Univerzitet Singidunum

Zaštita u računarskim mrežama

Doc. dr Nikola Savanović

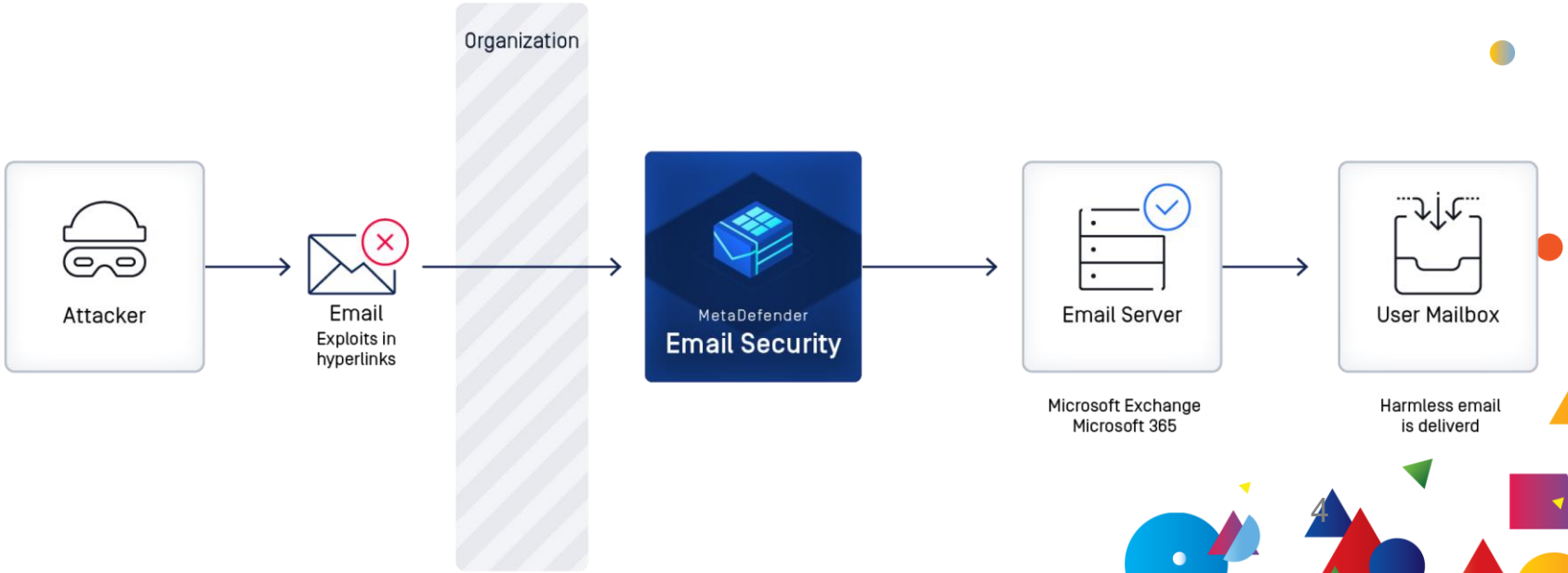
nsavanovic@singidunum.ac.rs

Zaštita e-pošte
DoS i DDoS napadi

Zaštita e-pošte

Ključne stavke


26


Organization
Attacker
Email
Exploits in hyperlinks
MetaDefender
Email Security
Email Server
Microsoft Exchange
Microsoft 365
User Mailbox
Harmless email is deliverd

Uvod u zaštitu e-pošte

- E-pošta predstavlja osnovni komunikacioni kanal u poslovanju i privatnom životu, ali je istovremeno i primarni vektor za sajber napade.
- Glavne pretnje uključuju neželjenu poštu (engl. spam), prevare putem pecanja podataka (engl. phishing), maliciozni softver (engl. malware) i poslovne kompromitacije (engl. Business Email Compromise, BEC).
- Prosečna organizacija prima stotine neželjenih e-poruka dnevno, što značajno utiče na produktivnost i bezbednost.
- Evolucija pretnji zahteva kontinuirano unapređenje mehanizama zaštite, sa fokusom na prevenciju i brzu detekciju.
- Razumevanje načina funkcionisanja ovih napada je prvi korak ka efektivnoj zaštiti e-pošte.
- Očekuje se da će veštačka inteligencija (engl. artificial intelligence, AI) igrati sve veću ulogu u detekciji sofisticiranih napada.
- Edukacija korisnika ostaje ključna odbrana protiv mnogih pretnji koje ciljaju ljudski faktor.

Uvod u zaštitu e-pošte

NC **Notifcation Center <info@perkinsltda.com.co>** September 16, 2024 at 10:03 AM
[E] You Have a New VN For Username 2024-09-16
To: Username@organization.com

Microsoft

Your Services Notification

Hello **Username**,

You're receiving this email because one of your contact left you a wireless caller message. This notification is provided by Organization VoIP service and is set to expire on 2024-09-16.

PLAY / LISTEN >

Thank you for using Microsoft products and services.

This email was sent from an unmonitored mailbox to camila.martinez1@vzw.com.
Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Microsoft

Microsoft Suspicious Login Alert

M Microsoft <login_alert@micrasoft.me>
To

This sender login_alert@micrasoft.me is from outside your organization.

CAUTION: This email originated from outside the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Microsoft

We noticed a login by **from a new device at 19-05-2025 04:13 (UTC+3).**

New Login

Location*	Moscow,Russia
Device	ChromeDesktop

*Location is approximate based on the login's IP address.

If this was you
You can ignore this message. There's no need to take any action.

If this wasn't you
Complete these steps now to protect your account.

1. Check this activity
2. Secure your account

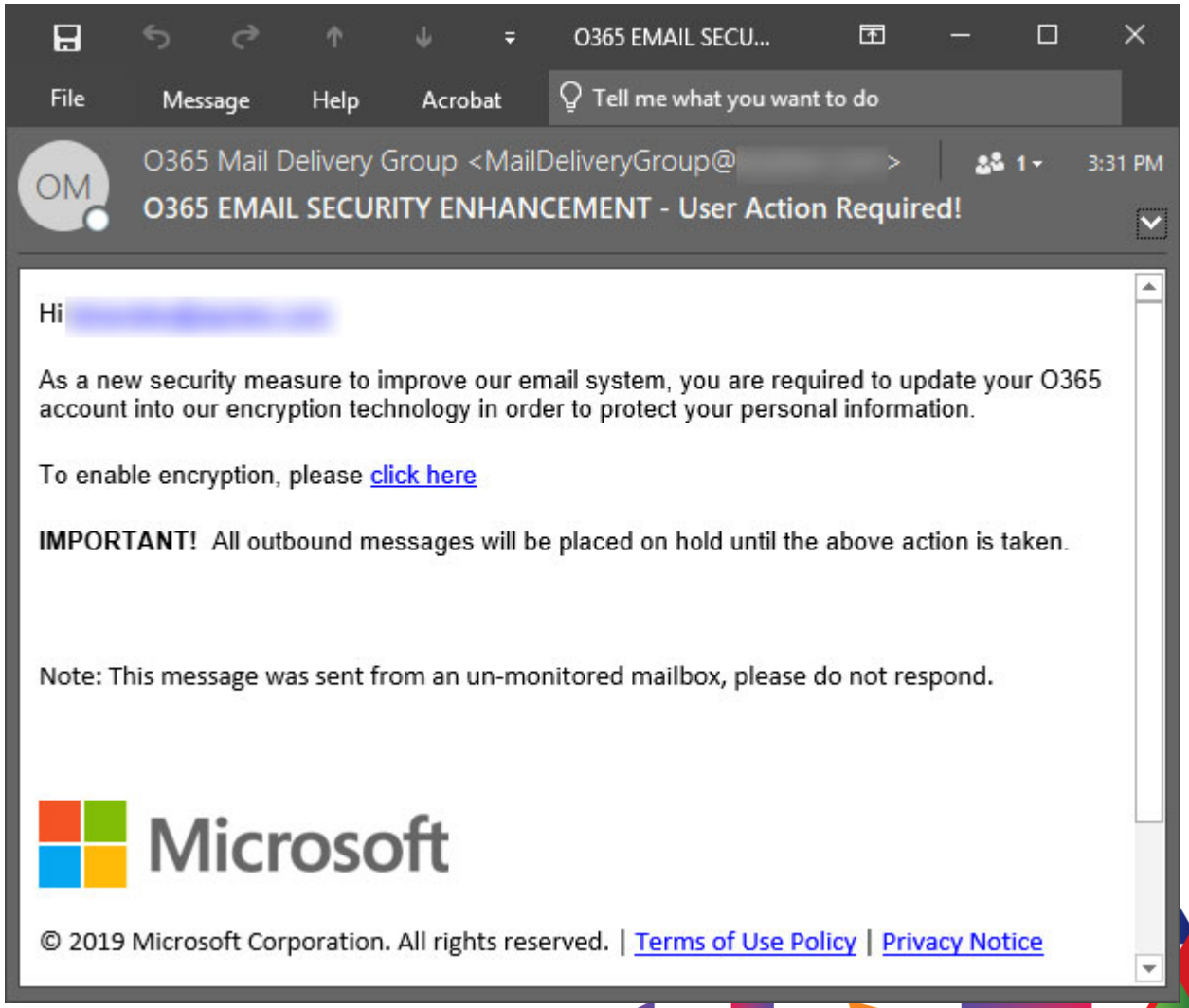
https://login.micrasoft.me/b8f7ac6987b2f772?l=150
Click or tap to follow link.

How do I know if an email is from Microsoft

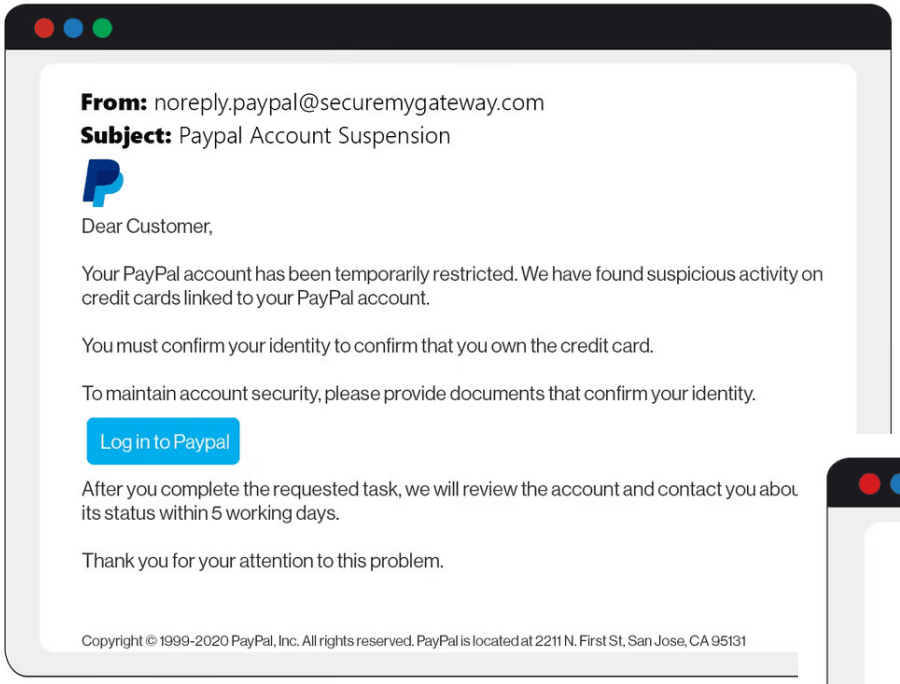
Links in this email will contain "https://" and contain "Microsoft.com". You browser will also display a padlock icon to let you know a site is secure.

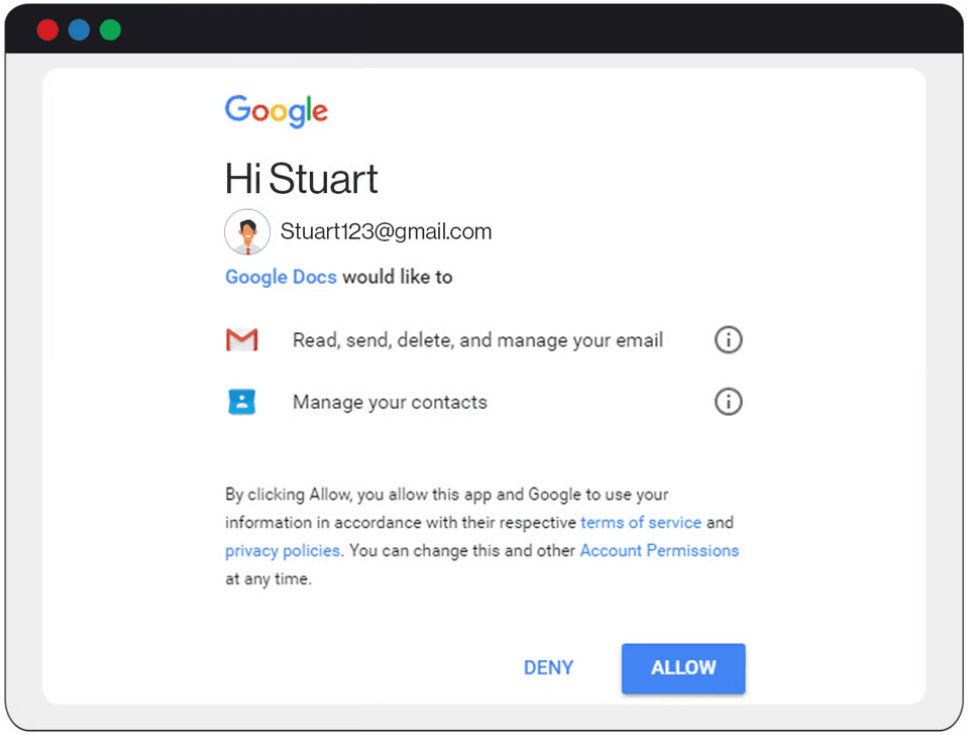
Microsoft

Uvod u zaštitu e-pošte



Uvod u zaštitu e-pošte



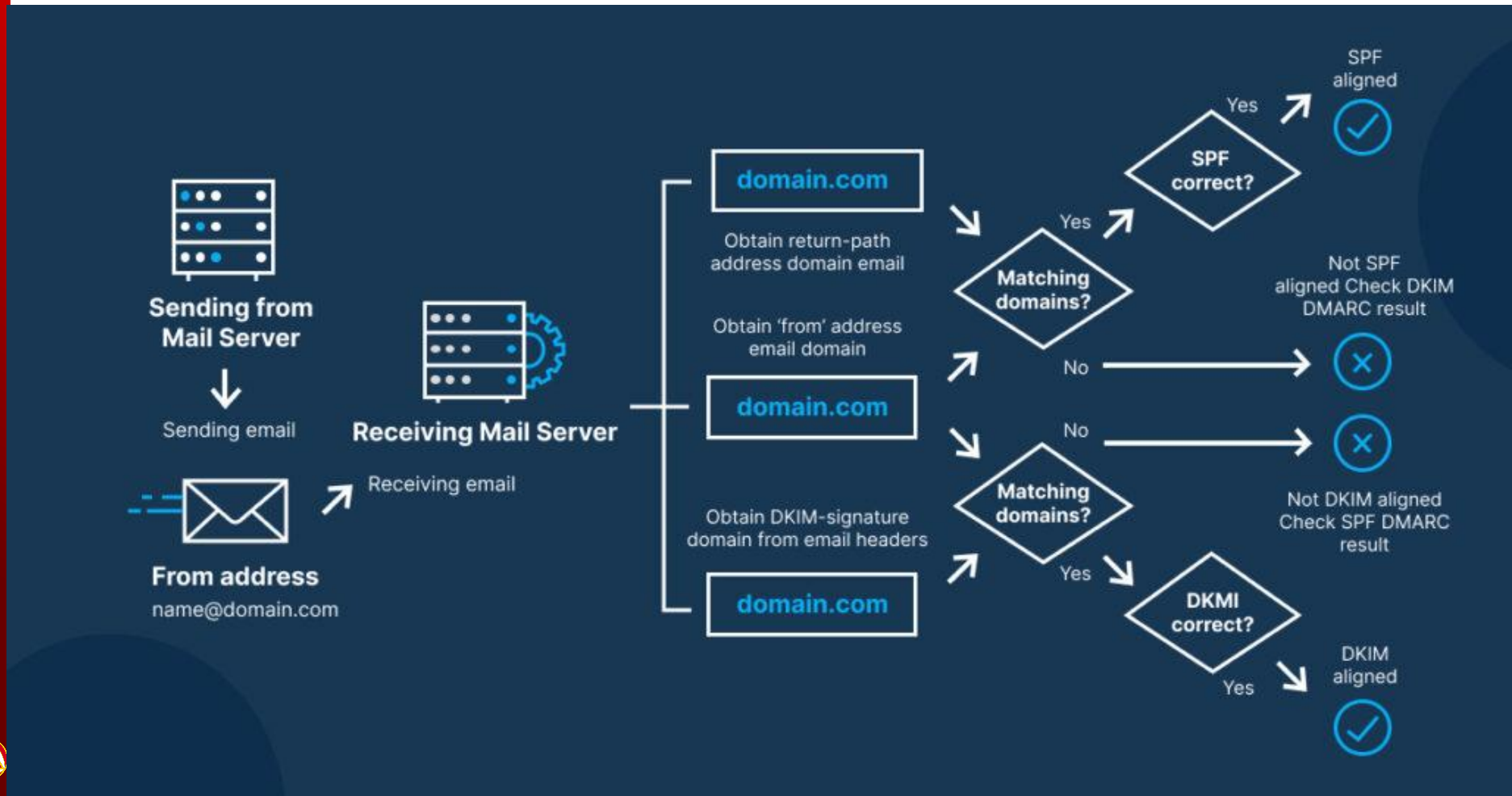


Pecanje podataka (phishing) i zaštita

- Pecanje podataka (engl. phishing) predstavlja socijalni inženjering kojim napadači pokušavaju da pribave osetljive informacije lažnim predstavljanjem.
- Napadi mogu biti opšteg tipa ili visoko targetirani (engl. spear phishing) prema određenim pojedincima.
- Primeri uključuju lažne stranice za prijavu, zahteve za promenu lozinke ili isporuku paketa.
- Zaštita podrazumeva korišćenje višefaktorske autentifikacije (engl. multi-factor authentication, MFA) i obuku zaposlenih.
- Napredna rešenja uključuju filtere za *pecanje* podataka (engl. anti-phishing filters) i analizu URL adresa u realnom vremenu.
- Korisnici treba uvek da proveravaju pošiljaoca i sumnjive linkove pre klika.
- Tehnike poput DMARC (engl. Domain-based Message Authentication, Reporting, and Conformance) pomažu u verifikaciji autentičnosti pošiljaoca.

