
VODIČ
ZA MREŽNU
SEGMENTACIJU
Net++ technology

SADRŽAJ

SADRŽAJ

UVOD

Mrežna segmentacija predstavlja strategiju za organizaciju i zaštitu mreže kroz razdvajanje uređaja, aplikacija i korisnika u izolovane segmente.

Ovi segmenti, poznati i kao bezbednosne zone, funkcionišu kao odvojene „mreže unutar mreže“, omogućavajući vam kontrolisanje pristupa između različitih delova mreže. Ova izolacija drastično smanjuje rizik od neovlašćenog pristupa i širenja zlonamernog softvera u slučaju napada.

Zašto je mrežna segmentacija ključna za sajber bezbednost?

Mrežna segmentacija povećava sajber bezbednost tako što umanjuje šanse da napadači napreduju kroz sistem

ako inicijalno dobiju pristup delu mreže.

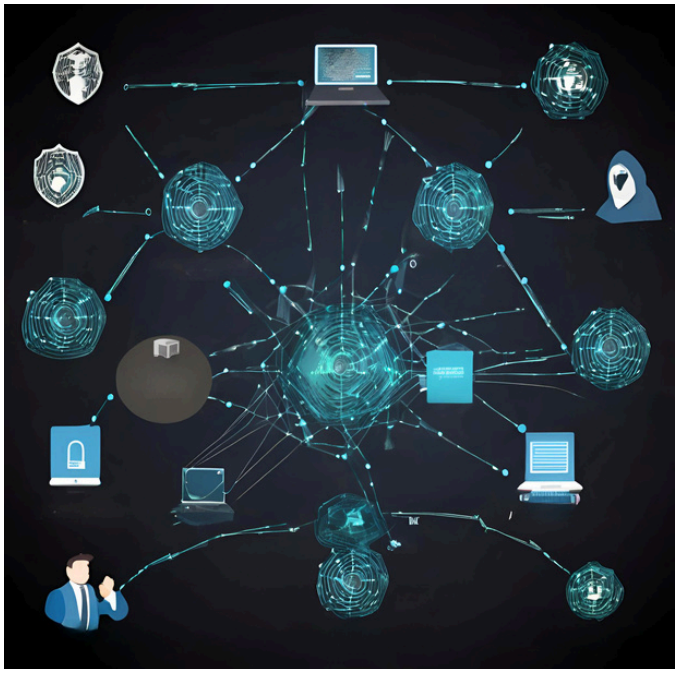
Na primer, ako su kritične baze podataka smeštene u zasebnoj zoni sa strogo kontrolisanim pristupom, mnogo je teže da napadač koji se infiltrira u deo mreže s manjom bezbednosnom zaštitom (npr. mrežu posetilaca ili zaposlenih) pristupi osetljivim informacijama.

Prednosti segmentacije:

- **Smanjuje rizik od lateralnog kretanja napadača:** U slučaju kompromitovanja, napadač će naići na prepreke u pokušaju prelaska iz jednog segmenta u drugi.
- **Poboljšava kontrolu pristupa:** Omogućava vam da postavite različite polise pristupa za svaku zonu, čime se preciznije kontroliše ko može pristupiti određenim resursima.
- **Ograničava širenje zlonamernog softvera:** Ako malver uđe u jedan deo mreže, segmentacija ograničava njegov pristup drugim zonama, smanjujući potencijalnu štetu.

Primer iz prakse:

U zdravstvenoj ustanovi, segmentacija može odvojiti medicinsku opremu povezanu na mrežu od sistema sa podacima pacijenata. U slučaju kompromitovanja IoT uređaja, napadač ne bi mogao direktno pristupiti osetljivim medicinskim podacima.



Kako funkcioniše mrežna segmentacija?

Mrežna segmentacija se postiže pomoću različitih tehnologija, među kojima su najčešće:

- VLAN-ovi (Virtual Local Area Networks),
- Firewall uređaji i
- Access Control List (ACL) pravila
- Software-Defined Networking (SDN).

Korišćenjem ovih alata, administratori mogu postaviti specifične polise koje regulišu koje zone ili uređaji imaju pristup određenim resursima i aplikacijama unutar mreže.

