od zahteva i bezbednosne politike administratorskog tima, na raspolaganju su dve osnovne strategije za upravljanje ponašanjem portova kada nijedna aplikacija ne sluša: tiho odbacivanje (*drop*) i aktivno odbijanje (*reject*). Ove opcije prikazane su u Tabeli 6.

Tabela 6. Definisanje `iptables` pravila za Linux firewall — simulacija TCP/UDP ponašanja kada niko ne sluša

Politika	Kod – Linux
DROP (tiho odbacivanje)	*# TCP paketi ka portu 22 (SSH) se tiho odbacuju* `iptables -A INPUT -p tcp --dport 22 -j DROP`
	# UDP paketi ka portu 53 (DNS) se tiho odbacuju `iptables -A INPUT -p udp --dport 53 -j DROP`
REJECT (aktivno odbijanje)	*# TCP paketi ka portu 22 se odbijaju sa TCP RST* `iptables -A INPUT -p tcp --dport 22 -j REJECT --reject-with tcp-reset`
	# UDP paketi ka portu 53 se odbijaju sa ICMP Port Unreachable `iptables -A INPUT -p udp --dport 53 -j REJECT --reject-with icmp-port-unreachable`

Izvor: Autor

Navedene komande se direktno unose u *iptables* — interfejs koji upravlja *netfilter* mehanizmom unutar Linux kernela. Svaka komanda:

- dodaje pravilo u *INPUT lanac* (dolazni saobraćaj),
- definiše ponašanje prema određenom portu i protokolu (TCP/UDP),
- odmah stupa na snagu i utiče na mrežni saobraćaj

Ukoliko se pravila ne sačuvaju, ona se gube nakon restartovanja sistema. Trenutna konfiguracija može se proveriti komandom:

```
iptables -L -n --line-numbers
```

Za trajno čuvanje pravila preporučuje se instalacija paketa:

```
sudo apt install iptables-persistent
```

Pravila se tada automatski smeštaju u:

`/etc/iptables/rules.v4` (za IPv4)
`/etc/iptables/rules.v6` (za IPv6)

Radi unapređenja bezbednosti, preporučuje se postavljanje default politike na DROP, čime se sav dolazni i prosleđeni saobraćaj odbacuje osim eksplicitno dozvoljenog:

- `iptables -P INPUT DROP`
- `iptables -P FORWARD DROP`
- `iptables -P OUTPUT ACCEPT`
  (ili `DROP`, u zavisnosti od potrebe),

Zatim se dodaju pravila za dozvoljene servise, npr. SSH (port 22) i HTTP (port 80):

- `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
- `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

Dodatno, preporučuje se dozvola za loopback interfejs i već uspostavljene konekcije:

- `iptables -A INPUT -i lo -j ACCEPT`
- `iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`

Ako se koristi direktno, `iptables` ne čuva pravila automatski. Potrebno ih je ručno sačuvati:

```
iptables-save > /etc/iptables/rules.v4
```

(Debian/Ubuntu)

Za upravljanje pravilima nakon restartovanja, moguće je koristiti *iptables-persistent* (Debian/Ubuntu) ili *firewalld* (npr. Fedora, CentOS), u zavisnosti od distribucije.

4.1.1 Napomena o `nftables` u savremenim distribucijama:

Iako se u ovom tekstu koristi *iptables* za ilustraciju pravila, moderne Linux distribucije (npr. Fedora, Debian, Ubuntu 22.04+) podrazumevano koriste *nftables* kao *backend*. U mnogim slučajevima, *iptables* komande se zapravo prevode u *nftables* pravila zahvaljujući sloju za kompatibilnost.

Kao primer može da posluži *iptables* blokiranje pristupa na portu 22 (Nickfetrat, 2024):

```
iptables -A INPUT -p tcp --dport 22 -j DROP
```

nftables ekvivalent bi bio:

```
nft add rule inet filter input tcp dport 22 drop
```

Ovaj *nftables* primer koristi objedinjenu tabelu *inet*. Korišćenjem *inet* tabele, pravila se automatski primenjuju na oba protokola — IPv4 i IPv6 — bez potrebe za dupliranjem.

Za trajno čuvanje pravila koristi se:

```
nft list ruleset > /etc/nftables.conf
sudo systemctl enable nftables
```

Na sistemima gde je *iptables* aktivan, moguće je koristiti oba interfejsa paralelno. Preporučuje se prelazak na *nftables* zbog bolje fleksibilnosti i performansi.

Bez obzira na to da li se koristi *iptables* ili *nftables*, pravilna konfiguracija firewall-a predstavlja ključnu komponentu mrežne bezbednosti. Kombinovanjem lokalnih i mrežnih pravila, administrator može precizno kontrolisati pristup aplikacija, minimizirati rizike i obezbediti stabilan rad sistema.

4.1.2 Napomena o ponašanju aplikacija pri instalaciji softvera

Pri instalaciji novog softvera, aplikacija obično zahteva dozvolu za pristup mreži. Operativni sistem tada proverava da li je aktivan lokalni firewall. Ukoliko jeste, korisniku se prikazuje dijalog sa pitanjem: „*Dozvoliti aplikaciji da pristupi mreži?*“

Ako korisnik da saglasnost, operativni sistem automatski dodaje odgovarajuće pravilo u lokalni firewall, čime se aplikaciji omogućava korišćenje mrežnih resursa. Lokalni firewall (npr. Windows Firewall ili *iptables*) reguliše pristup aplikacije ka određenim portovima, dok mrežni firewall (npr. na ruteru ili gateway-u) može dodatno filtrirati saobraćaj ka spoljnim serverima.

Na primer, aplikacije poput WhatsApp i Viber koriste dinamičke portove za izlazne konekcije (npr. opseg 50.000–60.000), ali se povezuju na unapred definisane servere. Važno je naglasiti da aplikacija ne „probija“ firewall, već koristi sistemske API-je da zatraži mrežni pristup. Ukoliko firewall ne dozvoli konekciju — aplikacija neće moći da se poveže.

4.2 Kako firewall utiče na MITM napade?

MITM napadi često počinju iskorišćavanjem ranjivosti na aplikacionom sloju, pri čemu napadač pristupa portu koji koristi ranjiva aplikacija. Ukoliko zaštita nije adekvatna, može da:

- Pokrene zlonamerni kod
- Preuzme kontrolu nad aplikacijom i/ili
- Indirektno pristupi procesoru i sistemskim resursima

Firewall ima ključnu ulogu u sprečavanju ovakvih scenarija. Kroz pravilno definisanu politiku pristupa, inspekciju aplikacionih protokola i integraciju sa sistemima za detekciju pretnji, firewall može da identifikuje pokušaje neautorizovanog pristupa i blokira ih pre nego što dođe do kompromitovanja sistema.