Pecanje podataka (phishing) i zaštita

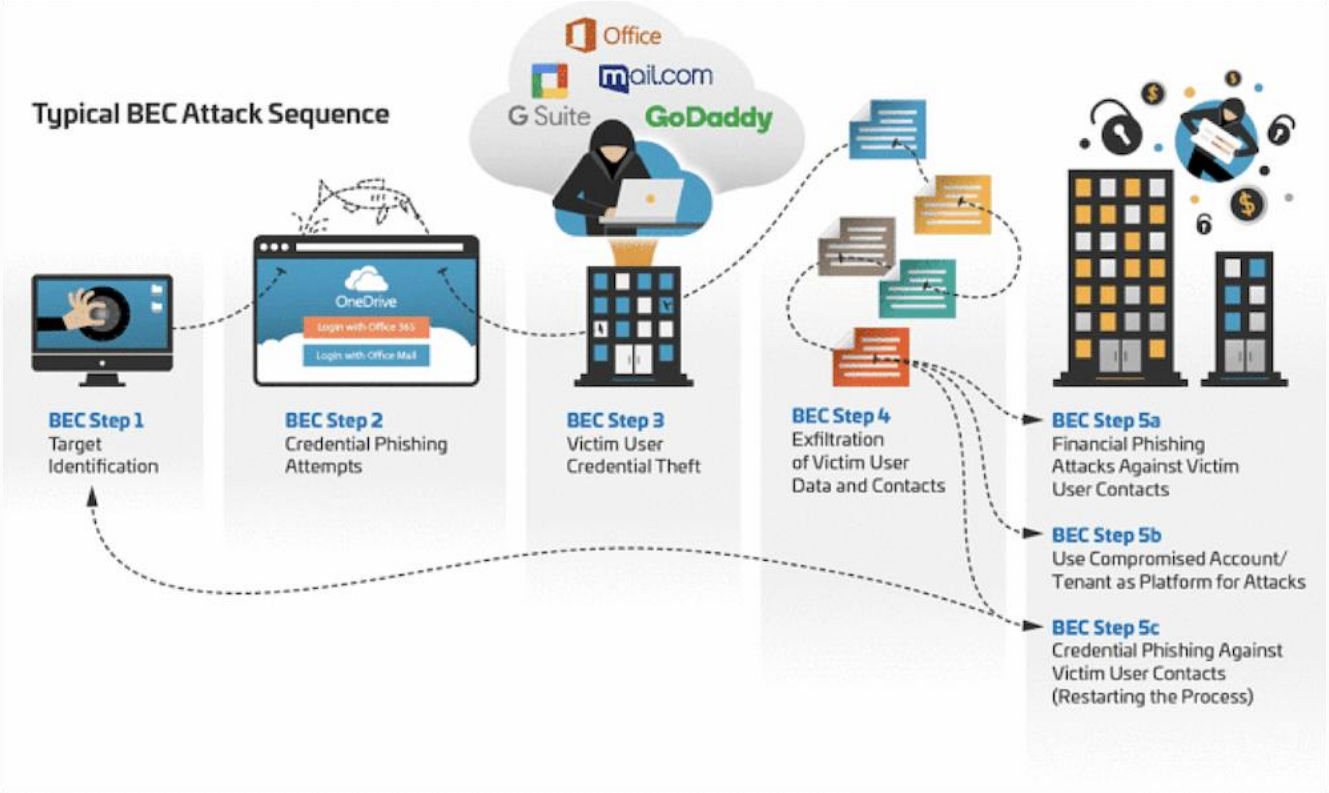
DMARC (engl. Domain-based Message Authentication, Reporting, and Conformance)



Poslovno kompromitovanje (BEC)

- Poslovna kompromitacija (engl. Business Email Compromise, BEC) je sofisticirana prevara koja cilja pojedince sa pristupom finansijama kompanije.
- Napadači se lažno predstavljaju kao rukovodioci ili poslovni partneri, zahtevajući hitne transfere sredstava.
- Ove prevare često koriste inženjering povlačenja (engl. trust engineering) i duboko istraživanje meta.
- Zaštita uključuje stroge protokole za verifikaciju finansijskih transakcija i korišćenje digitalnih potpisa.
- Anti-BEC rešenja bazirana na veštačkoj inteligenciji mogu analizirati anomalije u stilu pisanja i ponašanju e-pošte.
- Obuka zaposlenih o prepoznavanju sumnjivih zahteva je od vitalnog značaja za sprečavanje ovih skupih napada.
- Dvostruka verifikacija putem drugog kanala (npr. telefonskog poziva) je ključna pre izvršenja bilo kakvih finansijskih operacija.

Poslovno kompromitovanje (BEC)

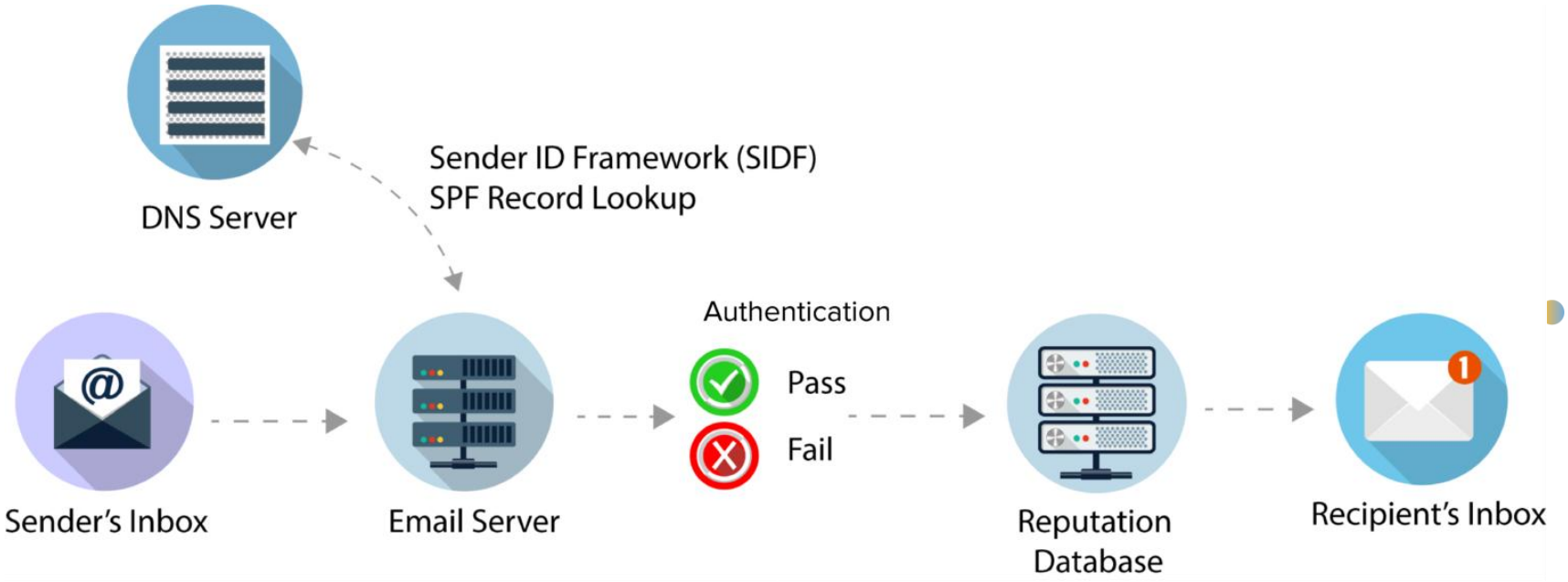


Tehnički mehanizmi zaštite e-pošte

- SMTP protokol (engl. Simple Mail Transfer Protocol) je osnova e-pošte, ali mu nedostaje ugrađena bezbednost za autentifikaciju pošiljaoca.
- SPF (engl. Sender Policy Framework) omogućava domenu da objavi koje IP adrese su ovlašćene za slanje e-pošte u njegovo ime.
- DKIM (engl. DomainKeys Identified Mail) dodaje digitalni potpis e-porukama, omogućavajući primaocu da verifikuje integritet i autentičnost poruke.
- DMARC (engl. Domain-based Message Authentication, Reporting, and Conformance) koordinira SPF i DKIM rezultate, pružajući smernice za postupanje sa neverifikovanim porukama.
- TLS enkripcija (engl. Transport Layer Security) se koristi za šifrovanje komunikacije između servera e-pošte tokom prenosa.
- Bez ovih mehanizama, e-pošta je izuzetno ranjiva na falsifikovanje i presretanje.
- Konfiguracija ovih protokola je neophodna za svaku organizaciju koja ceni bezbednost svojih komunikacija.

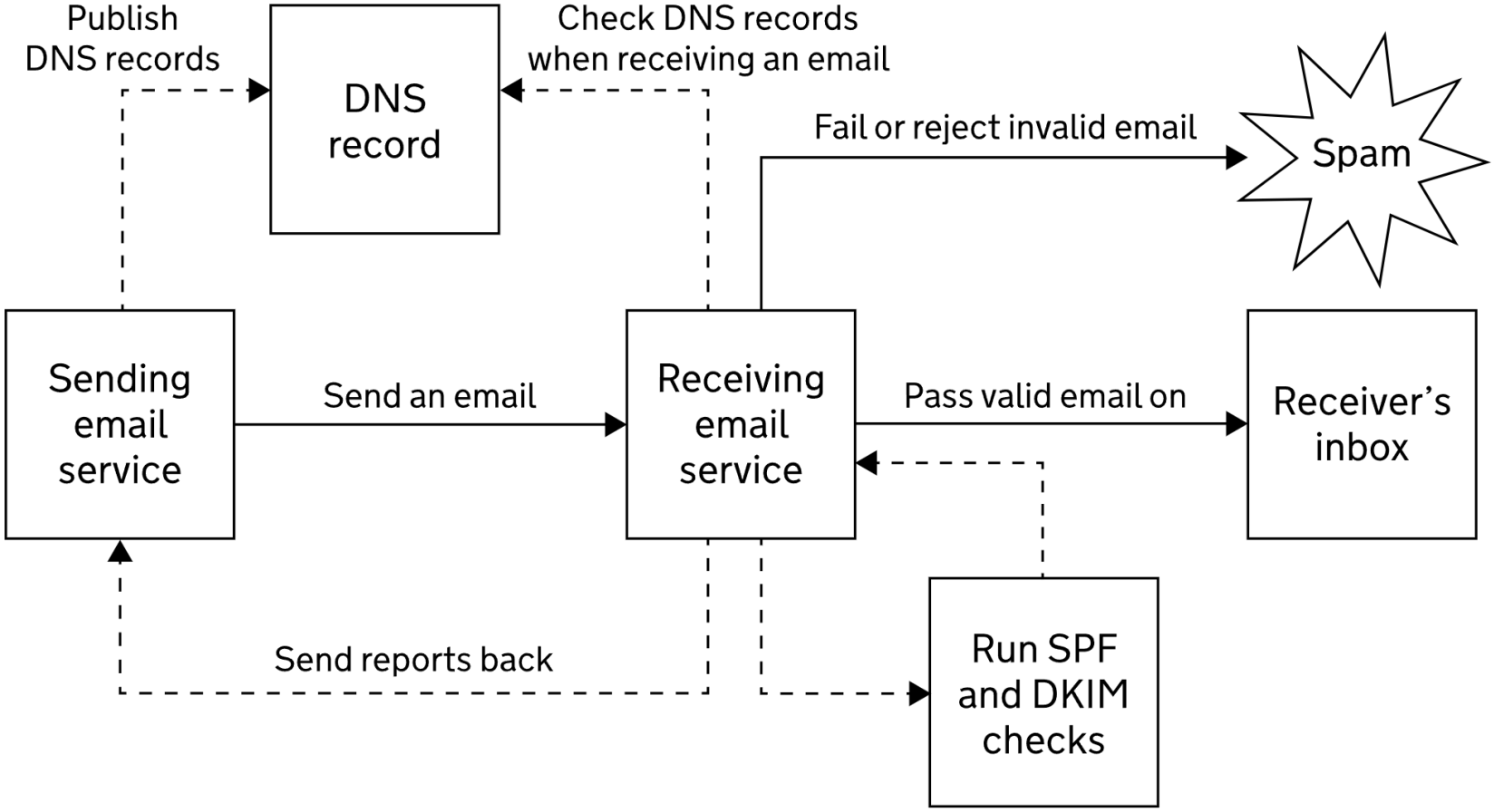
Tehnički mehanizmi zaštite e-pošte

Sender Policy Framework



Tehnički mehanizmi zaštite e-pošte

Domain-based Message Authentication, Reporting, and Conformance



Tehnički mehanizmi zaštite e-pošte

Domain-based Message Authentication, Reporting, and Conformance
U txt zapis u DNS-u se unosi/objavljuje

```
v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@mojdomen.rs
```

Ovo govori svakome ko primi e-poštu od vas sledeće:

- imate DMARC politiku (`v=DMARC1`)
- sve poruke koje ne prođu DMARC provere treba tretirati kao neželjenu poštu (`p=quarantine`)
- treba da tretiraju 100% vaših poruka na ovaj način (`pct=100`)
- treba da vam šalju izveštaje o primljenoj e-pošti (`rua=mailto:dmarc@mojdomen.rs`)

Tehnički mehanizmi zaštite e-pošte

Domain-based Message Authentication, Reporting, and Conformance

U txt zapis u DNS-u se unosi/objavljuje

```
v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@mojdomen.rs
```

v	**Verzija**	**DMARC1**	**Ovo uvek mora biti DMARC1 i označava da je zapis DMARC tipa.**
p	**Politika**	**quarantine**	**Definiše šta primalac treba da uradi sa porukama koje ne prođu DMARC proveru. Moguće vrednosti su:** *** none: Samo nadgledaj i šalji izveštaje. Poruka se isporučuje.** *** quarantine: Označi poruku kao spam/neželjenu poštu.** *** reject: Potpuno odbaci poruku.**
pct	**Procenat**	**100**	**Određuje procenat poruka koje treba podvrgnuti definisanoj politici (p). pct=100 znači da se pravilo primenjuje na sve poruke. Korisno je početi sa nižim procentom (npr. pct=10) i postepeno ga povećavati.**
rua	**Izveštaji (agregatni)**	**mailto:dmarc@mojdomen.rs**	**Definiše e-mail adresu na koju treba slati agregatne izveštaje. Ovi izveštaji se šalju obično jednom dnevno i sadrže XML podatke o svim DMARC proverama za taj dan, uključujući i one koje su prošle i one koje nisu.**

Zaštita od malicioznog softvera i spama

- Anti-spam filteri (engl. anti-spam filters) koriste različite tehnike (npr. crne liste, analizu sadržaja, heuristiku) za identifikaciju i blokiranje neželjene pošte.
- Anti-malver skeneri (engl. anti-malware scanners) skeniraju priloge e-pošte u potrazi za virusima, *ransomware*-om i drugim štetnim softverom.
- Sandbox tehnologije (engl. sandboxing) izvršavaju sumnjive priloge u izolovanom okruženju kako bi procenile njihovo ponašanje.
- URL *rewriting* mehanizam prepisuje linkove u e-porukama, preusmeravajući ih kroz bezbednosni proksi za analizu u realnom vremenu.
- Očekuje se da će mašinsko učenje (engl. machine learning, ML) i veštačka inteligencija značajno unaprediti efikasnost filtera protiv složenih pretnji.
- Redovna ažuriranja definicija malvera su ključna za efektivnu zaštitu.
- Integracija svih ovih elemenata u jedinstven sistem zaštite e-pošte pruža najbolju moguću odbranu.