Na primer, možete postaviti da finansijska zona ima pristup računovodstvenim serverima, ali ne i aplikacijama koje koristi razvojni tim.

RAZUMEVANJE MREŽNOG SAOBRAĆAJA

Da biste uspešno segmentirali mrežu, ključno je razumeti koji uređaji i korisnici komuniciraju međusobno i sa spoljnim resursima.

Ova analiza omogućava identifikaciju kritičnih tačaka mreže i pomaže u identifikaciji koji delovi mreže mogu biti odvojeni radi boljeg upravljanja bezbednošću.

Analiza mrežnog saobraćaja je ključna za efikasnu segmentaciju jer omogućava:

1. Identifikaciju kritičnih tačaka mreže
2. Razumevanje obrazaca komunikacije između uređaja
3. Otkrivanje potencijalnih bezbednosnih pretnji

Alati

Wireshark, ManageEngine OpManager, SolarWinds NetFlow Traffic Analyzer, Nagios

Ciljevi analize saobraćaja:

- Identifikacija uređaja koji najčešće komuniciraju jedni s drugima.
- Prepoznavanje servisa i protokola koji su ključni za poslovanje.
- Razumevanje obrasca dolaznog i odlaznog saobraćaja, što je ključno za identifikaciju pretnji.

Identifikacija uređaja i servisa na mreži

Mreža u srednje velikim kompanijama često sadrži uređaje poput računara, servera, mobilnih uređaja, IoT uređaja i specijalizovanih uređaja (npr. POS sistemi).
Razumevanje njihovih funkcija pomaže u pravilnom grupisanju, što dalje olakšava kontrolu pristupa.

Koraci za identifikaciju uređaja i servisa:

1. **Izvršite mrežni sken:** Koristite alate kao što su Nmap ili Advanced IP Scanner da identifikujete sve aktivne uređaje na mreži.
2. **Kategorizujte uređaje:** Grupisanje uređaja prema funkciji i vlasništvu (npr. korisnički uređaji, serverska oprema, IoT uređaji).
3. **Mapirajte servise i protokole:** Uočite koji servisi i protokoli (npr. HTTP, HTTPS, FTP) su u upotrebi i u kojoj meri su neophodni za poslovanje.

Ova klasifikacija pomaže pri definisanju bezbednosnih zona i planiranju pravila pristupa koja će obezbediti da svaka grupa uređaja ima odgovarajući nivo zaštite.

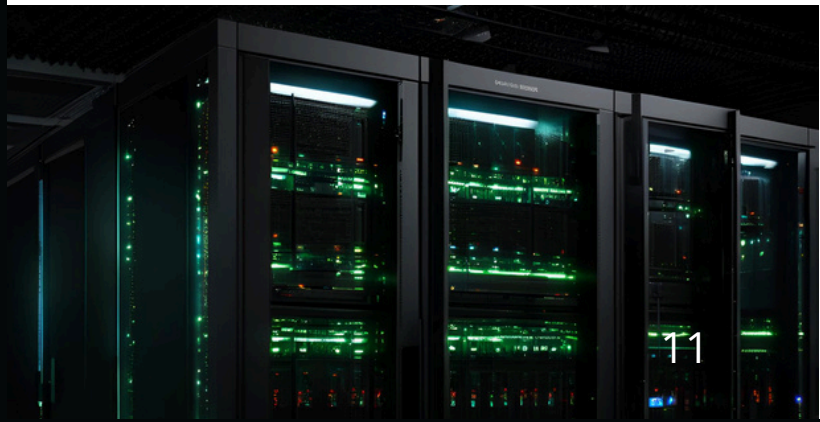
Kritična infrastruktura i određivanje prioriteta

U svakoj mreži postoje kritični uređaji ili servisi koji zahtevaju posebnu pažnju, kao što su finansijski serveri, baze podataka s osetljivim informacijama, ili uređaji koji kontrolišu važne procese (npr. proizvodna oprema). Segmentacija omogućava da se ovi sistemi dodatno zaštite postavljanjem u odvojene, posebno osigurane zone.

Kriterijumi za identifikaciju kritičnih uređaja:

- **Osetljivost podataka:** Baze podataka koje sadrže poverljive informacije.
- **Poslovna zavisnost:** Uređaji ili servisi čiji gubitak značajno utiče na poslovanje.
- **Pristup internetu:** Sistemi koji direktno komuniciraju sa internetom i podložni su višem riziku od napada.