U nastavku se razmatra firewall kao prva linija odbrane u kontekstu MITM napada.

4.2.1 Firewall u odbrani od MITM napada

Firewall može značajno doprineti sprečavanju MITM napada ukoliko je pravilno konfigurisan, pri čemu njegova efikasnost zavisi od pravca saobraćaja i tačke potencijalne kompromitacije. U kontekstu MITM zaštite, razlikuju se sledeće kategorije:

- *Inbound MITM*: Ovaj tip napada podrazumeva pokušaj neautorizovanog pristupa korisnikovoj mreži spolja, najčešće putem otvorenih portova ili ranjivih servisa. Firewall, uz adekvatno definisana pravila za ulazni saobraćaj i aktivnu inspekciju paketa, može da efikasno blokira takve konekcije.
  Firewall sa podrškom za *stateful* inspekciju ne analizira samo pojedinačne pakete, već prati celokupno stanje sesije — uključujući IP adrese, portove, protokole i tokove komunikacije. Time se omogućava dinamičko odlučivanje o legitimnosti saobraćaja, pri čemu firewall može efikasno blokirati neautorizovane pokušaje pristupa koji ne pripadaju postojećim sesijama, uključujući lažno predstavljene pakete i pokušaje neovlašćenog ubacivanja u tok komunikacije radi njenog preusmeravanja ili manipulacije.

- *Outbound MITM*: U ovom scenariju, aplikacija na korisnikovom uređaju pokušava da uspostavi vezu sa kompromitovanim eksternim serverom. Firewall sa podrškom za DNS filtering, reputacione liste i TLS inspekciju može da identifikuje i blokira sumnjive IP adrese, domene ili nevažeće sertifikate, čime se sprečava uspostavljanje štetne komunikacije.
  U kontekstu *Outbound MITM* zaštite, stateful inspekcija omogućava firewallu da prati tok izlazne sesije i identifikuje neuobičajene pokušaje uspostavljanja konekcije sa kompromitovanim serverima. U kombinaciji sa TLS inspekcijom, reputacionim listama i DNS filtriranjem, ova funkcionalnost značajno povećava šanse za pravovremeno otkrivanje i blokiranje štetnih konekcija.

Firewall ne može da detektuje kompromitaciju unutar šifrovanih sesija, jer se saobraćaj posmatra kao legitimna konekcija. Ako se koristi HTTPS, napadač mora da koristi lažni sertifikat — što ga primorava na tehnike poput SSL strippinga ili falsifikovanja sertifikata (certificate spoofing). Zbog ovih ograničenja, firewall se često kombinuje sa naprednim sistemima za detekciju i prevenciju pretnji (IDS/IPS), što je tema naredne sekcije.

4.2.2 Firewall + IDS/IPS = bolja zaštita

Firewall funkcioniše kao statistički filter — fokusiran na pravila saobraćaja, ali bez uvida u sadržaj paketa. Međutim, kada se kombinuje sa sistemima za detekciju i prevenciju upada (IDS/IPS), moguće je detektovati anomalije u mrežnom saobraćaju, uključujući:

- Promene u TLS handshaku
- Neobične DNS zahteve
- ARP spoofing pokušaje

Tabelom 7 je prikazana veza između firewall-a i MITM.

Tabela 7. Veza između firewall-a i MITM

Element	Uloga u MITM zaštiti
Firewall	Blokira neautorizovane konekcije, ali ne vidi šifrovani MITM
IDS/IPS	Analizira saobraćaj, detektuje anomalije
TLS/SSL	Sprečava MITM ako se sertifikati validiraju
Korisnik	Ako ignoriše upozorenje o sertifikatu — MITM uspeva

Izvor: Autor

Kombinovanjem firewall-a sa IDS/IPS sistemima, organizacije postižu slojevitu analizu saobraćaja i proaktivnu zaštitu od MITM napada, čime se značajno smanjuje rizik od kompromitacije čak i u šifrovanim komunikacionim kanalima.

5 MITM SCENARIJI

5.1 Noviji primeri MITM napada

U radu Cekerevac et al. (2025) prikazan je niz MITM napada koji su se odigrali između 2007. i 2023. godine, te ih ovde nećemo detaljno analizirati. Fokusiraćemo se na napade koji su se dogodili od kraja 2023. godine, uz napomenu da se precizan procenat MITM incidenata razlikuje u zavisnosti od izvora. Arad (2024) navodi da su MITM napadi tokom 2024. godine činili 23% sajber incidenata povezanih sa identitetom. Prema Microsoft Digital Defense Report-u za 2024. godinu (2024, p. 39) intenzitet password-based napada dostigao je nivo od 7.000 pokušaja u sekundi.

5.1.1 Napad grupe Salt Typhoon na američke telekomunikacione kompanije

U 2024. godini, hakerska grupa Salt Typhoon, povezana sa Kinom (Krouse, McMillan, & Volz, 2024), izvela je sofisticiran MITM napad na američke telekomunikacione kompanije, uključujući AT&T, Verizon, Lumen Technologies i T-Mobile. (Kapko, 2025; Lyons, 2024; Israel & Young, 2025)

Sofisticirani MITM napad izveden je neprimetno, omogućivši neovlašćen pristup metapodacima komunikacija — brojevima telefona, IP adresama i vremenskim oznakama (ne nužno sadržaj razgovora/poruka) — čime su kompromitovane privatne informacije korisnika, uključujući vladine službenike i političke kampanje.

Američka vlada je formirala radnu grupu za odgovor na incident, dok su pogođene kompanije pojačale saradnju sa bezbednosnim agencijama radi jačanja zaštite infrastrukture. (Jaikaran, 2025)

5.1.2 Cozy Bear napad na TeamViewer SE

U junu 2024. godine, nemačka kompanija TeamViewer SE, poznata po svom softveru za daljinsko praćenje i upravljanje (RMM) koji omogućava dobavljačima upravljanih usluga (MSP) i IT odeljenjima da upravljaju serverima, radnim stanicama, mrežnim uređajima i krajnjim tačkama, prijavila je proboj svoje korporativne mreže od strane ruske hakerske grupe Cozy Bear. Pristup je ostvaren putem legitimnih naloga. Nije precizirano kako su napadači došli do pristupnih podataka.

TeamViewer je naglasio da su korporativni IT sistemi strogo odvojeni od produkcionog okruženja softvera za daljinski pristup, čime je sprečeno širenje napada na korisničke podatke (Langley, 2024).