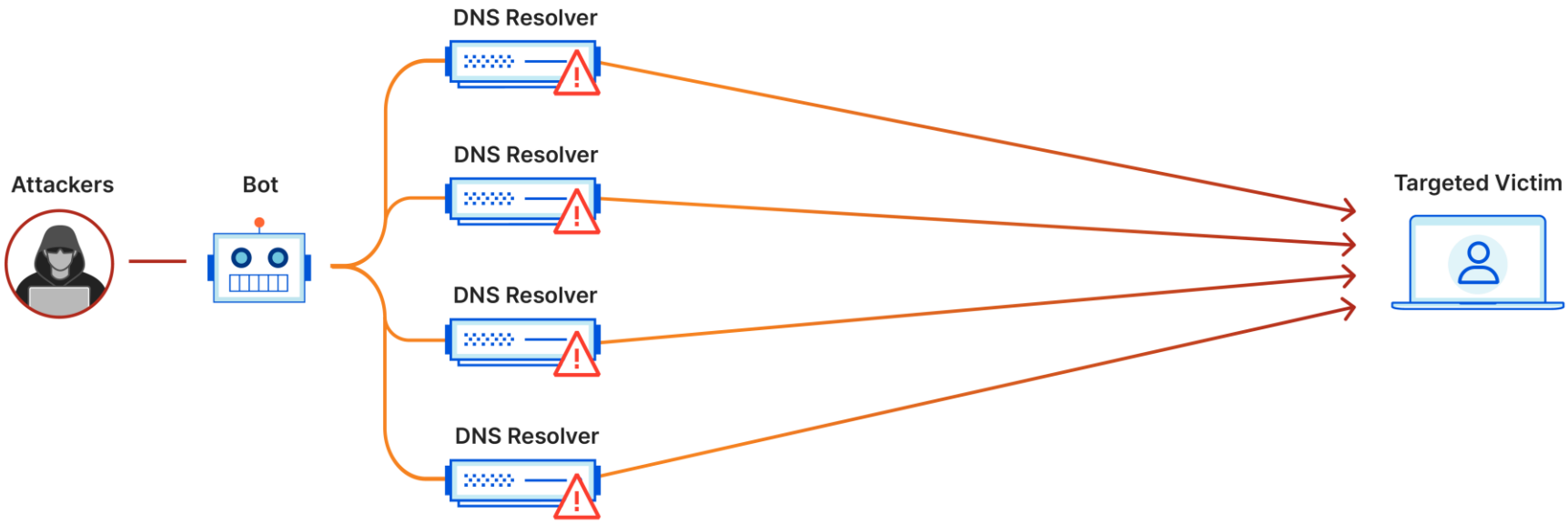
DoS i DDoS napadi

Ključne stavke

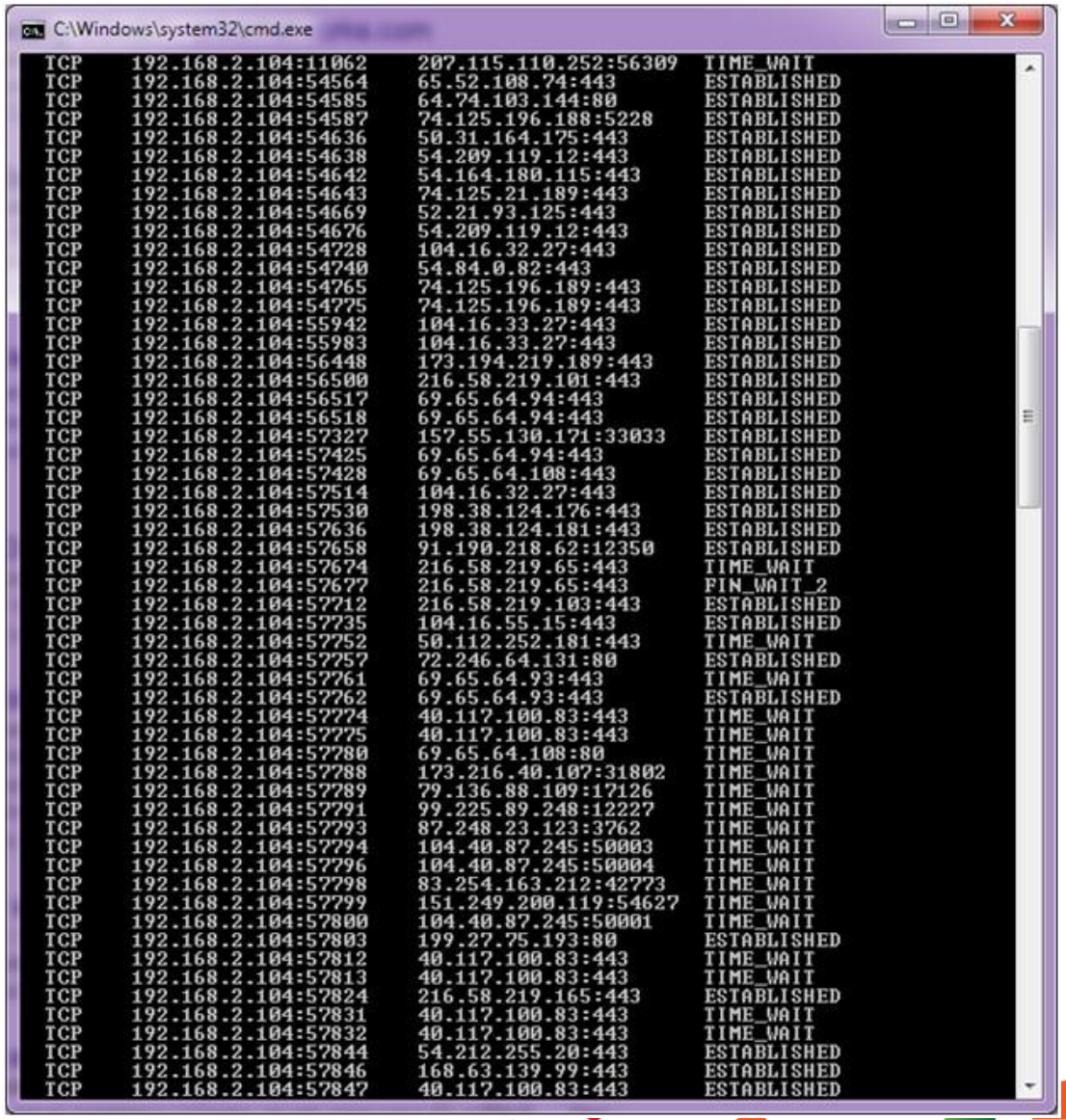
DoS i DDoS Napadi

- DoS (engl. Denial of Service) i DDoS (engl. Distributed Denial of Service) napadi imaju za cilj da onemoguće dostupnost servisa ili resursa.
- Oni to postižu preplavljivanjem sistema saobraćajem ili iskorišćavanjem softverskih ranjivosti.
- DDoS napadi koriste višestruke, često kompromitovane, izvore (engl. botnets) za koordinisano izvođenje napada.
- Posledice mogu uključivati finansijske gubitke, narušenu reputaciju i gubitak poverenja korisnika.
- Evolucija internet infrastrukture omogućila je sve moćnije i sofisticiranije DDoS napade.
- Napadači mogu biti aktivisti, kriminalci, ili državni akteri sa različitim motivima.
- Razumevanje različitih vrsta napada je ključno za izgradnju efikasnih odbrambenih strategija.

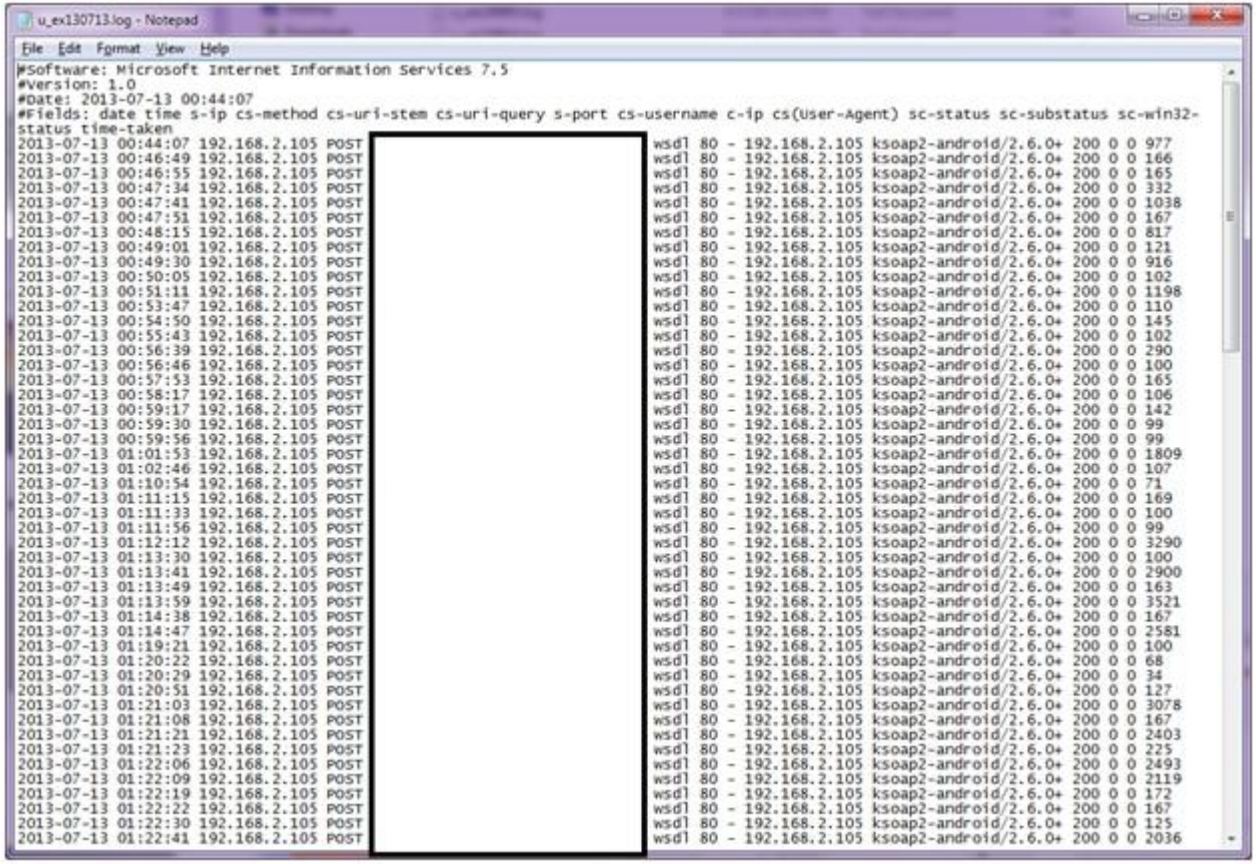
DoS i DDoS Napadi



DoS i DDoS Napadi



DoS i DDoS Napadi



Vrste DoS/DDoS napada –

Mrežni i aplikativni sloj

Napadi na mrežni i transportni sloj (L3 i L4)

Ciljaju protok mreže ili resurse servera.

- Primeri uključuju SYN Flood, UDP Flood, ICMP Flood.
- Ovi napadi pokušavaju da iskoriste ograničenja propusnog opsega ili broj konekcija.

Napadi na aplikativni sloj (L7)

Ciljaju specifične veb aplikacije i njihove resurse.

- Primeri uključuju HTTP Flood, Slowloris, napadi na API-je.
- Ovi napadi su teži za detekciju jer izgledaju kao legitiman saobraćaj.

Volumetrijski napadi (Volumetric Attacks)

Preplavljuju propusni opseg ogromnom količinom saobraćaja.

- Primeri uključuju DNS Amplification, NTP Amplification.

Napdi na mrežne protkole (Protocol Attacks)

Iskorišćavaju ranjivosti u protokolima (npr. SYN Flood).

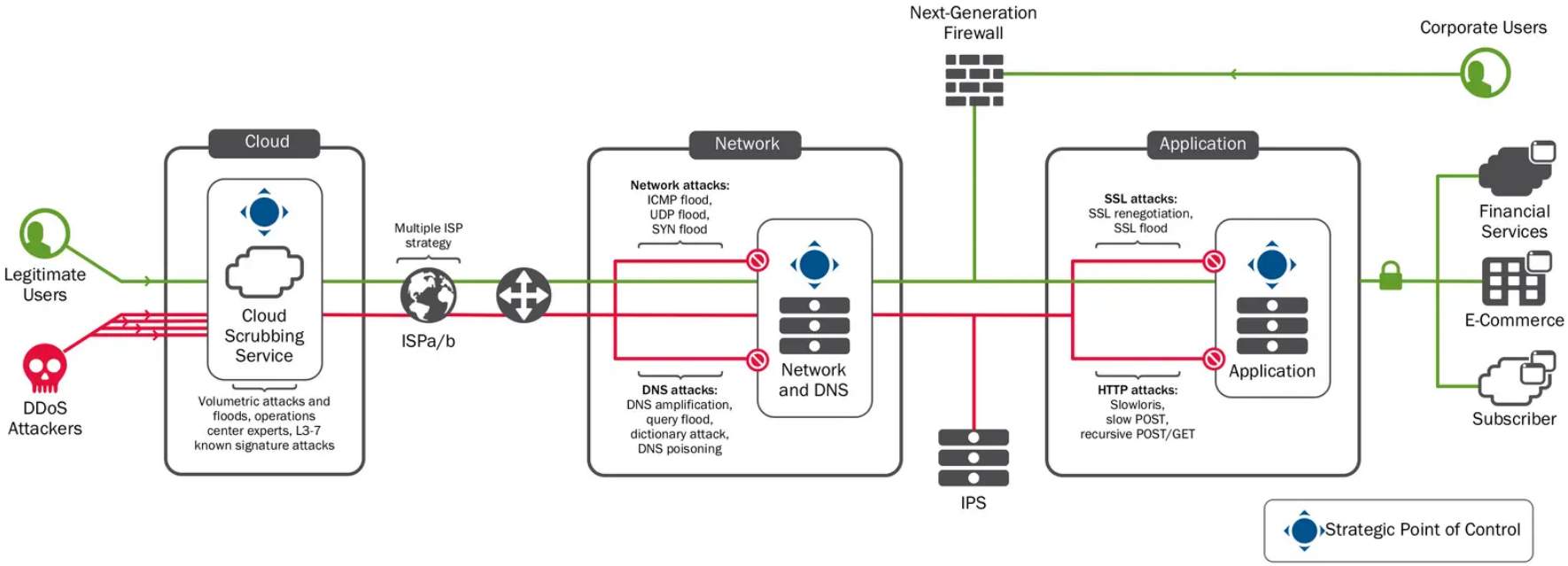
Napadi na resurse (Resource Exhaustion Attacks)

Iskorišćavaju ograničenja resursa servera (CPU, memorija, konekcije).

Vrste DoS/DDoS napada –

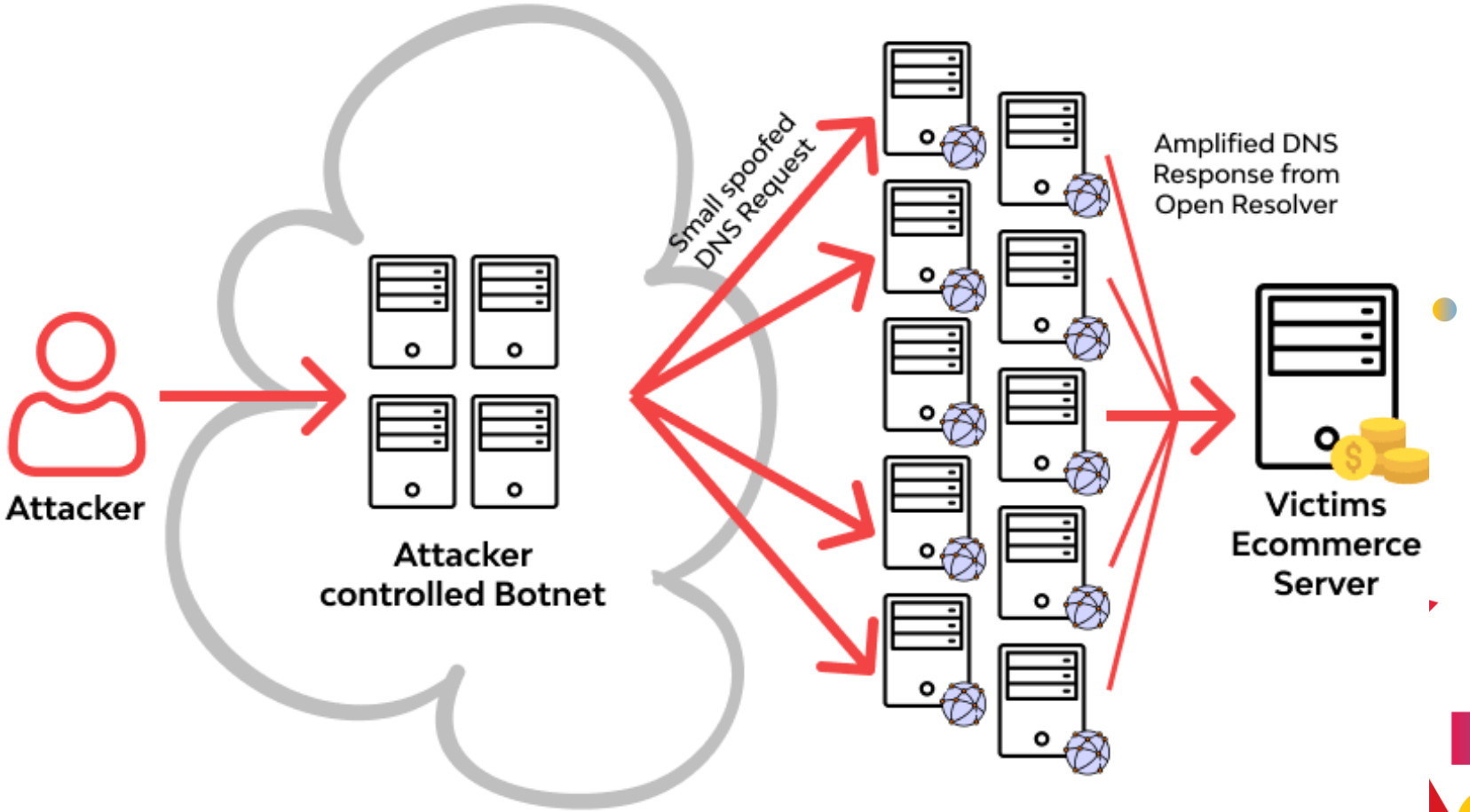
Mrežni i aplikativni sloj

L4



Vrste DoS/DDoS napada –

DNS Amplification



SYN Flood napad i odbrana

- SYN Flood je klasičan DoS napad koji cilja TCP *three-way handshake* protokol.
- Napadač šalje veliki broj SYN paketa bez odgovarajućih ACK paketa.
- Server zadržava resurse čekajući ACK, što dovodi do iscrpljivanja tabela konekcija i nedostupnosti servisa.

Odbrana od napada

SYN Cookies

Mehanizam koji odlaže alokaciju resursa za novu konekciju dok se ne primi validan ACK paket.

Povećanje kapaciteta

Proširivanje resursa servera i mrežnog propusnog opsega.

Rate Limiting

Ograničavanje broja SYN zahteva po IP adresi ili vremenskom periodu.

Firewall pravila

Konfiguracija zaštitnog zida za blokiranje anomalnog SYN saobraćaja.

DDoS *scrubbing* servisi

Preusmeravanje saobraćaja kroz specijalizovane servise koji filtriraju zlonamerni saobraćaj.

HTTP flood i slowloris napadi

HTTP flood

Napadač šalje veliki broj legitimnih HTTP GET ili POST zahteva, preplavljujući veb server.

- Ovi napadi su teški za razlikovanje od legitimnog saobraćaja i često koriste botnete.

Odbrana

Analiza ponašanja (engl. behavioral analytics), CAPTCHA, geografsko blokiranje, WAF (engl. Web Application Firewall).

Slowloris

Napad koji održava mnogo delimičnih HTTP konekcija otvorenim što je duže moguće.

- Šalje seriju delimičnih zahteva, držeći server da čeka na kompletan zahtev.
- Ispunjava sve dostupne konekcije servera, čineći ga nedostupnim za legitimne korisnike.

Odbrana

Konfiguracija veb servera (npr. Apache Timeout/Headers), WAF, *reverse proxy* serveri.