Segmentacija ključnih resursa pruža dodatni sloj zaštite i omogućava brži odgovor u slučaju napada.



Dokumentacija i mapa mrežnog saobraćaja

Precizna dokumentacija svih uređaja, servisa, i pravaca mrežnog saobraćaja je osnovna za planiranje segmentacije. Kreiranjem mape mrežnog saobraćaja, IT tim dobija vizuelni prikaz mrežne strukture, čime postaje lakše definisati bezbednosne zone i implementirati pravila pristupa.

Šta uključiti u dokumentaciju?

- Listu svih uređaja sa IP adresama
- Tip uređaja, uloga, i vlasništvo
- Prikaz povezanosti između uređaja i učestalosti komunikacije.

Koristani alati:

U skeniranju i dokumentovanju uređaja vam mogu pomoći **ManageEngine AssetManager Plus** ili **ServiceDesk Plus** koji imaju ugrađene ove mogućnosti.

Takođe, čak i jednostavni alati kao što su Excel ili Google Sheets mogu pomoći u kreiranju i održavanju ove dokumentacije.

Razumevanje mrežnog saobraćaja i identifikacija uređaja predstavljaju osnovne korake u procesu segmentacije mreže. Sa dobro definisanim pregledom uređaja i njihovih komunikacionih veza, postavljaju se temelji za bezbedniju i efikasniju mrežnu arhitekturu.

DEFINISANJE BEZBEDNOSNIH ZONA I POLISA PRISTUPA

Bezbednosne zone su logički segmenti unutar mreže koji obuhvataju grupe uređaja i korisnika sa sličnim bezbednosnim potrebama.

Različite zone omogućavaju da se primene specifična pravila pristupa, čime se smanjuje rizik od neovlašćenog pristupa i napredovanja napadača kroz mrežu.

Primeri uobičajenih bezbednosnih zona:

- **Kancelarijska zona:** Uključuje radne stanice, štampače i računare zaposlenih.
- **Serverska zona:** Sadrži kritične poslovne servere i baze podataka.
- **IoT zona:** Obuhvata sve IoT uređaje kao što su kamere, senzori i druge pametne komponente.
- **Demilitarizovana zona (DMZ):** Ova zona je posebno važna za servere koji su dostupni sa interneta, kao što su web serveri i mail serveri.

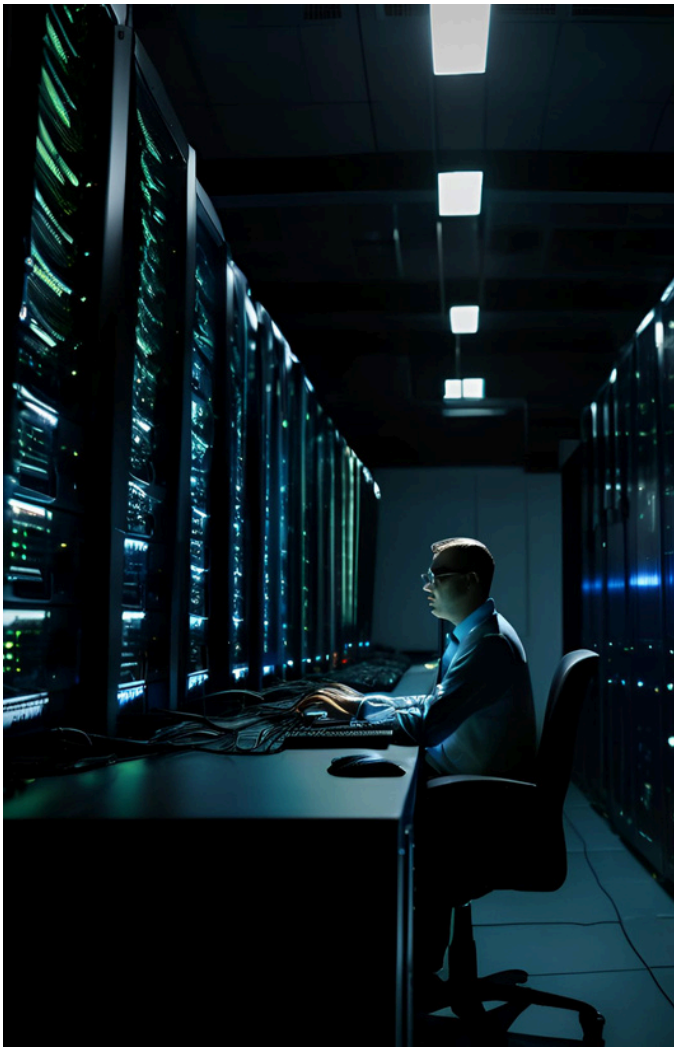
Segmentisanjem mreže na ovaj način smanjuje se šansa za neovlašćeni pristup osetljivim resursima i omogućava lakše praćenje bezbednosnih događaja u specifičnim zonama.