Iako proizvod za daljinski pristup nije bio kompromitovan, hakeri su pristupili osetljivim internim komunikacijama. Incident je dodatno osvetlio ranjivosti korporativnih IT sistema i rizike koje predstavljaju napredne uporne pretnje (APT) poput grupe Cozy Bear. (Lakshmanan, 2024; Poireault, 2023)

5.1.3 Terrapin napad na SSH protokol

U decembru 2023. godine, istraživači sa Ruhr University Bochum otkrili su ranjivost u SSH protokolu poznatu kao Terrapin Attack (CVE-2023-48795). Ova ranjivost omogućava MITM napadaču da manipuliše početnim porukama u SSH sesiji putem tehnike poznate kao prefix truncation. Time se manipuliše procesom pregovaranja sigurnosnih ekstenzija, što rezultira smanjenjem nivoa zaštite bez vidljivih indikatora za klijenta ili server.

Terrapin napad posebno cilja algoritme kao što su ChaCha20-Poly1305 i CBC šifre sa Encrypt-then-MAC, omogućavajući napadaču da deaktivira zaštitu od napada na vremensko razdvajanje pritisaka tastera (*keystroke timing*). Prema procenama iz nezvaničnih izvora, skoro 11 miliona javno dostupnih SSH servera bilo je izloženo riziku (Toulas, 2024; Popovici, 2024).

Ublažavanje ove ranjivosti zahteva istovremeno ažuriranje i klijentske i serverske strane, jer jednostrana zakrpa nije dovoljna. Programeri su uveli opciju Strict Key Exchange, koja resetuje brojače sekvenci i sprečava ubacivanje paketa tokom nešifrovanog dela handshakinga. Pored toga, objavljen je alat za skeniranje ranjivih hostova, dostupan na GitHub-u. (Mizrahi & Zohar, 2023; Ojha, 2023)

5.1.4 Iranski hakeri i predsednička kampanja u SAD

U avgustu 2024. godine, iranski hakeri povezani sa obaveštajnom jedinicom Islamske revolucionarne garde (IRGC) izveli su spear-phishing napad na predsedničku kampanju bivšeg predsednika Donalda Trampa. Napad je rezultirao kompromitovanjem naloga jednog visokorangiranog zvaničnika kampanje, što je omogućilo MITM presretanje komunikacija i krađu osetljivih dokumenata. Dokumenti su kasnije prosleđeni medijima putem anonimnog naloga, uključujući istraživački dosije o potpredsedničkom kandidatu JD Vanceu. (Sharma, 2024)

Prema izveštaju kompanije Microsoft, iranski akteri su koristili lažne prosleđene poruke sa linkovima koji vode kroz domen pod kontrolom napadača, čime su preusmeravali saobraćaj i sticali pristup poverljivim podacima (Sharma, 2024). FBI, CISA i ODNI su potvrdili da je Iran odgovoran za pokušaje kompromitovanja kampanja oba glavna kandidata — Trampa i Bajden-Haris tima. (Kochi, 2024)

Napad je izazvao zabrinutost zbog stranog mešanja u američke izbore, a kampanja je pojačala sajber bezbednosne protokole i započela saradnju sa federalnim organima na istrazi. Incident je istakao potrebu za jačom digitalnom zaštitom u političkim kampanjama. (Aijaz, 2025)

5.1.5 Ranjivost u OpenSSH klijentu omogućava MITM napade

U februaru 2025. godine, istraživači iz Qualys Threat Research Unit (2025) otkrili su ranjivost u OpenSSH klijentu (CVE-2025-26465) koja omogućava MITM napad kada je aktivirana opcija `VerifyHostKeyDNS` jer se greškom u kodu ne tretiraju svi povratni kodovi iz funkcije za verifikaciju host ključa. Napadač može da se predstavi kao legitimni server, čime se narušava integritet SSH sesije i omogućava presretanje ili modifikacija komunikacije. Ranjivost je prisutna u verzijama od 6.8p1 do 9.9p1, a posebno je bila aktivna na sistemima poput FreeBSD-a, gde je opcija bila podrazumevano uključena od septembra 2013 do marta 2023.

Programeri OpenSSH-a su zakrpili ranjivost objavom verzije 9.9p2 istog dana, što je potvrđeno

i u NVD bazi podataka o CVE-2025-26465 (NIST, CVE-2025-26465 Detail, 2025). Međutim, ranjivost je otvorila pitanje sigurnosnih podrazumevanih vrednosti u popularnim klijentima. (Abbasi, 2025)

5.1.6 MITM napadi putem zlonamernih Wi-Fi mreža i DNS spoofinga

Tokom 2025. godine, zabeležen je porast MITM napada u javnim mrežnim okruženjima, posebno putem tzv. *evil twin* Wi-Fi mreža i DNS spoofinga. Napadači su postavljali lažne pristupne tačke koje imitiraju legitimne mreže u kafićima, hotelima i aerodromima, presrećući komunikaciju korisnika i kradući osetljive podatke poput lozinki i brojeva kreditnih kartica. Ovi napadi su se pokazali posebno efikasnim zbog slabih enkripcionih protokola i automatskog povezivanja uređaja na poznate SSID[14]-ove. Bezbednosni stručnjaci su upozorili na potrebu za edukacijom korisnika i širu primenu VPN[15] rešenja u javnim mrežama. (JumpCloud, 2025)

Tokom 2024. godine zabeležen je značajan porast incidenata koji funkcionalno pozicioniraju napadača između korisnika i ciljanog sistema — sa ciljem neovlašćenog pristupa, nadgledanja, modifikacije ili eksfiltracije poverljivih podataka.

U cilju ilustracije šireg spektra MITM scenarija, koji ne obuhvataju isključivo presretanje mrežnog saobraćaja, već i kompromitovane softverske komponente, proxy phishing tehnike i zloupotrebu sesijskih tokena, u nastavku su prikazane simulacije napada u kontrolisanom okruženju.

5.2 Upotreba ICMP protokola u inicijalizaciji MITM napada

ICMP (Internet Control Message Protocol) predstavlja ključni element u mrežnoj komunikaciji, prvenstveno namenjen signalizaciji grešaka i dijagnostici (Postel, 1981). Iako sam po sebi nije dizajniran za zlonamernu upotrebu, ICMP se može instrumentalizovati u pripremnoj fazi MITM napada, posebno u kombinaciji sa tehnikama kao što su ARP spoofing i manipulacija rutiranjem (MITRE ATT&CK, n.d.-a).