Odbrana od DoS/DDoS napada

Prevencija

Izgradnja robusne mrežne infrastrukture, zaštitni zidovi, IDS/IPS sistemi (engl. Intrusion Detection/Prevention Systems).

Detekcija

Sistemi za nadzor saobraćaja, analitika logova, *behavioral analytics* za anomalije.

Mitigacija (ublažavanje)

DDoS scrubbing servisi

- Klaud provajderi koji filtriraju zlonamerni saobraćaj pre nego što dođe do mreže klijenta.

Crne liste (Blacklisting)

- Blokiranje poznatih zlonamernih IP adresa.

Ograničavanje brzine (Rate Limiting)

- Ograničavanje broja zahteva po IP adresi.

Geo-blokiranje (Geo-blocking)

- Blokiranje saobraćaja iz određenih geografskih regiona.

Odbrana od DoS/DDoS napada

Plan oporavka

- Definisani protokoli za brz oporavak sistema nakon napada.

Implementacija multi-CDN strategije (engl. Content Delivery Network)

- Distribucija sadržaja preko više provajdera za veću otpornost.

Priprema i testiranje

- Redovno testiranje odbrambenih mehanizama i planova za reagovanje.

Zaštita e-pošte

Kriptografija e-pošte i upravljanje ključevima

- Kriptografija e-pošte koristi algoritme za šifrovanje i dešifrovanje poruka, osiguravajući poverljivost i integritet.
- Javna kriptografija (engl. Public Key Cryptography) se oslanja na par ključeva: javni ključ za šifrovanje i privatni ključ za dešifrovanje.
- Upravljanje ključevima je izazov, jer korisnici moraju sigurno generisati, čuvati i razmenjivati svoje privatne ključeve.
- Infrastruktura javnih ključeva (engl. Public Key Infrastructure, PKI) pruža okvire za izdavanje i upravljanje digitalnim sertifikatima.
- Greške u upravljanju ključevima mogu dovesti do gubitka pristupa šifrovanim podacima ili kompromitacije sigurnosti.

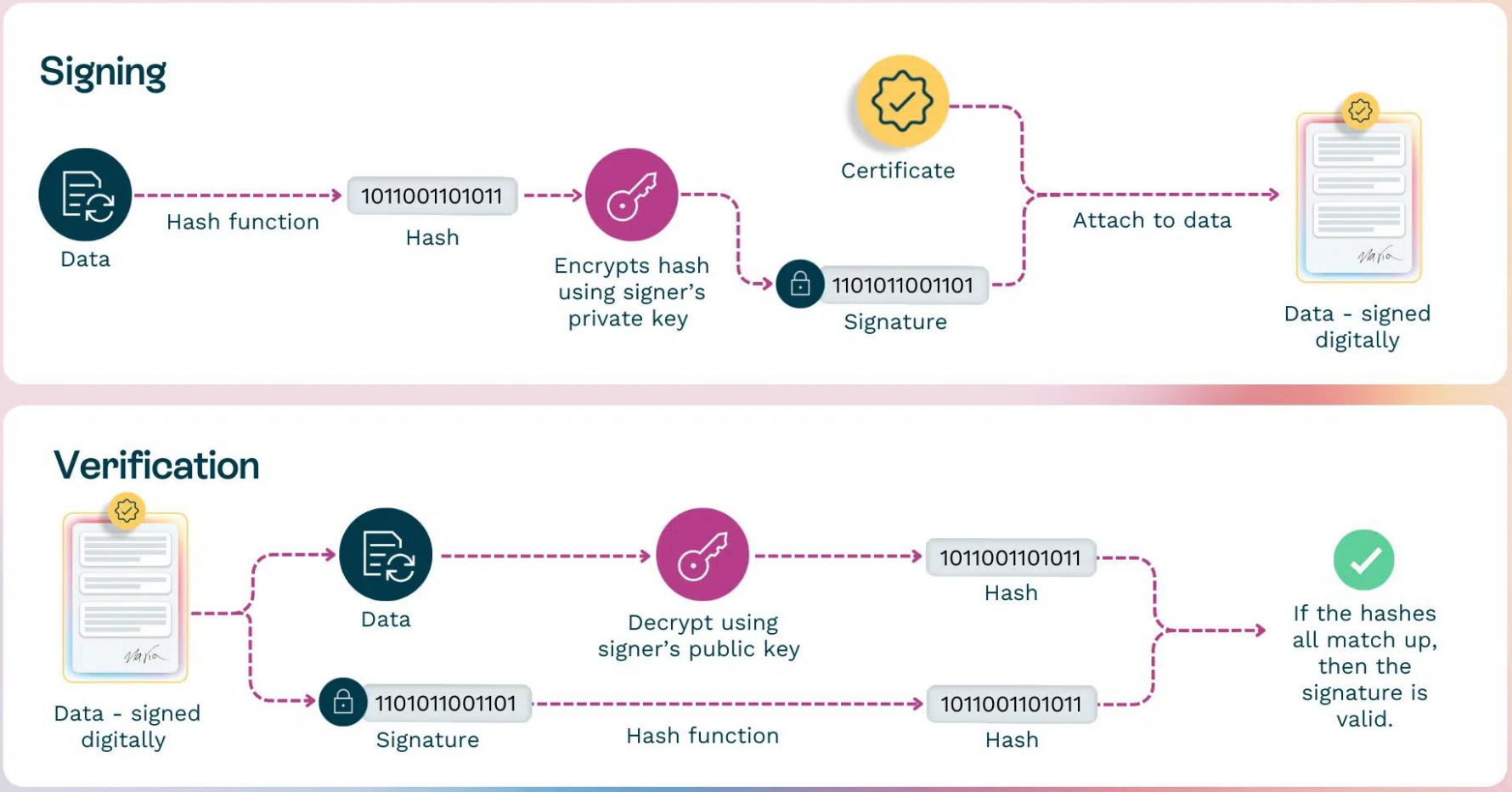
Očekuje se da će blokčejn (engl. blockchain) tehnologije unaprediti decentralizovano upravljanje i verifikaciju identiteta ključeva. Uvodi se automatizovano upravljanje ključevima (engl. Automated Key Management) kao standardna praksa, smanjujući rizik od ljudskih grešaka.

Digitalni potpisi i provera integriteta

- Digitalni potpisi (engl. Digital Signatures) služe za potvrdu autentičnosti pošiljaoca i integriteta sadržaja e-poruke.
- Oni osiguravaju da je poruku poslala osoba koja tvrdi da je poslala i da sadržaj nije menjan tokom prenosa.
- Proces uključuje hešovanje poruke i šifrovanje heš vrednosti privatnim ključem pošiljaoca.
- Primalac dešifruje heš vrednost javnim ključem pošiljaoca i upoređuje je sa sopstvenim hešom primljene poruke.
- Neslaganje heš vrednosti ukazuje na potencijalnu kompromitaciju integriteta poruke.
- Standardi poput S/MIME (engl. Secure/Multipurpose Internet Mail Extensions) i PGP (engl. Pretty Good Privacy) koriste digitalne potpise.

Biometrijske metode verifikacije postaju integrisane sa digitalnim potpisima za povećanu sigurnost.

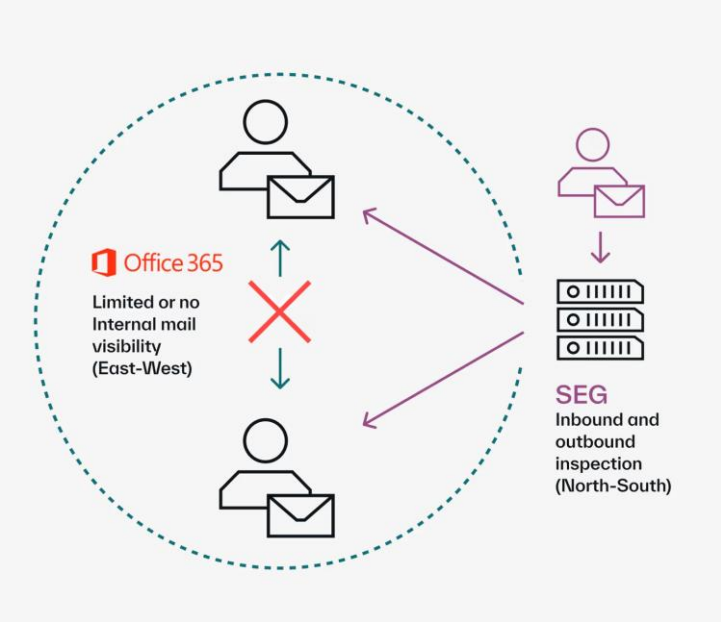
Digitalni potpisi i provera integriteta



Sigurnosna rešenja za e-poštu na gejtveju

- Sigurnosna rešenja na gejtveju (engl. Email Gateway Security) predstavljaju prvu liniju odbrane, skenirajući sav dolazni i odlazni saobraćaj e-pošte.
- Ova rešenja primenjuju višestruke slojeve zaštite, uključujući anti-spam, anti-malver i anti-phishing filtere pre nego što poruke stignu do korisnika.
- Gejtvej može da vrši analizu URL adresa, skeniranje priloga u sandboks okruženju (engl. sandbox analysis) i primenu DMARC, SPF, DKIM protokola.
- Omogućavaju centralizovano upravljanje bezbednosnim politikama i izveštavanje o detektovanim pretnjama.
- Rešenja na gejtveju smanjuju opterećenje internih servera e-pošte i računara korisnika.

Gejtveji se sve više oslanjaju na veštačku inteligenciju (engl. Artificial Intelligence, AI) i mašinsko učenje (engl. Machine Learning, ML) za detekciju napada nultog dana (engl. zero-day attacks) i sofisticiranih socijalnih inženjeringa. Integracija sa sistemima za upravljanje bezbednosnim informacijama i događajima (engl. Security Information and Event Management, SIEM) omogućava sveobuhvatnu vidljivost pretnji.

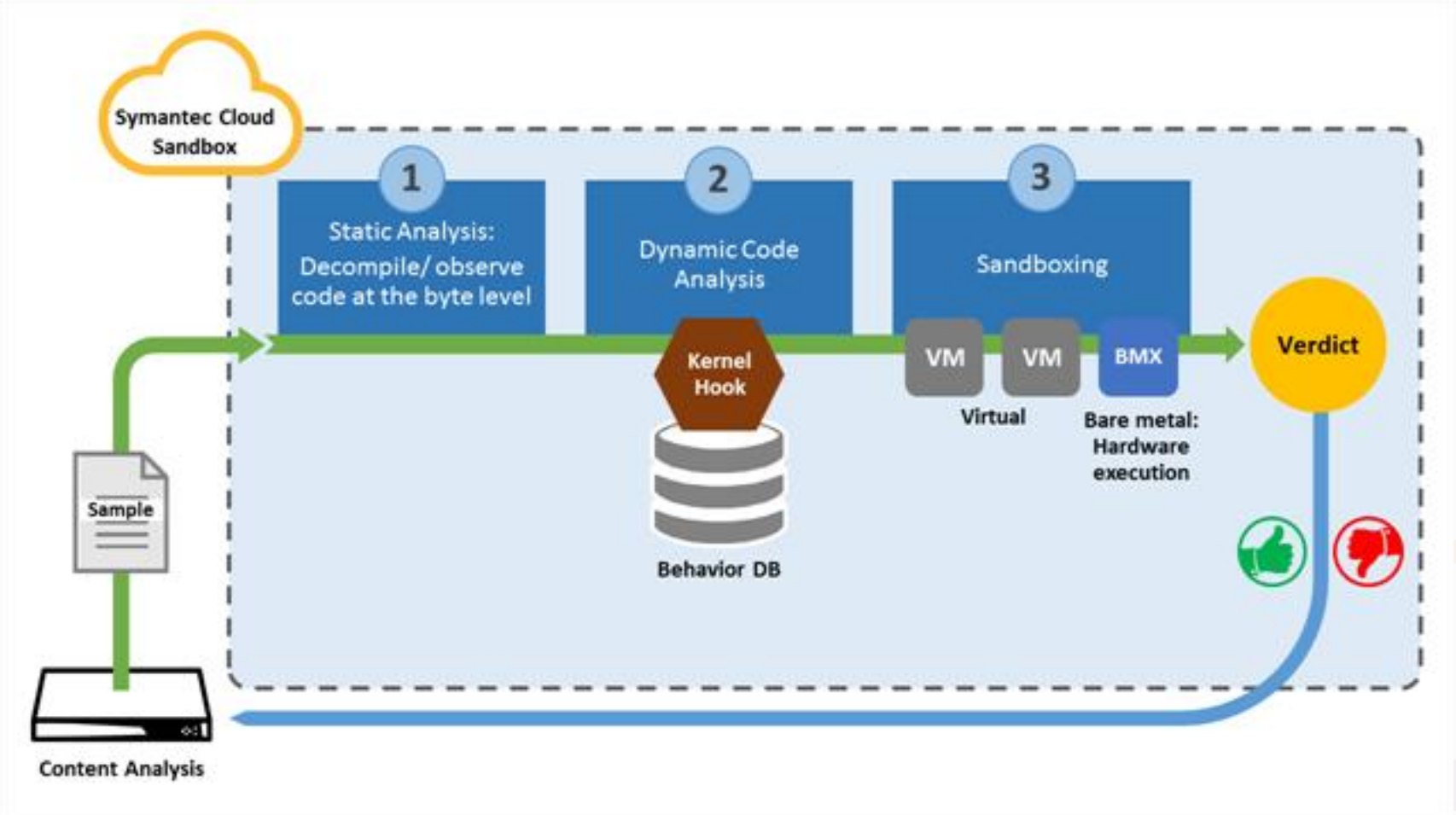


Sandboks analiza (Sandbox Analysis) i komore za detonaciju (Detonation Chambers)

- Sandboks analiza je tehnika gde se sumnjivi prilozi ili linkovi e-pošte otvaraju i izvršavaju u izolovanom, kontrolisanom okruženju.
- Ovo okruženje, poznato kao sandboks (engl. sandbox), imitira stvarne sisteme, omogućavajući praćenje ponašanja potencijalno malicioznog softvera.
- Ako se maliciozni softver pokuša da pristupi osetljivim resursima, šifruje fajlove ili komunicira sa C2 serverima, to se evidentira.
- Komore za detonaciju (engl. Detonation Chambers) su naprednije verzije sandboksa, dizajnirane da pružaju dublju analizu i izbegnu detekciju od strane malvera koji prepoznaje sandboks.
- Ove tehnologije su ključne za detekciju ranije nepoznatog malicioznog softvera (engl. zero-day malware) koji bi zaobišao tradicionalne antivirusne skenere.

Predviđa se da će sandboks rešenja koristiti emulaciju hardvera (engl. hardware emulation) i analizu memorije (engl. memory analysis) u realnom vremenu za još precizniju detekciju. AI i ML algoritmi se koriste za analizu ponašanja u sandboksu i identifikaciju suptilnih anomalija koje ukazuju na pretnju.

Sandboks analiza (Sandbox Analysis)



AI i ML u zaštiti e-pošte

- Veštačka inteligencija i mašinsko učenje transformišu zaštitu e-pošte, omogućavajući naprednu detekciju pretnji.
- AI/ML algoritmi analiziraju ogromne količine podataka o e-pošti, uključujući obrasce slanja, sadržaj, zaglavlja i ponašanje korisnika.
- Ovi sistemi mogu identifikovati anomalije i sumnjive obrasce koji ukazuju na spam, phishing, BEC napade ili prisustvo malicioznog softvera, čak i pre nego što su pretnje poznate.
- Detekcija nultog dana (engl. zero-day detection) je značajno poboljšana zahvaljujući sposobnosti ML modela da prepoznaju nove i mutirajuće pretnje.
- Sistemi se kontinuirano uče i prilagođavaju novim taktikama napadača, pružajući proaktivnu odbranu.

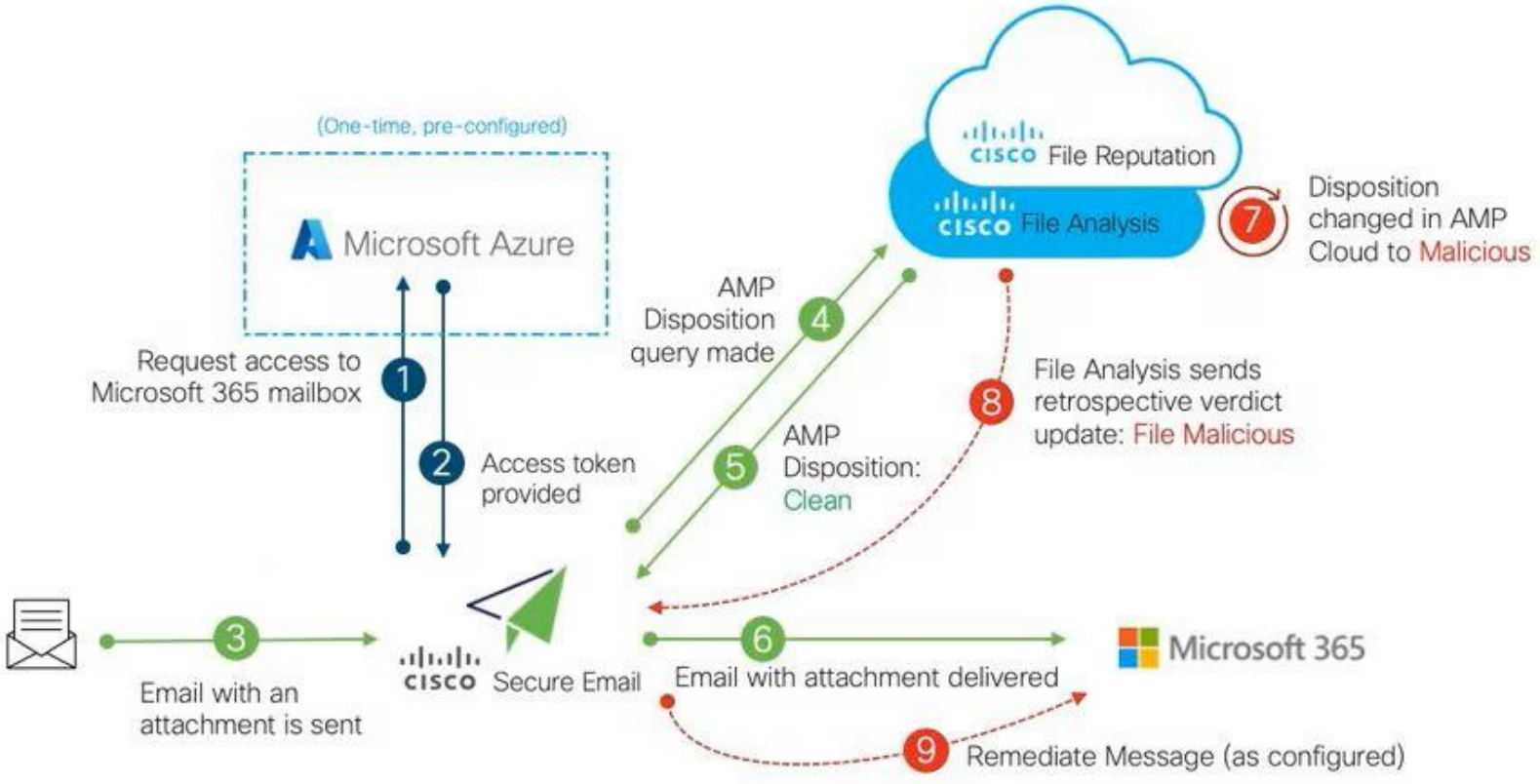
Generativna AI (engl. Generative AI) se koristi za predviđanje evolucije pretnji i simulaciju napada, omogućavajući razvoj robusnijih odbrambenih mehanizama. Automatizovani odgovor na incidente (engl. Automated Incident Response) podržan AI-jem smanjuje vreme reakcije na detektovane pretnje.

Integrisana bezbednost e-pošte (ISE)

- Integrisana bezbednost e-pošte (engl. Integrated Email Security, ISE) predstavlja sveobuhvatan pristup koji kombinuje više bezbednosnih funkcionalnosti u jedinstveno rešenje.
- Umesto pojedinačnih alata za spam, malver ili phishing, ISE platforme nude objedinjenu zaštitu od celokupnog spektra pretnji putem e-pošte.
- Ova rešenja obično uključuju anti-spam filtere, anti-malver skenere, sandboks analizu, zaštitu od phishinga i BEC napada, kao i enkripciju e-pošte.
- Prednosti ISE-a su pojednostavljeno upravljanje, poboljšana koordinacija između bezbednosnih modula i smanjena kompleksnost infrastrukture.
- Cilj je eliminisati "bezbednosne praznine" koje mogu nastati upotrebom različitih, nekoordinisanih rešenja.

ISE platforme integrišu naprednu analizu ponašanja korisnika i entiteta (engl. User and Entity Behavior Analytics, UEBA) kako bi detektovale interne pretnje i kompromitovane naloge. Povezivanje sa platformama za obaveštavanje o pretnjama (engl. Threat Intelligence Platforms) omogućava dinamičko prilagođavanje odbrane.

Integrisana bezbednost e-pošte (ISE)



Politike zadržavanja e-pošte (Email Retention Policies) i arhiviranje

- Politike zadržavanja e-pošte (engl. Email Retention Policies) definišu koliko dugo organizacija mora da čuva e-poruke i sa njima povezane podatke.
- Ove politike su ključne za usklađenost sa zakonskim, regulatornim i internim zahtevima (npr. GDPR, HIPAA, SOX).
- Pravilno sprovedene politike pomažu u upravljanju rizikom od parnica i podržavaju e-otkrivanje (engl. e-discovery) procese.
- Arhiviranje e-pošte (engl. Email Archiving) je proces skladištenja i indeksiranja e-poruka u sigurnom, neizmenljivom formatu za dugoročno čuvanje.
- Arhiviranje omogućava brz pristup istorijskim podacima i olakšava oporavak u slučaju gubitka podataka ili napada.

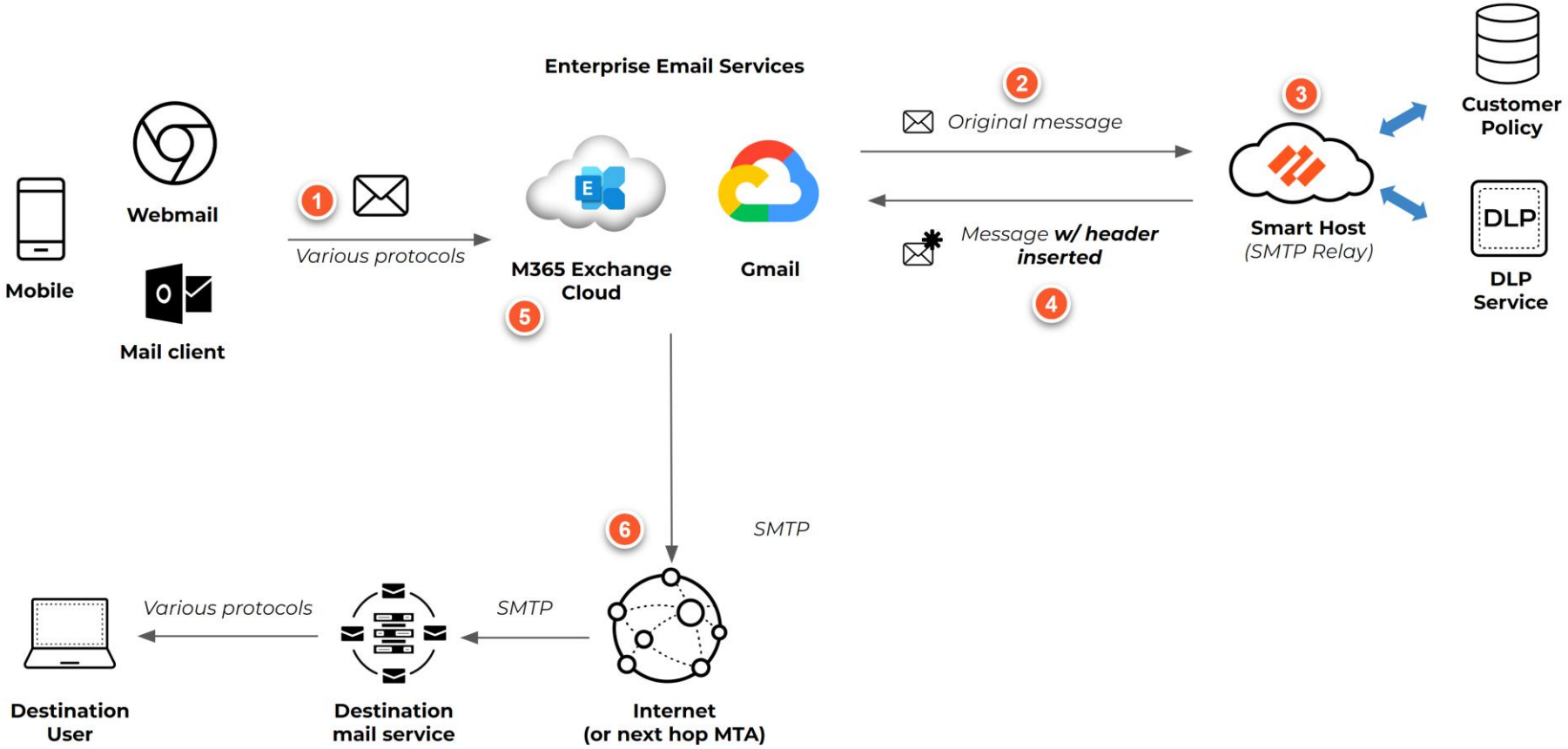
Rešenja za arhiviranje koriste mašinsko učenje za automatsko kategorizovanje i označavanje osetljivih podataka, olakšavajući usklađenost i pretragu. Raste upotreba "immutable" skladišta (skladišta koja se ne mogu menjati) kako bi se osigurala autentičnost arhiviranih podataka.

Data Loss Prevention (DLP) za e-poštu

- Rešenja za prevenciju gubitka podataka (engl. Data Loss Prevention, DLP) za e-poštu dizajnirana su za sprečavanje neovlašćenog izlaska osetljivih informacija iz organizacije putem e-pošte.
- DLP sistemi skeniraju odlazne e-poruke i priloge u potrazi za specifičnim obrascima, ključnim rečima ili tipovima podataka (npr. brojevi kreditnih kartica, lični identifikacioni brojevi).
- Kada se detektuju osetljivi podaci, DLP može blokirati slanje poruke, šifrovati je, upozoriti pošiljaoca ili obavestiti bezbednosni tim.
- Ovo je ključno za usklađenost sa propisima o privatnosti podataka i zaštitu intelektualne svojine.
- DLP politike se mogu prilagoditi specifičnim potrebama organizacije i regulatornim zahtevima.

Napredni DLP sistemi koriste kontekstualnu analizu i mašinsko učenje za preciznije prepoznavanje osetljivih podataka i namere korisnika, smanjujući lažne pozitive. Integracija sa sistemima za upravljanje identitetom i pristupom (engl. Identity and Access Management, IAM) omogućava detaljnije kontrole na osnovu uloga korisnika.

Data Loss Prevention (DLP) za e-poštu



Izveštavanje i revizija (Reporting and Auditing)

- Sistemi za zaštitu e-pošte generišu detaljne izveštaje o detektovanim pretnjama, blokiranim porukama i performansama filtera.
- Izveštavanje omogućava administratorima da prate efikasnost bezbednosnih kontrola i identifikuju trendove u napadima.
- Revizija (engl. auditing) podrazumeva pregled logova i aktivnosti sistema e-pošte radi provere usklađenosti sa politikama i identifikacije potencijalnih bezbednosnih incidenata.
- Regulatorne revizije često zahtevaju detaljnu dokumentaciju o bezbednosnim merama i incidentima.
- Automatski generisani izveštaji pomažu u ispunjavanju zahteva za usklađenost i internim revizijama.

Interaktivne kontrolne table (engl. interactive dashboards) sa vizualizacijom podataka u realnom vremenu postaju standard, pružajući administratorima brzi uvid u stanje bezbednosti e-pošte.AI se koristi za analizu izveštaja i predviđanje budućih pretnji, kao i za identifikaciju obrazaca koje ljudsko oko može propustiti.

Bezbednost e-pošte u oblaku (Cloud Email Security)

- Rešenja za bezbednost e-pošte u oblaku (engl. Cloud Email Security, CES) pružaju zaštitu kao uslugu, hostovanu od strane eksternih provajdera.
- Umesto instaliranja i održavanja lokalnog hardvera i softvera, organizacije preusmeravaju svoj saobraćaj e-pošte kroz provajderove bezbednosne sisteme.
- Prednosti uključuju skalabilnost, visoku dostupnost, automatska ažuriranja i smanjeno opterećenje internih IT resursa.
- CES rešenja često koriste naprednu analizu pretnji, AI/ML i globalnu inteligenciju o pretnjama (engl. global threat intelligence) za brzu detekciju novih napada.
- Pogodna su za organizacije svih veličina, posebno za one koje nemaju resurse za kompleksna lokalna bezbednosna rešenja.

CES platforme se integrišu sa platformama za zaštitu radnog opterećenja u oblaku (engl. Cloud Workload Protection Platforms, CWPP) za holističku bezbednost oblaka. Naglasak je na "zero-trust" arhitekturama u oblaku koje primenjuju stroge kontrole pristupa čak i unutar perimetra.

Obnova i oporavak e-pošte

- Obnova i oporavak e-pošte (engl. Email Backup and Recovery) odnosi se na procese i tehnologije za kreiranje rezervnih kopija (engl. backup) e-poruka i njihovo vraćanje u slučaju gubitka podataka.
- Gubitak podataka e-pošte može nastati usled ljudske greške, tehničkog kvara, malicioznog softvera (poput ransomvera) ili prirodnih katastrofa.
- Strategije rezervnog kopiranja uključuju potpune, inkrementalne i diferencijalne kopije, često skladištene na različitim lokacijama (on-premise i u oblaku).
- Brz i efikasan oporavak je ključan za minimiziranje zastoja u poslovanju i osiguravanje kontinuiteta poslovanja.
- Testiranje planova oporavka je neophodno kako bi se osiguralo da su funkcionalni u kritičnim situacijama.

Obuka o bezbednosti

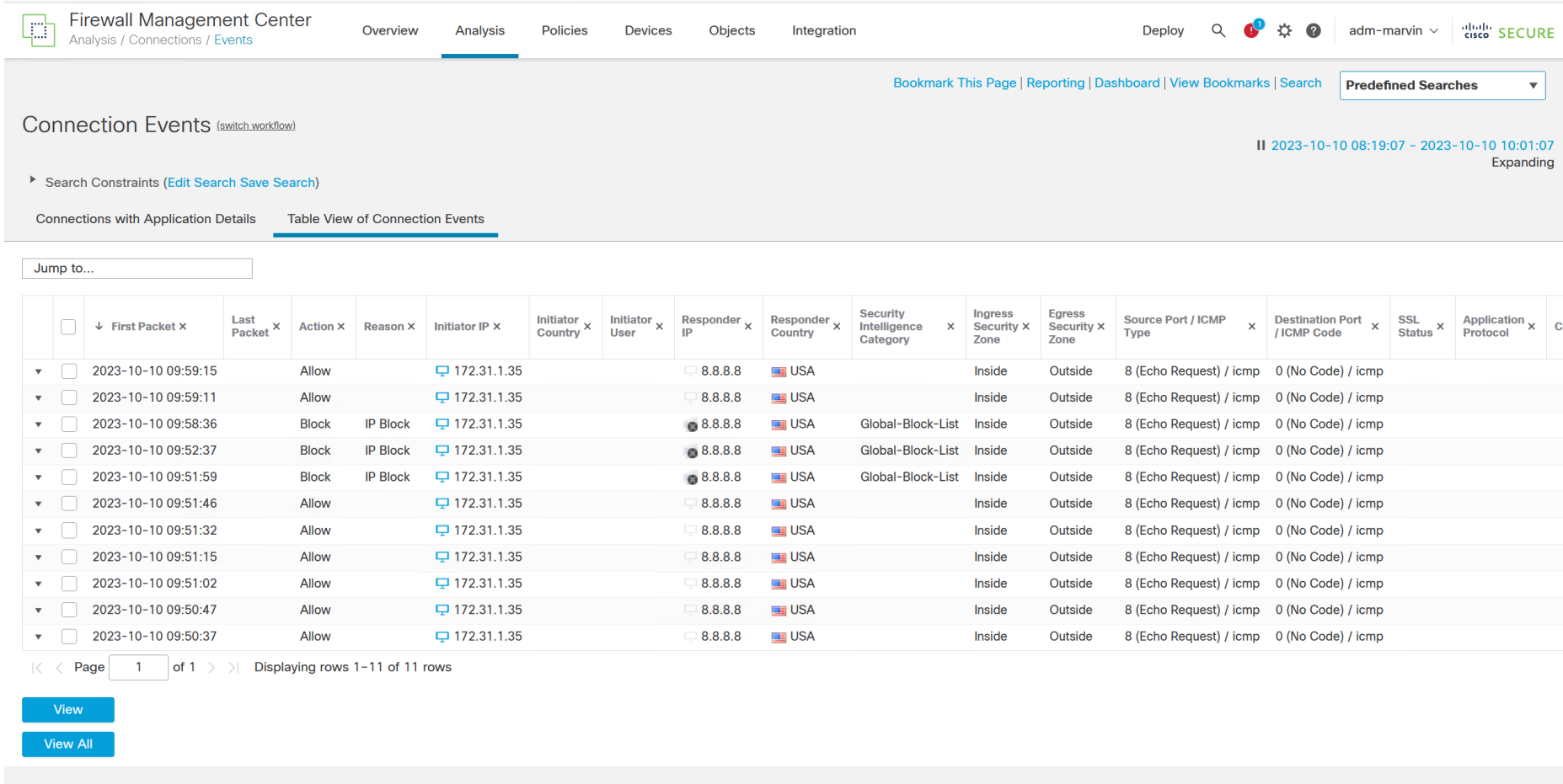
- Obuka o bezbednosti (engl. Security Awareness Training) je kontinuirani proces edukacije zaposlenih o najnovijim sajber pretnjama i najboljim praksama za zaštitu informacija.
- Cilj je podići svest o rizicima, naučiti zaposlene kako da prepoznaju phishing, BEC i druge napade, te kako da reaguju na njih.
- Obuka treba da bude interaktivna, relevantna za ulogu zaposlenog i redovno ažurirana kako bi odražavala nove pretnje.
- Uključuje simulirane phishing napade, kvizove, video materijale i radionice.
- Zaposleni su često najslabija karika u bezbednosnom lancu, pa je njihova edukacija ključna za jačanje ukupne otpornosti organizacije.
- Unapređenje 2025/2026: Personalizovane platforme za obuku koriste adaptivno učenje (engl. adaptive learning) i gamifikaciju (engl. gamification) kako bi obuka bila angažovanija i efikasnija.
- Analiza ponašanja korisnika se koristi za identifikaciju zaposlenih koji su podložniji napadima i pružanje ciljane dodatne obuke.