U kontekstu MITM scenarija, ICMP poruke se koriste za izazivanje legitimnih mrežnih reakcija koje napadaču omogućavaju da se pozicionira između dve komunikacione strane. Na primer, slanjem ICMP Echo Request poruke ka ciljanom uređaju, napadač može inicirati ARP zahtev, čime se otvara prostor za slanje lažnog ARP odgovora i preusmeravanje saobraćaja. Ova tehnika omogućava napadaču da neprimetno presretne, modifikuje ili prosledi mrežne pakete, bez izazivanja sumnje kod krajnjih korisnika (SANS Institute, 2020).

Dodatno, ICMP Redirect poruke, ukoliko nisu blokirane na nivou firewalla, mogu se zloupotrebiti za manipulaciju rutama, čime se saobraćaj usmerava ka kompromitovanim čvorovima. Iako savremeni operativni sistemi i mrežni uređaji često ignorišu ICMP Redirect poruke, njihova prisutnost u nezaštićenim ili loše konfigurisanim mrežama predstavlja značajan bezbednosni rizik (MITRE ATT&CK, n.d.-b).

Zloupotreba ICMP protokola u pripremi MITM napada naglašava potrebu za preciznim firewall pravilima koja kontrolišu ne samo TCP i UDP saobraćaj, već i ICMP poruke — posebno one koje mogu izazvati neželjene mrežne reakcije. U tom kontekstu, preporučuje se eksplicitno filtriranje ICMP Redirect poruka, kao i monitoring neobičnih ICMP obrazaca koji mogu ukazivati na pokušaj pozicioniranja MITM entiteta.

Na grafikonu na slici 3 se jasno uočavaju sledeće faze:

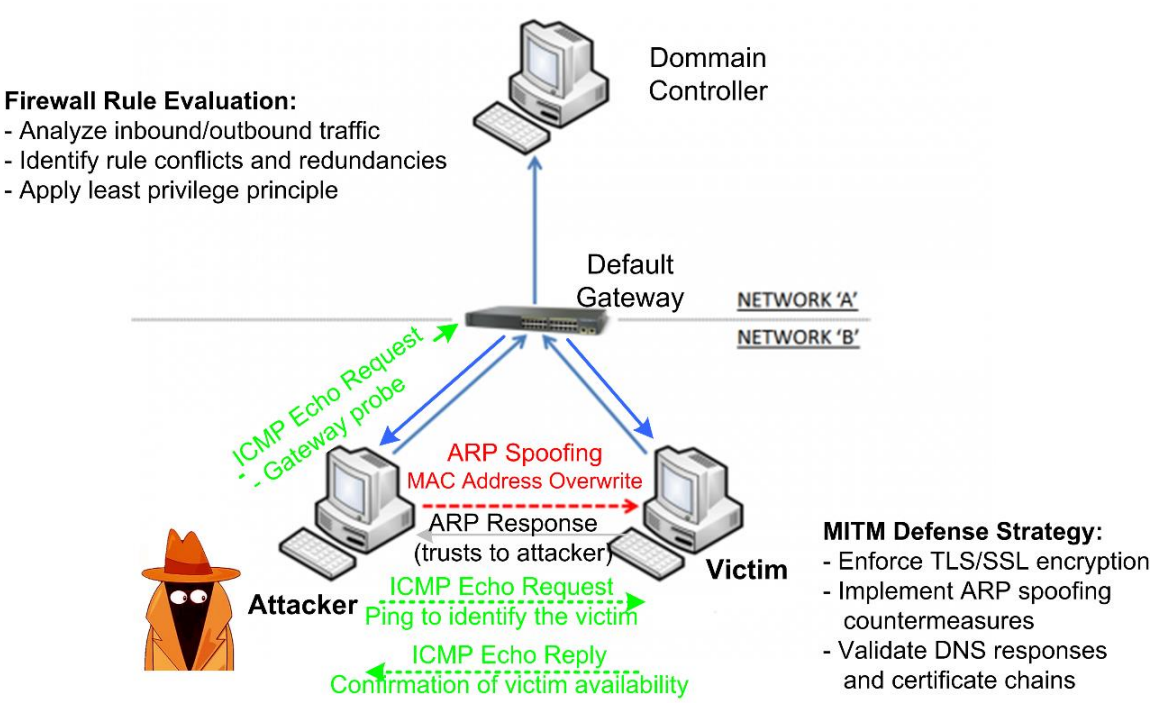
- *Faza 1 – ICMP Echo Request/Reply*: Prikazana strelicama između napadača i žrtve, inicira mrežnu aktivnost.
- *Faza 2 – ARP razmena*: ICMP komunikacija izaziva ARP zahtev od strane žrtve, što otvara prostor za manipulaciju.
- *Faza 3 – Lažni ARP odgovor*: Napadač šalje spoofovani ARP odgovor, čime se pozicionira između žrtve i gateway-a.
- *Faza 4 – MITM pozicioniranje*: Strelice sa dvostrukim pravcem prikazuju presretanje i prosleđivanje paketa.

[14] SSID je niz do 32 alfanumerička znaka koji identifikuje određenu Wi-Fi mrežu (Nicole, 2025).

[15] VPN (Virtualna privatna mreža) predstavlja tehnologiju koja omogućava bezbednu, šifrovanu komunikaciju između korisnika i udaljene mreže putem javnog interneta. Korišćenjem VPN-a, sav mrežni saobraćaj se odvija kroz zaštićeni kanal, čime se obezbeđuju poverljivost, integritet i anonimnost podataka. (Kaspersky, 2025)

- *Faza 5 – ICMP Redirect*: Prikazana kao dodatna strelica ka kompromitovanom čvoru, ukazuje na manipulaciju rutama. Manipulacija rutom putem ICMP Redirect poruke omogućava napadaču da trajno preusmeri saobraćaj kompromitovanog čvora, čime se uspostavlja stabilna MITM pozicija bez daljeg oslanjanja na ARP spoofing.

Grafikon toka na slici 3 prikazuje sekvencijalnu interakciju između ICMP i ARP protokola u kontekstu MITM napada. Prikazana dinamika ilustruje kako se legitimna ICMP komunikacija koristi kao okidač za ARP razmenu, koju napadač zloupotrebljava za pozicioniranje između žrtve i gateway-a. Ključni trenutak je slanje lažnog ARP odgovora, kojim se napadač lažno predstavlja kao mrežni izlaz, čime stiče mogućnost presretanja i manipulacije saobraćajem.



Slika 3 Dijagram MITM inicijalizacije zasnovane na ICMP-u putem ARP lažiranja
Source: Author based on (CoreLabs Team, 2020)

Ova vizualizacija omogućava da se jasno sagleda tehnička logika napada i identifikuju tačke u kojima se može primeniti zaštita — posebno kroz firewall pravila, ARP monitoring i ICMP filtriranje.