DoS/DDoS napadi i rast pretnji

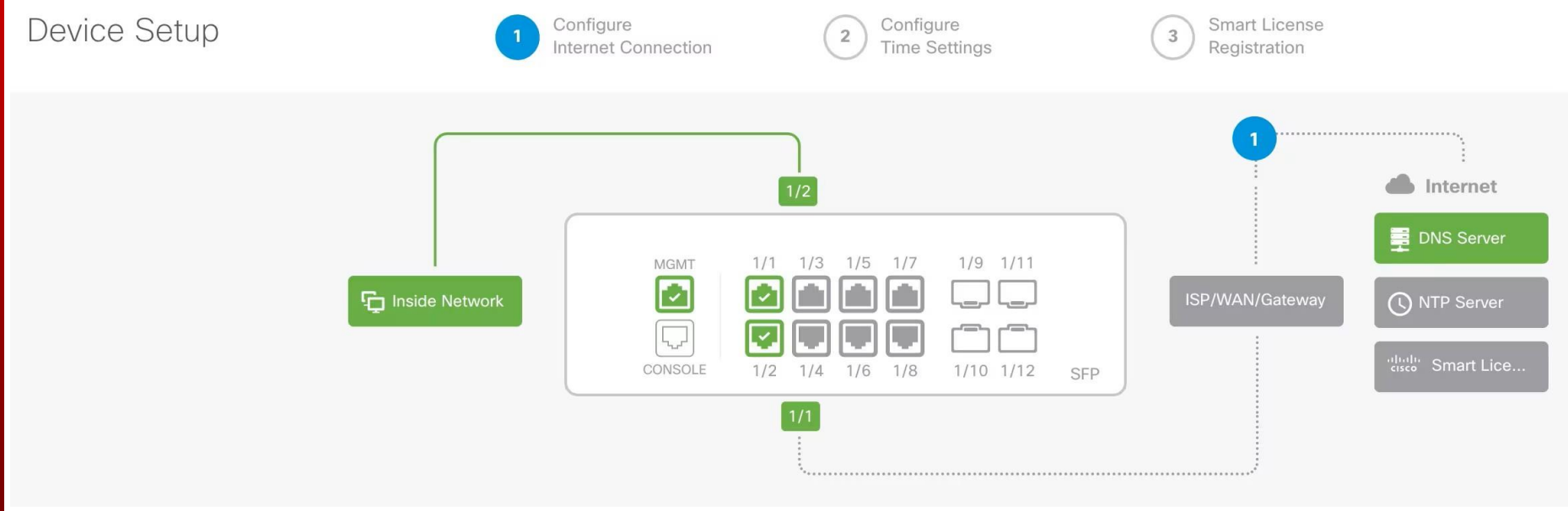
Filtriranje i blokiranje IP adresa

- Filtriranje i blokiranje IP adresa su osnovne, ali efikasne mere za ublažavanje DDoS napada.
- Kreiranje crnih lista (engl. blacklists) IP adresa poznatih napadača omogućava blokiranje njihovog saobraćaja na mrežnom gejtveju ili ruteru.
- Ove liste se mogu dinamički ažurirati na osnovu obaveštajnih podataka o pretnjama (engl. threat intelligence) u realnom vremenu.
- Međutim, napadači često menjaju izvorne IP adrese (engl. IP spoofing) ili koriste botnete sa velikim brojem adresa, što otežava statično blokiranje.
- Blokiranje celih geografskih regiona (engl. geo-blocking) sa kojih dolazi nelegitiman saobraćaj takođe može biti privremeno rešenje.
- Dinamičko filtriranje IP adresa zasnovano na ponašanju (engl. behavior-based IP filtering) pomoću veštačke inteligencije omogućava preciznije blokiranje malicioznih izvora, minimizirajući kolateralnu štetu.
- Sve veća upotreba RPKI (engl. Resource Public Key Infrastructure) protokola pomaže u verifikaciji izvornih IP adresa i smanjenju *IP spoofing*-a.

Filtriranje i blokiranje IP adresa



Filtriranje i blokiranje IP adresa

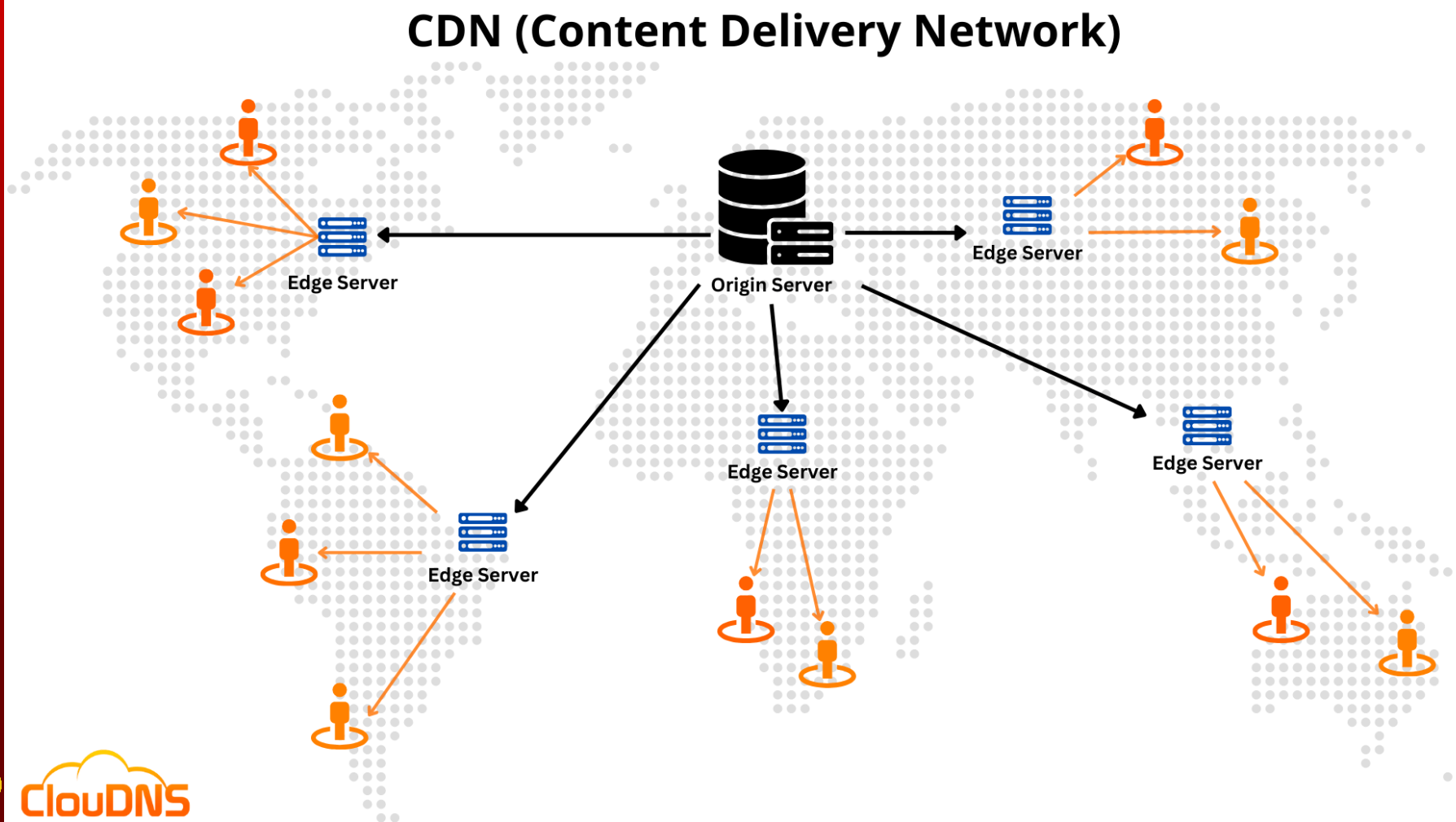


Keširanje sadržaja (Content Caching) i CDN (Content Delivery Networks)

- Keširanje sadržaja (engl. Content Caching) je tehnika skladištenja često traženih podataka bliže korisnicima radi bržeg pristupa i smanjenja opterećenja na glavnim serverima.
- Mreže za isporuku sadržaja (engl. Content Delivery Networks, CDN) su globalno distribuirane mreže servera koji keširaju statički i dinamički sadržaj veb sajtova.
- Tokom DDoS napada, CDN može apsorbovati veliki deo volumetrijskog saobraćaja, isporučujući keširani sadržaj sa svojih ivica (engl. edge servers) i tako štiteći izvorni server.
- CDN-ovi su dizajnirani sa ogromnim propusnim opsegom i mogu efikasno da skaliraju odbranu tokom napada.
- Pored zaštite, CDN-ovi poboljšavaju performanse veb sajtova i korisničko iskustvo.

CDN-ovi integrišu napredne veštačke inteligencije (AI) algoritme za detekciju anomalija i adaptivno ublažavanje DDoS napada u realnom vremenu. Edge computing (računarstvo na ivici mreže) i *serverless* funkcije (engl. serverless functions) u CDN-ovima omogućavaju sofisticiraniju logiku za filtriranje saobraćaja pre nego što stigne do centralne infrastrukture.

Keširanje sadržaja (Content Caching) i CDN (Content Delivery Networks)

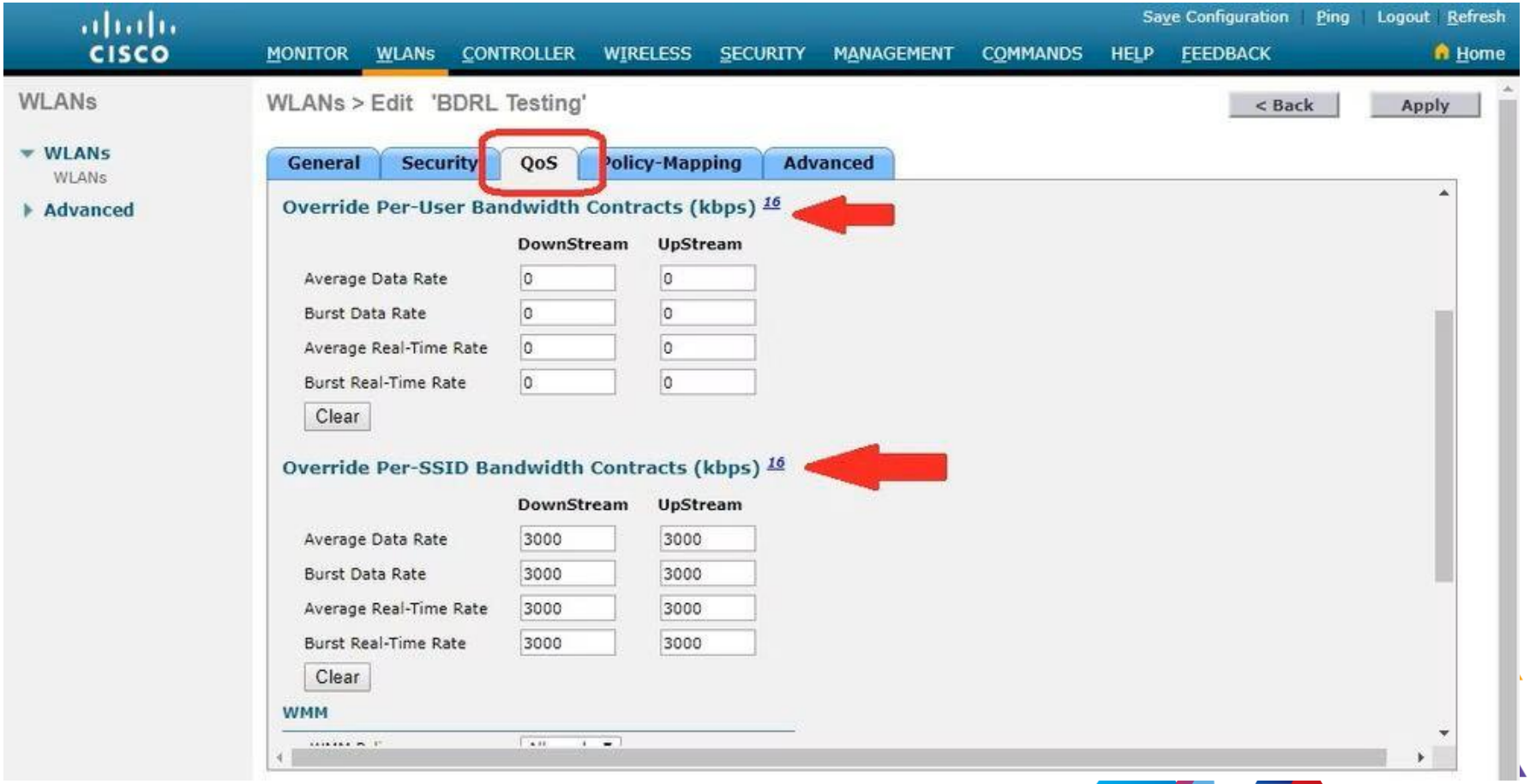


Ograničavanje stope (Rate Limiting)

- Ograničavanje stope (engl. Rate Limiting) je bezbednosna tehnika koja kontroliše broj zahteva koje klijent (ili IP adresa) može poslati serveru u određenom vremenskom periodu.
- Cilj je sprečavanje preopterećenja resursa servera ili aplikacije od strane prevelikog broja zahteva, što je česta karakteristika DDoS napada.
- Može se primeniti na različitim nivoima – na nivou mreže (za opšti saobraćaj), na nivou aplikacije (za specifične API pozive) ili na veb serveru.
- Efektivno ublažava određene vrste DoS i DDoS napada, posebno one koji se oslanjaju na veliki broj zahteva sa ograničenog broja izvora.
- Međutim, agresivno ograničavanje stope može blokirati i legitimne korisnike u trenucima visokog saobraćaja.

Dinamičko ograničavanje stope (engl. adaptive rate limiting) uz pomoć mašinskog učenja prilagođava pragove na osnovu normalnog ponašanja korisnika i detektovanih pretnji. Integracija sa sistemima za prepoznavanje botova (engl. bot detection systems) omogućava preciznije razlikovanje legitimnog saobraćaja od zlonamernih botova.

Ograničavanje stope (Rate Limiting)

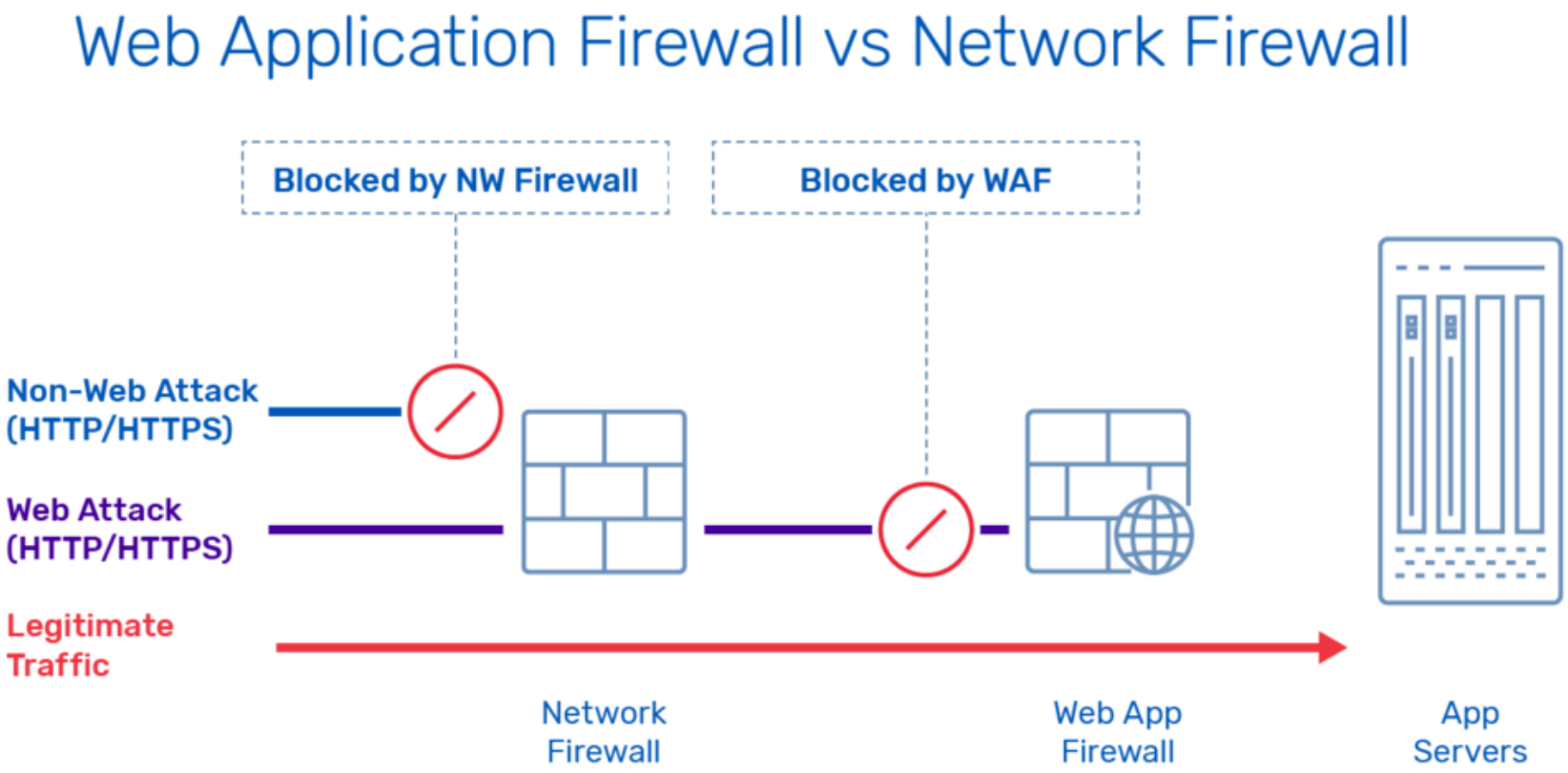


Filtriranje paketa i WAF

- Filtriranje paketa (engl. Packet Filtering) se vrši na ruterima i firewall-ima, analizirajući zaglavlja paketa (izvornu/odredišnu IP adresu, port) i odbacujući one koji ne ispunjavaju definisana pravila.
- Web Application Firewall (WAF) je specijalizovani *firewall* dizajniran da štiti veb aplikacije od napada na aplikativnom sloju (L7), uključujući SQL injekciju, XSS i DDoS napade.
- WAF analizira HTTP/HTTPS saobraćaj i može da blokira maliciozne zahteve pre nego što stignu do veb servera.
- Ključan je za zaštitu od aplikativnih DDoS napada koji oponašaju legitimne korisničke interakcije.
- WAF može da obavlja i ograničavanje stope, zaštitu od botova i filtriranje po geolokaciji.

WAF-ovi integrišu napredne veštačke inteligencije (AI) modele za analizu anomalija u HTTP saobraćaju i detekciju sofisticiranih aplikativnih napada u realnom vremenu. Cloud-native WAF rešenja pružaju fleksibilnost i skalabilnost potrebnu za dinamička okruženja.