5.3 Simulacija DNS Spoofing napada na Viber

MITM napadi putem DNS spoofinga predstavljaju ozbiljnu pretnju za aplikacije koje se oslanjaju na nešifrovane DNS zahteve i neadekvatnu TLS validaciju. Sledeći scenario ilustruje kako napadač može kompromitovati komunikaciju između korisnika i Viber servera u realnim uslovima.

5.3.1 Okruženje

Zamislimo korisnika koji koristi Viber na laptopu ili pametnom telefonu dok sedi u kafiću i povezuje se na javni Wi-Fi. Mreža deluje legitimno, ali je zapravo postavljena od strane napadača koji koristi alat poput *Wi-Fi Pineapple* za kreiranje lažnog pristupnog čvora. Uz pomoć alata kao što su *Ettercap* ili *dnsspoof*, napadač preusmerava DNS zahteve ka lažnom DNS serveru koji emituje manipulativne odgovore.

5.3.2 Tok napada

1. Napadač postavlja lažni Wi-Fi AP sa poznatim SSID-om (npr. „Café_Free_WiFi“), čime stvara privid legitimnosti.
2. Korisnik se automatski povezuje, ne znajući da je mreža pod kontrolom napadača.
3. Svi DNS zahtevi koje korisnik šalje (npr. za `api.viber.com`) bivaju presretnuti i zamenjeni lažnim IP adresama koje vode ka napadačevom serveru.

4. Viber aplikacija pokušava da uspostavi TLS konekciju sa serverom, ali zapravo komunicira sa napadačem.
5. Napadač koristi lažni TLS sertifikat kako bi imitirao pravi Viber server.
6. Ako aplikacija ne izvrši adekvatno validiranje sertifikata, konekcija se uspostavlja — MITM napad je uspešan.
7. U suprotnom, ako Viber detektuje neautentičan sertifikat, konekcija se prekida, a korisnik dobija upozorenje (koje može ignorisati).

5.3.3 Uloga firewall-a u ovom scenariju

Firewall može igrati značajnu ulogu u ublažavanju ovog napada, ali njegova efikasnost zavisi od nivoa konfiguracije i prisustva dodatnih bezbednosnih slojeva:

Firewall može pomoći ako:

- Implementira DNS filtering (npr. putem *Pi-hole*-a ili DoH[16]), čime se sprečava presretanje i manipulacija DNS odgovorima.
- Blokira nepoznate IP adrese i neautentične TLS handshake[17], koristeći napredne inspekcijske mehanizme.
- Radi u saradnji sa IDS/IPS sistemima koji detektuju anomalije u DNS saobraćaju i pokušaje falsifikovanja sertifikata.

Firewall ne može pomoći ako:

- Dozvoljava sav izlazni saobraćaj bez restrikcija.
- DNS zahtevi se šalju nešifrovano (klasični UDP port 53), što omogućava lako presretanje.
- Nema TLS inspekciju — u tom slučaju firewall vidi samo da je konekcija „dozvoljena“, bez uvida u sadržaj sertifikata.

U tabeli 8 je sumirana zaštita od MITM napada u slučaju napada na aplikaciju Viber.

Tabela 8. Zaštita od MITM napada preko Viber aplikacije

Element	Da li štiti od MITM?	Napomena
Firewall	Delimično	Mora imati DNS filtering i TLS inspekciju
DNS over HTTPS	Da	Sprečava presretanje DNS zahteva
TLS validacija	Od presudne važnosti	Ako aplikacija ignoriše grešku — MITM uspeva
Korisnik	Ne štiti ako ignoriše upozorenje	Ljudski faktor je često najslabija karika

Izvor: Autor

TLS validacija predstavlja kritičnu tačku zaštite — bez nje, svi ostali slojevi (firewall, DNS filtering, IDS/IPS) mogu biti zaobiđeni. Ako aplikacija ne proverava sertifikat, ili ako korisnik ignoriše upozorenje o nevažećem sertifikatu, napadač može uspešno imitirati server i ostvariti punu kontrolu nad komunikacijom.

5.4 Hipotetički MITM scenario sa WhatsApp-om

1. Korisnik se povezuje na javni Wi-Fi.
2. Napadač koristi *Wi-Fi Pineapple* da kreira lažni AP.
3. WhatsApp pokušava da se poveže na server.
4. Napadač presreće saobraćaj i pokušava da ubaci lažni sertifikat.
5. Standardni L3/L4 firewall može da pročita Server Name Indication (SNI) tokom TLS handshaka, ali bez TLS inspekcije ne može da verifikuje lanac sertifikata, pa lažni sertifikat može proći neopaženo. Mnoge aplikacije sa implementiranim certificate pinning-om, što je česta praksa kod E2E servisa poput WhatsApp-a, dodatno onemogućavaju TLS presretanje i time ograničavaju mogućnosti inspekcije na nivou firewall-a.
6. WhatsApp detektuje neodgovarajući sertifikat i prekida konekciju.

Iako su po nameni slični, između MITM scenarija za Viber i WhatsApp-a postoji značajna razlika. Ključne karakteristike prikazane su tabelom 9.

[16] DoH je skraćenica za *DNS over HTTPS*

[17] TLS handshake je proces kojim klijent (npr. web pregledač) i server (npr. example.com) uspostavljaju sigurnu, šifrovanu vezu.

Tabela 9. Poređenje otpornosti na MITM napade na primeru aplikacije WhatsApp

Aspekt	Viber	WhatsApp
TLS verzija	TLS 1.2/1.3 uz nekonzistentnu validaciju	TLS 1.3 sa PSK za obnovu sesije
Validacija sertifikata	Dozvoljava ignorisanje grešaka u nekim verzijama	Strogo prekida vezu pri nepouzdanom sertifikatu
SNI validacija	U nekim verzijama ne validira SNI	SNI se proverava pre šifrovanja
Otpornost na lažne sertifikate	Niža, prihvata generičke sertifikate	Visoka, proverava CN/SAN i autoritet izdavaoca
Ažuriranje i zakrpe	Nema javno dokumentovanih CVE za MITM	Brzo ispravlja ranjivosti, npr. CVE-2021-24027 (NIST, CVE-2021-24027 Detail, 2024)

Napomena: Tabela je sastavljena na osnovu izjava i izveštaja dostupnih do avgusta 2025. Za najsvežije podatke pratiti zvanične bezbednosne biltene.

Izvor: Autor

5.5 Simulacija mogućeg MITM napada na port 443

Ako firewall dozvoljava sav dolazni saobraćaj na portu 443 bez dodatne inspekcije, MITM napadač može da koristi TLS stripping[18] i da se ubaci u komunikaciju.

U tom scenariju:

- Korisnik pokušava da pristupi HTTPS sajtu (npr. `https://example.com`)
- Napadač presreće zahtev i vraća HTTP verziju sajta (`http://example.com`)
- Korisnik nesvesno komunicira putem nešifrovanog HTTP protokola
- Napadač održava zasebnu HTTPS sesiju sa serverom i prosleđuje podatke, čime postaje transparentni posrednik

Pravilno konfigurisan firewall bi:

- Prepoznao neautentične sertifikate i pokušaje downgrade-a
- Blokirao nešifrovane zahteve koji dolaze ka šifrovanim destinacijama (npr. putem HSTS politike[19])
- Alarmirao administratora o pokušaju manipulacije TLS sesije.

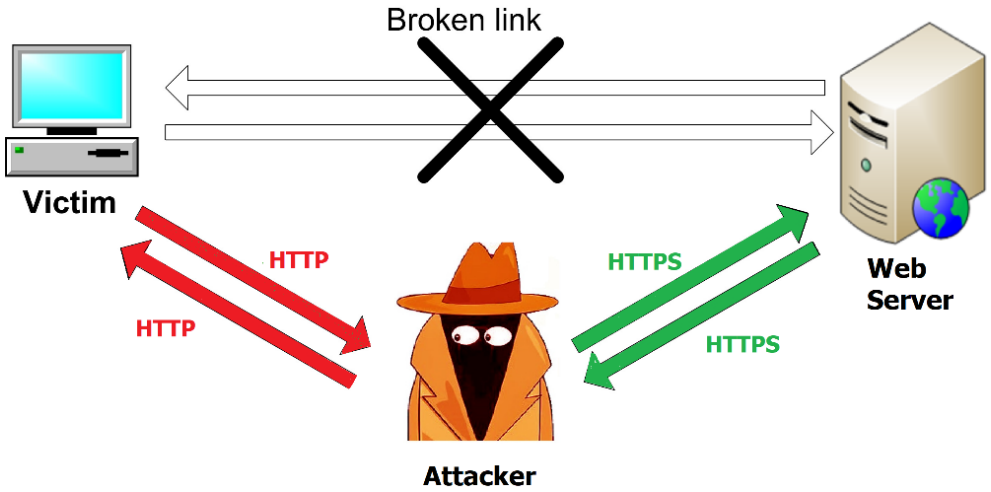
Grafikon prikazan na slici 4 prikazuje TLS stripping napad u MITM scenariju na portu 443.

Napad se odvija na sledeći način:

1. **Žrtva** (Victim) želi da pristupi sajtu
   - Unosi `example.com` u browser — **ne kuca https://**, već samo naziv sajta.
   - Browser šalje inicijalni zahtev preko HTTP-a (port 80), jer nema HSTS politiku u kešu.
2. **Napadač** (Attacker) presreće HTTP zahtev
   - Napadač je u MITM poziciji (npr. lažni Wi-Fi AP).
   - Umesto da dozvoli browseru da pređe na HTTPS, on zadržava komunikaciju na HTTP-u.
3. **Napadač** uspostavlja HTTPS sesiju sa serverom
   - Napadač se povezuje sa `example.com` putem **HTTPS-a** (port 443).
   - Dobija šifrovani odgovor od servera — npr. login forma.
4. **Napadač** dešifruje odgovor i konvertuje ga u HTTP
   - Prikazuje korisniku *nešifrovanu verziju sajta* — izgleda isto, ali nije zaštićena.
   - Korisnik vidi formu, unosi podatke — *ne zna da je stranica HTTP*.
5. **Žrtva** šalje podatke putem HTTP-a
   - Login podaci idu nešifrovano ka napadaču.
   - Napadač ih zatim prosleđuje serveru putem HTTPS-a — server ne zna da je korisnik bio prevaren.

[18] TLS stripping je napredna MITM tehnika kojom se onemogućava automatski prelazak sa HTTP na HTTPS, čime se korisnik zadržava u nešifrovanom režimu komunikacije

[19] HSTS (HTTP Strict Transport Security) je sigurnosna politika web servera koja štiti korisnike od napada kao što su downgrade napadi i presretanje saobraćaja (MITM) – primorava pregledač da koristi isključivo HTTPS kada komunicira sa određenim domenom.



Slika 4 Prikaz TLS stripping napada u MITM scenariju na portu 443

Izvor: Autor

Pored toga što je načinio grešku i priključio se na zlonameran hot-spot, Žrtva je načinila i grešku što nije upisala oznaku https://.

Da je oznaka https:// bila u prvom zahtevu, TLS stripping napad ne bi bio moguć, jer bi tada pregledač odmah uspostavio direktnu HTTPS sesiju sa serverom. Napadač ne bi mogao da vidi sadržaj, niti da ga modifikuje — jer bi saobraćaj bio šifrovan od početka. TLS stripping bi bio onemogućen, osim ako napadač poseduje validan certifikat (što je izuzetno teško bez kompromitacije CA).

Zato se preporučuje:

- Uvek unositi punu adresu s https://.
- Koristiti VPN na javnim mrežama. Preferirati sajtove sa HSTS politikom i validnim TLS certifikatima.

Koristiti HSTS i „HTTPS-Only Mode“.

6 ZAKLJUČAK: FIREWALL I ZAŠTITA OD MITM NAPADA

Na osnovu izvršene analize, može se zaključiti da firewall može biti iskorišćen u zaštiti od MITM napada, što je ujedno i pozitivan odgovor na prvo istraživačko pitanje (RQ1).

Takođe, analiza je dala odgovor i na drugo istraživačko pitanje (RQ2). U scenarijima MITM napada, kao što je DNS spoofing, firewall zaštita može igrati značajnu ulogu u zaštiti korisnika — pod uslovom da je pravilno konfigurisana i integrisana u širu bezbednosnu strategiju.

To nas navodi na zaključke:

- *Firewall nije samodovoljan*: Osnovna pravila pristupa i port filtriranje nisu dovoljni za sprečavanje sofisticiranih MITM napada.
- *DNS filtering* i *DoH*: Sprečavaju presretanje i manipulaciju DNS zahteva, čime se eliminiše jedna od najčešćih MITM tehnika.
- *TLS validacija je kritična*: Aplikacije moraju striktno proveravati sertifikate servera — bez toga, napad može uspeti čak i uz firewall zaštitu.
- *Napredne funkcije firewalla* (IDS/IPS, TLS inspection, segmentacija mreže) omogućavaju detekciju anomalija i blokiranje sumnjivog saobraćaja.
- *Ljudski faktor ostaje stalna ranjivost*: Ignorisanje upozorenja o sertifikatima ili povezivanje na nepoznate mreže može poništiti tehničke mere zaštite.
- Firewall može biti efikasan alat protiv MITM napada, ali samo kao deo višeslojne bezbednosne arhitekture koja uključuje:
  - Šifrovane DNS zahteve
  - Validaciju TLS sertifikata
  - Detekciju anomalija
  - Edukaciju korisnika

U kontekstu aplikacija koje koriste end-to-end enkripciju, kao što je npr. Viber, firewall može pomoći da se spreči pristup lažnim serverima, ali ne može zameniti bezbednosne mehanizme unutar same aplikacije.