Filtriranje paketa i WAF

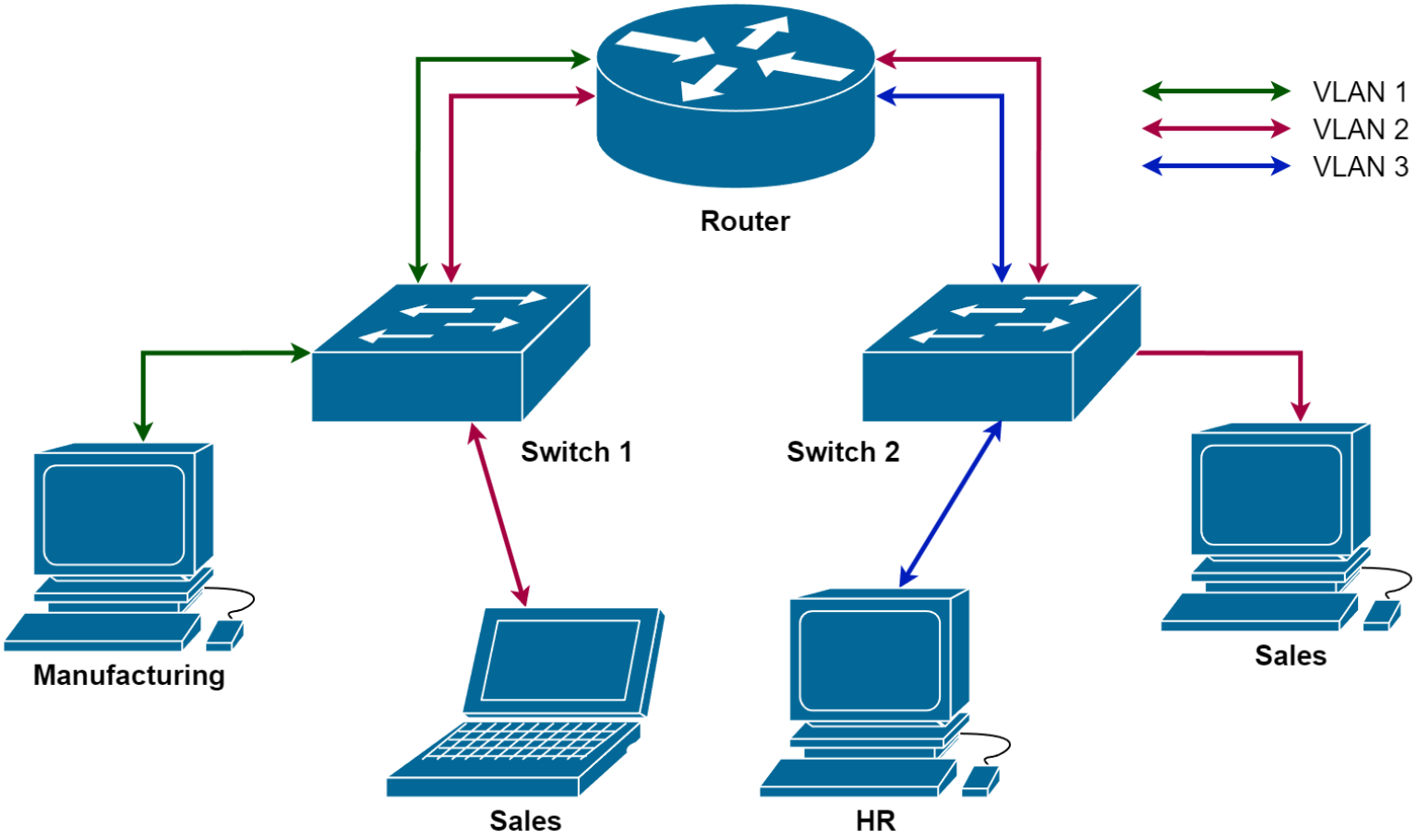


Mrežna segmentacija

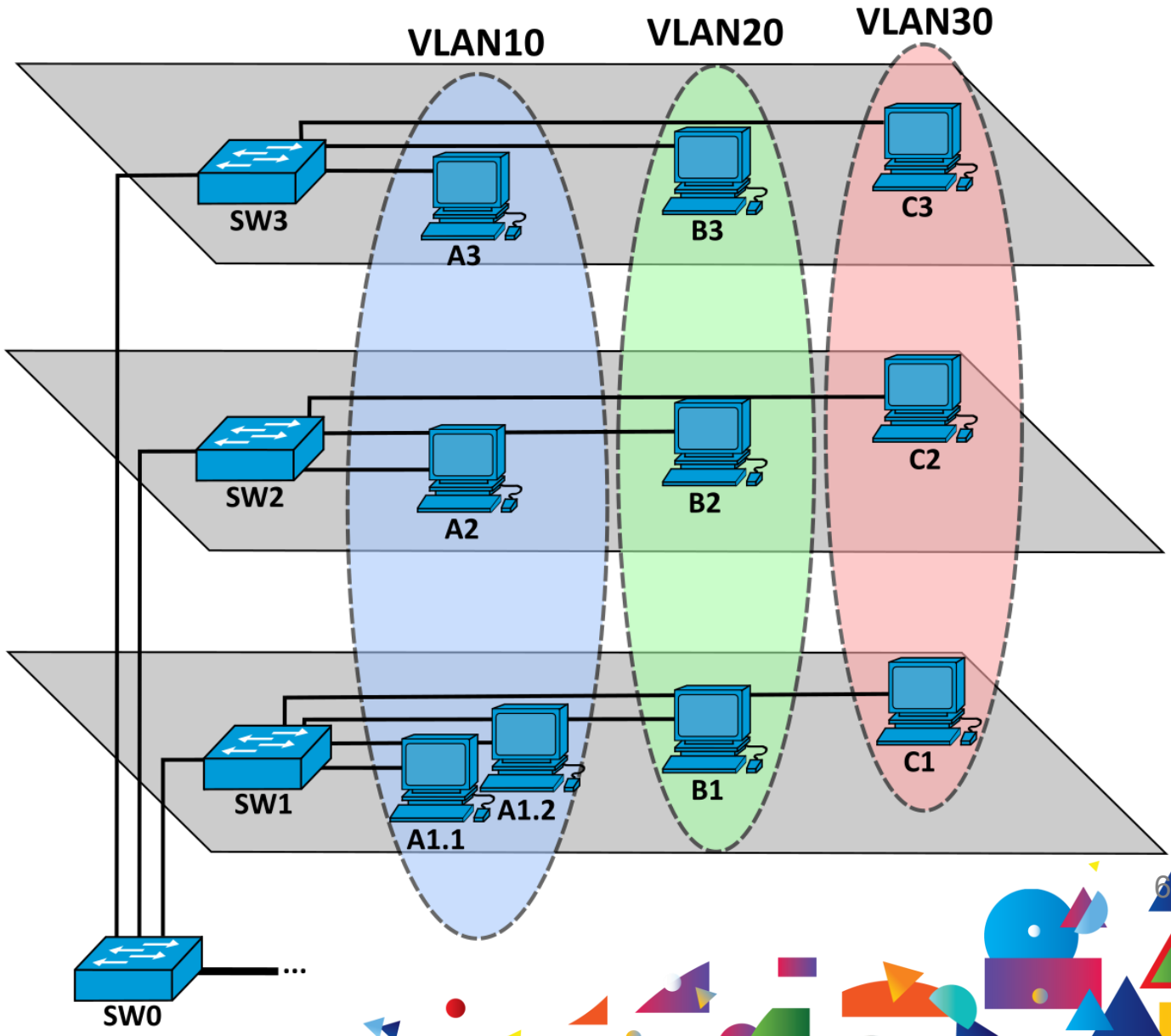
- Mrežna segmentacija (engl. Network Segmentation) podrazumeva podelu veće računarske mreže na manje, izolovane segmente (podsisteme).
- Cilj je ograničiti širenje malicioznog saobraćaja i uticaj DDoS napada samo na kompromitovani segment, štiteći ostatak infrastrukture.
- Korišćenje VLAN-ova (engl. Virtual Local Area Networks), *firewall*-ova i listi za kontrolu pristupa (engl. Access Control Lists, ACLs) za razdvajanje kritičnih sistema od javnih servisa.
- U slučaju napada, lakše je izolovati pogođeni segment bez uticaja na funkcionalnost cele organizacije.
- Mrežna segmentacija je osnovni princip "zero-trust" arhitektura (engl. zero-trust architectures) koje pretpostavljaju da se pretnje mogu pojaviti i unutar mreže.

Softverski definisano umrežavanje (engl. Software-Defined Networking, SDN) i *micro-segmentacija* postaju standard, omogućavajući dinamičku i granularnu kontrolu nad mrežnim tokovima. Automatizacija se koristi za dinamičku preraspodelu mrežnih resursa i izolaciju pogođenih segmenata tokom napada.

Mrežna segmentacija



Mrežna segmentacija



Mrežna segmentacija

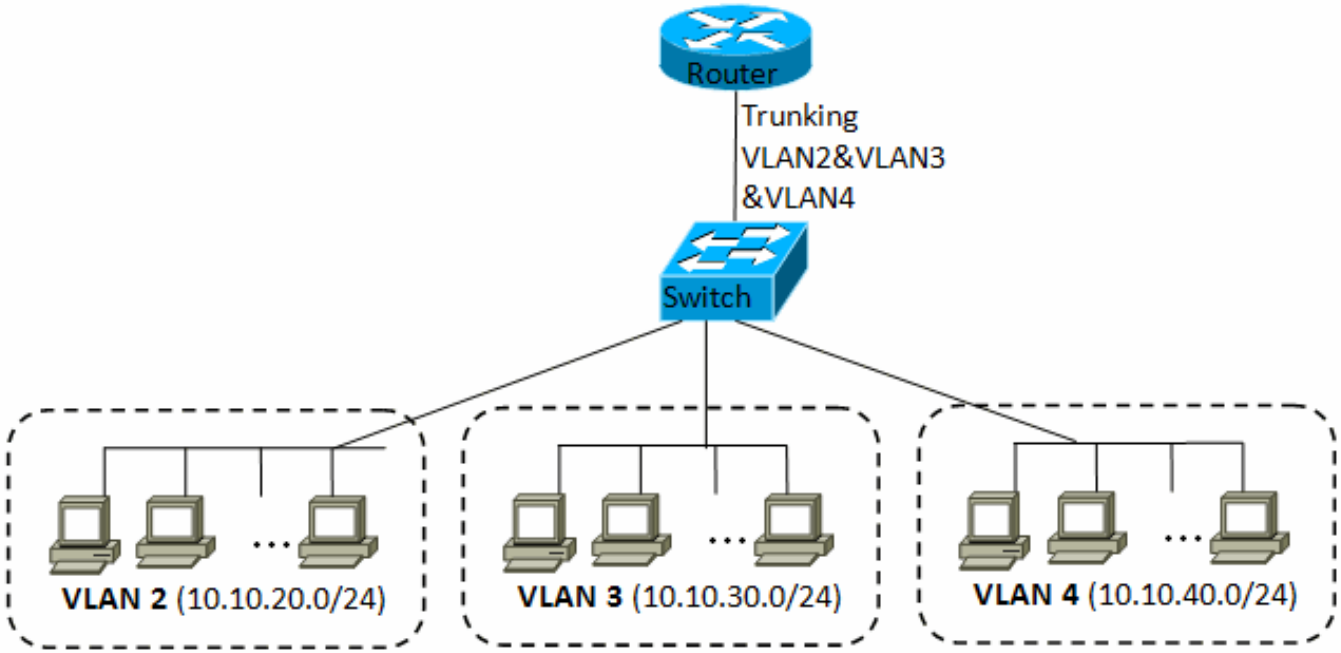


Figure 12.5. 802.1Q trunk between the router and the switch

Mrežna segmentacija

```
R1(config)#
R1(config)#ip access-list resequence OutBoundAccess 10 10
R1(config)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
    10 permit ip 192.168.1.0 0.0.0.255 any
    20 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
    30 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
    40 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
    50 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
    60 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
    70 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
    80 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
    90 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
    100 deny tcp 192.168.2.0 0.0.0.127 any eq irc
    110 permit ip 192.168.2.0 0.0.0.255 any
    120 permit ip 192.168.3.0 0.0.0.255 any
    130 permit ip 192.168.4.0 0.0.0.255 any
    140 permit ip 192.168.5.0 0.0.0.255 any
R1(config)#
R1(config)#
```

Geo-blokiranje (Geo-Blocking)

- Geo-blokiranje (engl. Geo-Blocking) je tehnika filtriranja mrežnog saobraćaja na osnovu geografske lokacije izvorne IP adrese.
- U kontekstu DDoS napada, geo-blokiranje se može koristiti za blokiranje saobraćaja iz zemalja ili regiona koji su poznati izvori napada ili sa kojima organizacija nema poslovne veze.
- Ova mera može značajno smanjiti količinu malicioznog saobraćaja koji dopire do cilja.
- Međutim, postoji rizik od blokiranja legitimnih korisnika koji se nalaze u geo-blokiranim regionima ili koriste VPN (engl. Virtual Private Network) servise.
- Geo-blokiranje se obično primenjuje na nivou *firewall*-a, WAF-a ili usluga za zaštitu od DDoS napada.

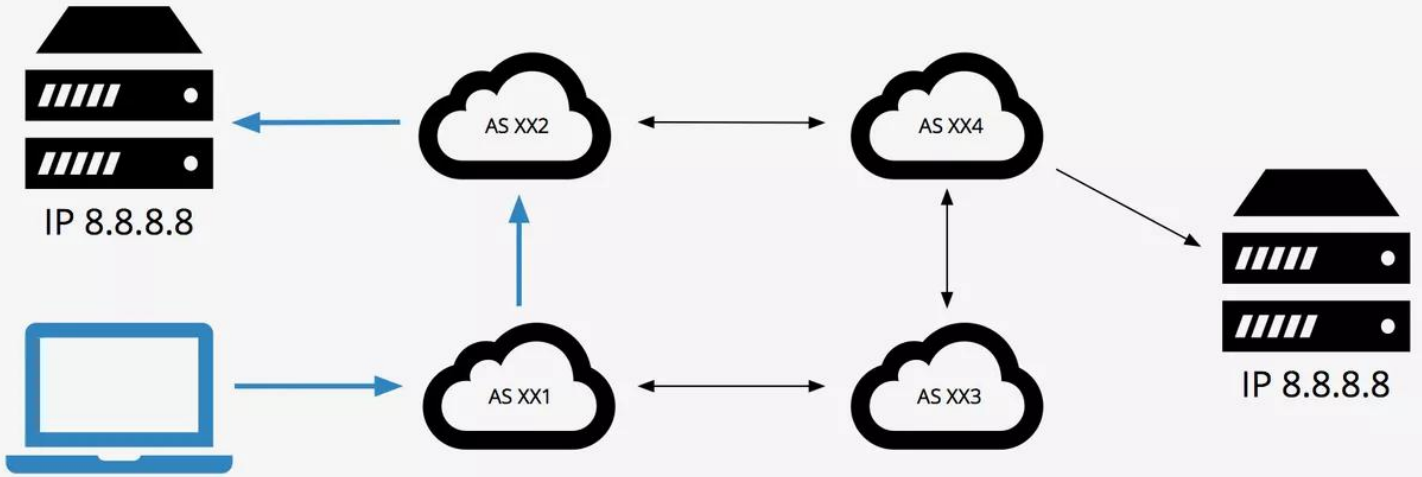
Dinamičko geo-blokiranje uz pomoć veštačke inteligencije (AI) koristi podatke o reputaciji IP adresa i obrasce saobraćaja kako bi se izbeglo blokiranje legitimnih korisnika. Integracija sa obaveštajnim podacima o globalnim pretnjama (engl. global threat intelligence) omogućava preciznije i efikasnije odluke o geo-blokiranju.

Anycast mreže i distribuirani DNS

- Anycast je mrežna tehnika rutiranja gde se isti IP prefiks (IP adresa) oglašava sa više lokacija u globalnoj mreži.
- Saobraćaj upućen Anycast IP adresi rutira se do najbliže (u smislu rutiranja) dostupne lokacije.
- U kontekstu DDoS odbrane, Anycast mreže i distribuirani DNS serveri mogu značajno ublažiti volumetrijske napade.
- DDoS saobraćaj se raspoređuje na više servera širom sveta, umesto da se koncentriše na jednu metu, čime se efektivno "razvodnjava" napad.
- Čak i ako jedan Anycast čvor bude preopterećen, ostali nastavljaju da servisiraju legitimne korisnike.

Korišćenje Anycast mreža sa AI algoritmima za optimizaciju rutiranja saobraćaja i dinamičko preusmeravanje tokom napada. Integracija sa "zero-trust" mrežnim arhitekturama za poboljšanu otpornost distribuiranih servisa.