CITIRANA DELA

AAG. (2025, July 1). *The latest 2025 cyber crime statistics (updated July 2025).* https://aag-it.com/the-latest-cyber-crime-statistics/

Abbasi, S. (2025, February 18). *Qualys TRU discovers two vulnerabilities in OpenSSH: CVE-2025-26465 & CVE-2025-26466.* https://blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discovers-two-vulnerabilities-in-openssh-cve-2025-26465-cve-2025-26466

Aijaz, D. (2025, January 1). *Year-end analysis: Man-in-the-middle attacks in the US in 2024.* https://www.purewl.com/man-in-the-middle-attacks-in-the-us-in-2024/

APWG. (2025, July 2). *Phishing activity trends reports: 1st quarter 2025.* https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf

Arad, R. (2024, November 20). *6 ways to prevent man-in-the-middle (MITM) attacks.* https://www.memcyco.com/6-ways-to-prevent-man-in-the-middle-mitm-attacks/

Astra Security. (2023, July 7). *13 man-in-the-middle attack statistics you must know about.* https://securityescape.com/man-in-the-middle-attack-statistics/

Cekerevac, Z. (2025, August 25). Firewall-based defense strategies against man-in-the-middle attacks. MEST Journal. https://mest.meste.org/MEST_Najava/XXVII_Cekerevac_Firewall.pdf

Cekerevac, Z., Cekerevac, P., Prigoda, L., & Naima, F. A. (2025, January 15). Security risks from the modern man-in-the-middle attacks. *MEST Journal, 13*(1), 34–51. https://doi.org/10.12709/mest.13.13.01.04

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017a). Internet of things and the man-in-the-middle attacks – Security and economic risks. *MEST Journal, 5*(2), 15–25. https://doi.org/10.12709/mest.05.05.02.03

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Techno-economic aspect of the man-in-the-middle attacks. *Communications, 2*, 166–172. https://doi.org/10.26552/com.C.2017.2.166-172

Citakovic, S. (2023, May 23). *10 SQL injection attacks statistics to know in 2023.* https://securityescape.com/sql-injection-attacks-statistics/

CoreLabs Team. (2020, May 22). *MS15-011 – Microsoft Windows Group Policy real exploitation via a SMB MiTM attack.* https://www.coresecurity.com/core-labs/articles/ms15-011-microsoft-windows-group-policy-real-exploitation-via-a-smb-mitm-attack

CVEdetails. (2025). *Security vulnerabilities, CVEs published in 2024.* https://www.cvedetails.com/vulnerability-list/year-2024/vulnerabilities.html

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium* (Vol. 13, p. 17). USENIX Association. https://doi.org/10.5555/1251375.1251396

Hackmanac. (2024, July 24). *Global cyber attacks report 2024.* https://hackmanac.com/hackmanac-global-cyber-attacks-report-2024

Hlapisi, N. (2023, July 16). *Vulnerabilities and attacks on Bluetooth LE devices—Reviewing recent info.* https://www.allaboutcircuits.com/technical-articles/vulnerabilities-and-attacks-on-bluetooth-le-devicesreviewing-recent-info/

IBM. (2025). *Cost of a data breach.* https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

Israel, K., & Young, R. (2025, January 10). *Verizon provides update on Salt Typhoon matter.* https://www.verizon.com/about/news/verizon-provides-update-salt-typhoon-matter

Jackson, M. (2024, November 8). *The state of SQL injection.* https://www.aikido.dev/blog/the-state-of-sql-injections

Jaikaran, C. (2025, January 23). *Salt Typhoon hacks of telecommunications companies and federal response implications.* https://www.congress.gov/crs-product/IF12798

JumpCloud. (2025, March 7). *What is an evil twin WiFi attack?* https://jumpcloud.com/it-index/what-is-an-evil-twin-wifi-attack

Kapko, M. (2025, January 7). *AT&T, Verizon say they evicted Salt Typhoon from their networks.* https://www.cybersecuritydive.com/news/att-verizon-salt-typhoon/736680/

Kaspersky. (2025, June 20). *What is a VPN? How it works, types, and benefits.* https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

Kochi, S. (2024, August 19). *Intelligence groups say Iran behind hacking attempts in Biden-Harris and Trump campaign.* https://eu.usatoday.com/story/news/politics/elections/2024/08/19/fbi-concludes-iran-hacking-attempt-trump/74866004007/

Krouse, S., McMillan, R., & Volz, D. (2024, September 26). *China-linked hackers breach U.S. internet providers in new 'Salt Typhoon' cyberattack. The Wall Street Journal.* https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

Lakshmanan, R. (2024, June 28). *TeamViewer detects security breach in corporate IT environment.* https://thehackernews.com/2024/06/teamviewer-detects-security-breach-in.html

Langley, M. (2024, July 2). *TeamViewer confirms breach by notorious Russian hacking group Cozy Bear.* https://dailysecurityreview.com/security-spotlight/teamviewer-confirms-breach-by-notorious-russian-hacking-group-cozy-bear/

Lyons, J. (2024, December 30). *More telcos confirm China Salt Typhoon security breaches as White House weighs in.* https://www.theregister.com/2024/12/30/att_verizon_confirm_salt_typhoon_breach/

McAfee. (2016). *McAfee Labs threats report.* Intel Security.

Microsoft. (2024). *Microsoft digital defense report 2024.* https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

MITRE ATT&CK. (n.d.-a). *Adversary-in-the-middle (T1557).* https://attack.mitre.org/techniques/T1557/

MITRE ATT&CK. (n.d.-b). *Non-application layer protocol (T1095).* https://attack.mitre.org/techniques/T1095/

Mizrahi, Y., & Zohar, M. (2023, December 25). *SSH protocol flaw – Terrapin attack CVE-2023-48795: All you need to know.* https://jfrog.com/blog/ssh-protocol-flaw-terrapin-attack-cve-2023-48795-all-you-need-to-know/

Morgan, S. (2023, October 3). *Software supply chain attacks to cost the world $60 billion by 2025.* https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/

Morgan, S. (2025, March 12). *Global ransomware damage costs predicted to hit.* https://elastio.com/wp-content/uploads/2025/04/RANSOMWARE-REPORT-2025-final.pdf

Mullvad. (2025, March 27). *Successful security assessment of our Android app.* https://mullvad.net/en/blog/successful-security-assessment-of-our-android-app/

NETSCOUT. (2024). *DDoS threat intelligence report – 1H 2024 (Issue 13).* https://www.netscout.com/threatreport/wp-content/uploads/2024/09/TR_1H2024_Web.pdf

Nickfetrat, F. (2024, October 9). *iptables vs nftables: What's new in Linux firewalling?* https://dev.to/farshad_nick/iptables-vs-nftables-whats-new-in-linux-firewalling-4a36

Nicole, S. (2025, July 4). *What is an SSID & why naming conventions matter.* https://exactlyhowlong.com/what-is-an-ssid-why-naming-conventions-matter/

NIST. (2024, November 21). *CVE-2021-24027 detail.* https://nvd.nist.gov/vuln/detail/CVE-2021-24027

NIST. (2025, June 2). *CVE-2025-26465 detail.* https://nvd.nist.gov/vuln/detail/CVE-2025-26465

Ojha, D. (2023, December 22). *SSH prefix truncation vulnerability used in Terrapin attacks (CVE-2023-48795).* https://threatprotect.qualys.com/2023/12/22/ssh-vulnerability-used-in-terrapin-attacks-cve-2023-48795/

Okoruwa, S., & Chapman, S. (2025, April 25). *25 ransomware statistics, facts & trends in 2025.* https://www.cloudwards.net/ransomware-statistics/

OWASP. (2025). *XML security cheat sheet.* https://cheatsheetseries.owasp.org/cheatsheets/XML_Security_Cheat_Sheet.html#man-in-the-middle-mitm-attack

Palatty, N. J. (2025, June 20). *How many cyber attacks per day: The latest stats and impacts in 2025.* https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/

Poireault, K. (2023, December 14). *Cozy Bear hackers target JetBrains TeamCity servers in global campaign. Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/cozy-bear-russia-jetbrains-teamcity/

Postel, J. (1981, September). *RFC 792: Internet control message protocol.* https://datatracker.ietf.org/doc/html/rfc792

Qualys Threat Research Unit. (2025, February 19). *2023 Qualys TruRisk research report.* https://www.qualys.com/forms/tru-research-report/

Red Hat. (2024, October 6). *CVE-2023-48795.* https://access.redhat.com/security/cve/cve-2023-48795

SANS Institute. (2020). *ICMP abuse in network attacks.* https://www.sans.org

Sharma, S. (2024, August 12). *Trump campaign suffers sensitive data breach in alleged Iranian hack.* https://www.csoonline.com/article/3485643/trump-campaign-suffers-sensitive-data-breach-in-alleged-iranian-hack.html

Smith, G. (2025, June 4). *Top +35 DDoS statistics (2025).* https://www.stationx.net/ddos-statistics/

Snape, G. (2025, February 19). *Supply chain cyber attacks surge over 400%, expected to continue rising – Cowbell report.* https://www.insurancebusinessmag.com/us/news/cyber/supply-chain-cyber-attacks-surge-over-400-expected-to-continue-rising--cowbell-report-525369.aspx

SOCRadar. (2024, June 13). *Phishing in 2024: 4,151% increase since launch of ChatGPT; AI mitigation methods.* https://socradar.io/phishing-in-2024-4151-increase-since-chatgpt/

Spring, T. (2016, August 11). *Bluetooth hack leaves many smart locks, IoT devices vulnerable.* https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

SSL Insights. (2025, May 30). *Phishing statistics for 2025: Latest figures and trends.* https://sslinsights.com/phishing-statistics/

Stanescu, B. (2012, May 17). *Top 5: Corporate losses due to hacking.* Hot for Security*: Industry News*. Retrieved from https://hotforsecurity.bitdefender.com/blog/top-5-corporate-losses-due-to-hacking-1820.html [Link no longer active]

StormWall. (2025, May 28). *What's new in the world of DDoS? StormWall's Q1 2025 report.* https://stormwall.network/resources/blog/ddos-report-q1-2025

Threat Hunter Team. (2025, February 20). *Ransomware 2025: Attacks keep rising as threat shows its resilience.* https://www.security.com/threat-intelligence/ransomware-trends-2025

Toulas, B. (2024, January 3). *Nearly 11 million SSH servers vulnerable to new Terrapin attacks.* https://www.bleepingcomputer.com/news/security/nearly-11-million-ssh-servers-vulnerable-to-new-terrapin-attacks/

Vahab, A. B. (2025, May 06). *OWASP IoT Top 10 Vulnerabilities (2025 Updated)*. Wattlecorp Cybersecurity Labs: https://www.wattlecorp.com/owasp-iot-top-10/

Verizon. (2025). *2025 data breach investigations report.* https://www.verizon.com/business/resources/reports/dbir/

Wabuge, D. (2023, July 7). *13 man-in-the-middle attack statistics you must know about.* https://securityescape.com/man-in-the-middle-attack-statistics/

Watlecorp. (2025, May 6). *OWASP IoT top 10 vulnerabilities (2025 updated).* https://www.wattlecorp.com/owasp-iot-top-10/

Received for publication: 12.08.2025
Revision received: 17.08.2025
Accepted for publication: 25.08.2025.

How to cite this article?

Style – **APA** *7th Edition:*

Cekerevac, Z. (2025, August 15). Firewall as the first line of defense against MITM attacks. MEST Journal – SP FBIM Transactions, 13(SP-2), 1–25. https://doi.org/10.12709/mest.13.13.SP2.01

Style – **Chicago** *Sixteenth Edition:*

Cekerevac, Zoran. "Firewall as the first line of defense against MITM attacks." *MEST Journal – SP FBIM Transactions* 13, no. SP-2 (August 15, 2025): 1–25. https://doi.org/10.12709/mest.13.13.SP2.01

Style – **GOST** *Name Sort:*

Cekerevac Z. Firewall as the first line of defense against MITM attacks // MEST Journal – SP FBIM Transactions. 2025. Vol. 13, No. SP-2. P. 1–25. DOI 10.12709/mest.13.13.SP2.01.

Style – **Harvard** *Anglia:*

Cekerevac, Z. (2025) 'Firewall as the first line of defense against MITM attacks', *MEST Journal – SP FBIM Transactions*, 13(SP-2), pp. 1–25. doi: 10.12709/mest.13.13.SP2.01

Style – **ISO 690** *Numerical Reference:*

Cekerevac, Z., 2025. Firewall as the first line of defense against MITM attacks. *MEST Journal – SP FBIM Transactions*, 13(SP-2), pp. 1–25. Available at: https://doi.org/10.12709/mest.13.13.SP2.01