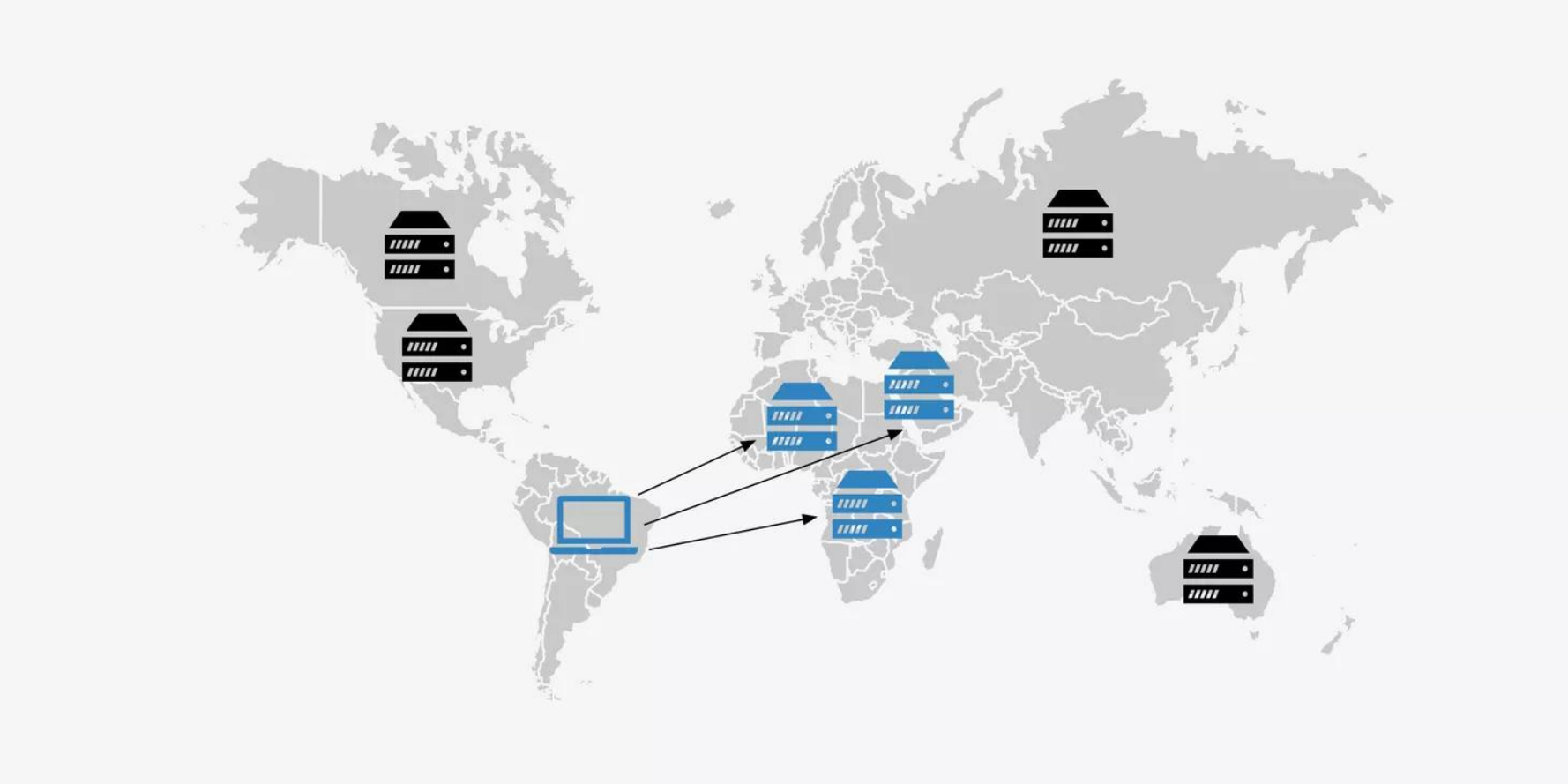
Anycast mreže i distribuirani DNS



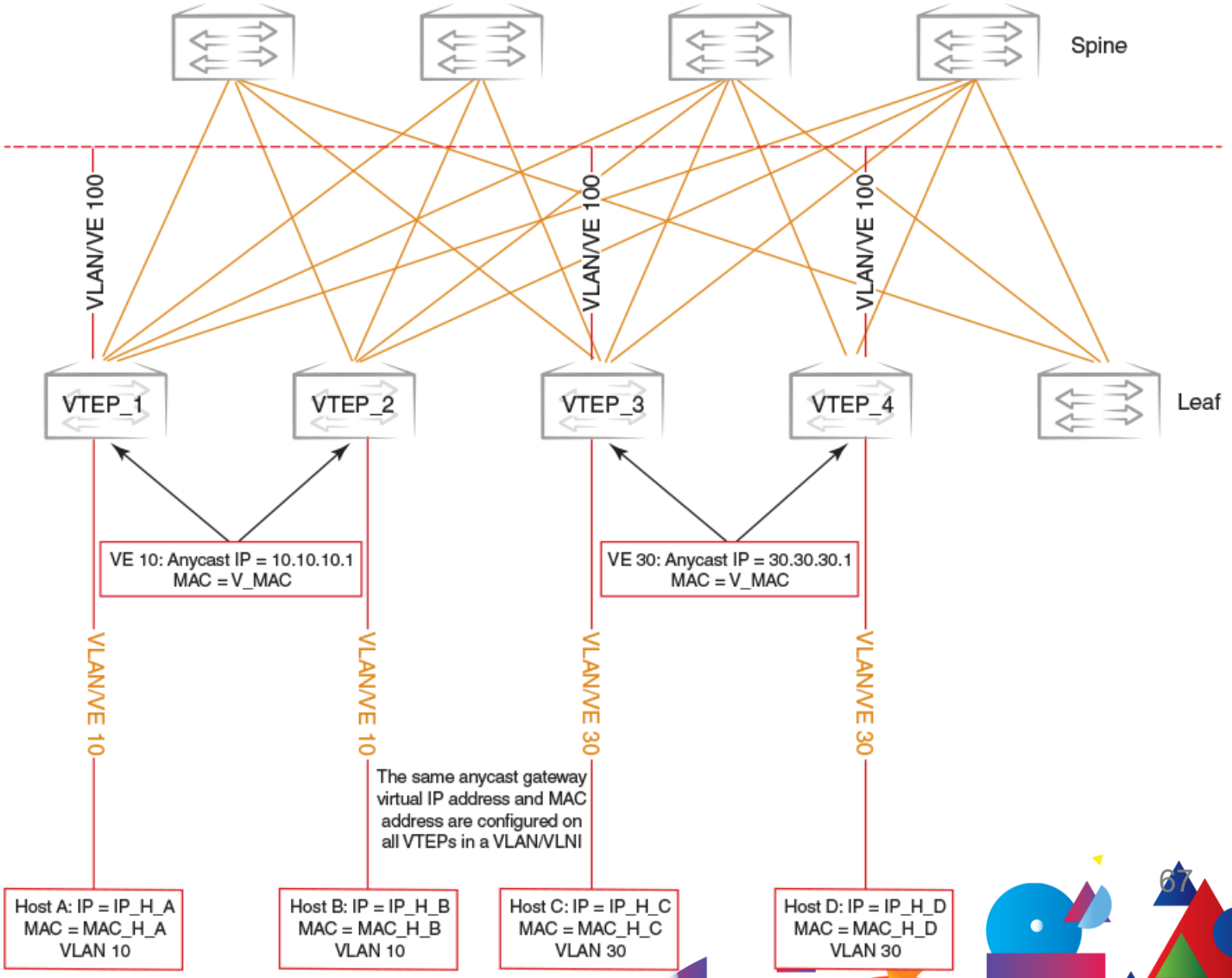
Anycast

Shortest Path: 8.8.8.8 AS path xx1 xx2
8.8.8.8 AS path xx1 xx3 xx4
8.8.8.8 AS path xx1 xx2 xx4
8.8.8.8 AS path xx1 xx3 xx4 xx2

Anycast mreže i distribuirani DNS



Anycast mreže i distribuirani DNS



Oporavak i kontinuitet poslovanja

- Planovi za oporavak od katastrofa (engl. Disaster Recovery, DR) i kontinuitet poslovanja (engl. Business Continuity, BC) su ključni za ublažavanje dugoročnih posledica DDoS napada.
- DR plan definiše korake za oporavak IT infrastrukture i podataka nakon velikog incidenta (uključujući DDoS), dok BC plan osigurava da kritične poslovne funkcije mogu nastaviti sa radom.
- Uključuje redovno kreiranje rezervnih kopija podataka, uspostavljanje redundantnih sistema i lokacija, kao i definisanje procedura za *failover* i *fallback*.
- Testiranje ovih planova kroz simulacije je od vitalnog značaja za proveru njihove efikasnosti i obuku tima.
- Cilj je minimizirati vreme zastoja (engl. downtime) i gubitak podataka, te osigurati otpornost organizacije na poremećaje.

Automatizovani DR i BC planovi, podržani veštačkom inteligencijom, omogućavaju brži i efikasniji oporavak, sa minimalnom ljudskom intervencijom. Sve veća upotreba *cloud-based* rešenja za DRaaS (engl. Disaster Recovery as a Service) omogućava fleksibilnost i skalabilnost.

Forenzička analiza nakon DDoS napada

- Forenzička analiza (engl. Forensic Analysis) nakon DDoS napada je proces prikupljanja, očuvanja i analize digitalnih dokaza kako bi se razumeo napad.
- Cilj je identifikovati izvor napada, korišćene vektore, obim štete i, ako je moguće, identitet napadača.
- Uključuje analizu mrežnih logova, saobraćaja (PCAP), sistemskih logova i drugih relevantnih podataka.
- Dobijeni podaci su ključni za jačanje odbrane, unapređenje bezbednosnih politika i, u nekim slučajevima, za pravne radnje.
- Oporavak i analiza su poslednje faze plana reagovanja na incidente.

AI alati za forenzičku analizu mogu brže da procesuiraju i korelišu ogromne količine podataka, automatski identifikujući ključne indikatore kompromitacije (engl. Indicators of Compromise, IoCs). Integracija sa platformama za obaveštavanje o pretnjama (engl. Threat Intelligence Platforms) obogaćuje forenzičke podatke kontekstom o poznatim napadačkim grupama i tehnikama.

Uloga internet provajdera (ISP) u DDoS zaštiti

- Internet provajderi (engl. Internet Service Providers, ISP) igraju ključnu ulogu u zaštiti svojih korisnika od DDoS napada zbog svoje pozicije u mrežnoj hijerarhiji.
- Oni imaju mogućnost da detektuju i ublaže velike volumetrijske napade mnogo pre nego što saobraćaj stigne do mreže klijenta.
- Mnogi ISP-ovi nude usluge zaštite od DDoS napada (engl. DDoS mitigation services) kao deo svojih ponuda.
- Primenjuju tehnike poput filtriranja izvornih IP adresa (engl. BCP 38), *blackholing*-a i usmeravanja saobraćaja kroz svoje "scrubbing" centre.
- Saradnja između organizacija i njihovih ISP-ova je ključna za efikasno reagovanje na velike napade.

ISP-ovi sve više koriste SDN (engl. Software-Defined Networking) za dinamičku alokaciju resursa i brzo preusmeravanje saobraćaja tokom napada. AI-pokretana analiza saobraćaja na ivici mreže omogućava ISP-ovima da detektuju i ublaže napade na ranijim fazama.

DDoS zaštita za specifične aplikacije

- Pored generičke mrežne zaštite, specifične aplikacije zahtevaju ciljane mere zaštite od DDoS napada.
- Napadi na aplikativnom sloju (Layer 7) su posebno opasni jer oponašaju legitimne korisničke interakcije i mogu biti teški za detekciju.
- Rešenja uključuju WAF (engl. Web Application Firewall), API gejtveje (engl. API Gateways) sa ograničavanjem stope i napredne sisteme za prepoznavanje botova.
- Optimizacija performansi aplikacije, kao što je efikasno korišćenje baze podataka i keširanje, takođe može pomoći u apsorbovanju opterećenja.
- Primena *captcha* testova (engl. CAPTCHA) može delimično ublažiti neke bot-bazirane napade.

AI analiza ponašanja korisnika (engl. User Behavior Analytics, UBA) integriše se u aplikativnu zaštitu kako bi se razlikovali legitimni korisnici od sofisticiranih botova. *Serverless* arhitekture (engl. serverless architectures) i mikrousluge (engl. microservices) mogu poboljšati otpornost aplikacija na DDoS napade kroz inherentnu skalabilnost i izolaciju komponenti.

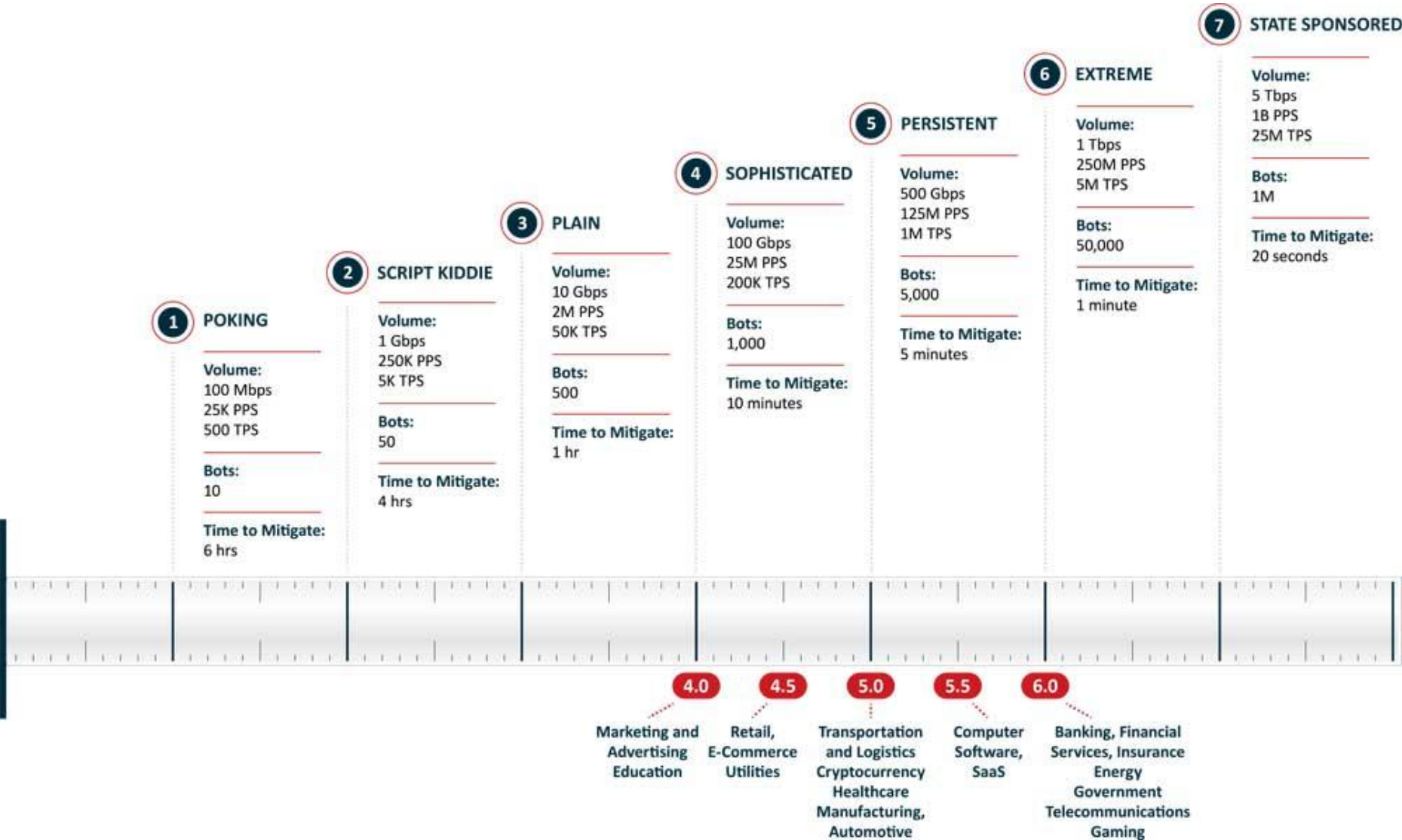
Zaštita DNS infrastrukture od DDoS napada

- DNS (engl. Domain Name System) infrastruktura je kritična meta za DDoS napade, jer je ključna za funkcionisanje interneta.
- Napad na DNS servere može učiniti veb sajtove i usluge nedostupnim, čak i ako su sami serveri aplikacija ispravni.
- Mere zaštite uključuju distribuirane DNS arhitekture sa više lokacija (Anycast), redundansu servera i korišćenje specijalizovanih DNS provajdera sa DDoS zaštitom.
- Implementacija DNSSEC-a (engl. Domain Name System Security Extensions) pomaže u sprečavanju DNS *spoofing*-a i trovanja keša (engl. cache poisoning).
- Ograničavanje stope DNS upita (engl. DNS query rate limiting) može sprečiti preopterećenje servera prevelikim brojem zahteva.
- AI se koristi za predviđanje i ublažavanje DNS DDoS napada analizom globalnog DNS saobraćaja i prepoznavanjem anomalija. Decentralizovane DNS rešenja zasnovana na blokčejnu (engl. blockchain-based DNS) istražuju se kao buduća alternativa za poboljšanu otpornost.

Testiranje DDoS otpornosti

- Testiranje DDoS otpornosti (engl. DDoS Resilience Testing) je proces simulacije DDoS napada na sopstvenu infrastrukturu.
- Cilj je proceniti sposobnost sistema, mreže i procedura da izdrže napad i utvrditi slabosti pre nego što ih iskoriste stvarni napadači.
- Izvodi se u kontrolisanom okruženju, često uz pomoć specijalizovanih firmi ili platformi koje simuliraju različite tipove napada.
- Rezultati testiranja pomažu u optimizaciji konfiguracije, jačanju odbrane i obuci tima za reagovanje na incidente.
- Važno je sprovoditi testiranja redovno, jer se infrastruktura i pretnje kontinuirano razvijaju.

Testiranje DDoS otpornosti



Obaveštavanje o pretnjama za DDoS

- Obaveštavanje o pretnjama (engl. Threat Intelligence) pruža proaktivne informacije o najnovijim DDoS vektorima, botnetima, napadačkim grupama i njihovim taktikama.
- Prikupljaju se podaci iz različitih izvora, uključujući javne baze podataka, bezbednosne vendore, forume i vlastitu analizu.
- Ove informacije pomažu organizacijama da unaprede svoje bezbednosne sisteme, prilagode pravila *firewall*-a i WAF-a, i razviju efikasnije strategije ublažavanja.
- Deljenje obaveštajnih podataka unutar industrije i sa bezbednosnim zajednicama je ključno za kolektivnu odbranu.
- Uključuje informacije o C2 (Command and Control) serverima, listama kompromitovanih IP adresa i domenima.

Univerzitet Singidunum

Pitanja?
Diskusija.
Savremeni pravci istraživanja.

Hvala na pažnji

Ova prezentacija je nekomercijalna.

Slajdovi mogu da sadrže materijale preuzete sa Interneta, stručne i naučne građe, koji su zaštićeni Zakonom o autorskim i srodnim pravima.

Ova prezentacija se može koristiti samo privremeno tokom usmenog izlaganja nastavnika u cilju informisanja i upućivanja studenata na dalji stručni, istraživački i naučni rad i u druge svrhe se ne sme koristiti –

Član 44 - Dozvoljeno je bez dozvole autora i bez plaćanja autorske naknade za nekomercijalne svrhe nastave:

(1) javno izvođenje ili predstavljanje objavljenih dela u obliku neposrednog poučavanja na nastavi;

- ZAKON O AUTORSKOM I SRODNIM PRAVIMA ("Sl. glasnik RS", br. 104/2009 i 99/2011)

Nikola Savanović – nsavanovic@singidunum.ac.rs