Formulacija pravila pristupa za svaku zonu

Nakon što su zone definisane, sledeći korak je postavljanje kontrolisanih pravila pristupa koja uređuju komunikaciju između zona i unutar svake zone. Ova pravila jasno definišu koji uređaji, korisnici, ili aplikacije imaju dozvoljen pristup specifičnim resursima i uslugama.

Ključna pravila pristupa između zona:

1. **Princip najmanjeg pristupa**: Obezbedite da svaki uređaj ili korisnik ima samo minimum neophodnih prava za obavljanje svog posla.
2. **Kontrola komunikacije između zona**: Na primer, radne stanice u kancelarijskoj zoni možda neće imati direktan pristup kritičnim serverima u serverskoj zoni bez dodatne autentifikacije.
3. **Ograničavanje pristupa internetu**: U zavisnosti od zone, pristup internetu može biti limitiran, posebno u IoT i proizvodnim zonama.



Primeri polisa:

Zona izvora	Zona odredišta	Dozvoljeni protokoli	Komentar
Kancelarijska	Serverska	HTTP, HTTPS	Pristup web aplikacijama
IoT	Serverska	MQTT	Komunikacija sa IoT platformom
DMZ	Internet	HTTP, HTTPS, DNS	Ograničen izlazni saobraća

Najbolje prakse za postavljanje polisa pristupa

Prilikom postavljanja polisa pristupa, postoje opšte smernice koje mogu pomoći u osiguravanju da segmentacija bude efikasna i bezbedna:

- **Koristite identifikaciju i autentifikaciju korisnika:** Obezbedite da su svi korisnici koji pristupaju osetljivim zonama prethodno autentifikovani i autorizovani.
- **Implementirajte dvofaktorsku autentifikaciju (2FA):** Posebno za pristup kritičnim resursima.
- **Kontinuirano pratite i prilagođavanje pravila:** Pristup pravilima bi trebalo redovno ažurirati kako se mreža menja, uključujući uklanjanje zastarelih uređaja ili korisnika.
- **Pratite i analizirajte saobraćaj unutar zona:** Kontrola saobraćaja omogućava brzo otkrivanje neuobičajenih aktivnosti, koje mogu biti signal napada.

Definisanje zona i polisa pristupa predstavlja ključni deo procesa segmentacije mreže. Pažljivim planiranjem i kontrolisanjem pristupa između različitih delova mreže, organizacije mogu efikasnije zaštititi osetljive podatke i sisteme, smanjujući šanse za napad i potencijalnu štetu.

Alati za upravljanje pristupom i segmentacijom

Postoje mnogi alati koji mogu pomoći u postavljanju i upravljanju pravilima pristupa između zona:

- Firewall uređaji: Omogućavaju granularnu kontrolu saobraćaja između različitih zona.
- Network Access Control (NAC): Ovaj alat može dodatno osigurati da samo autorizovani uređaji pristupaju specifičnim zonama.
- Identity and Access Management (IAM) sistemi: Koriste se za upravljanje identi-tetima i autentifikaciju korisnika i uređaja.

Primer:

Palo Alto Networks firewall može biti konfigurisan da segmentira saobraćaj između zona, dok NAC uređaj dodatno omogućava kontrolu nad uređajima koji pristupaju mreži, osiguravajući da samo provereni uređaji imaju dozvoljen pristup kritičnim zonama.

PRIMENA VLAN-OVA ZA LOGIČKU IZOLACIJU UNUTAR MREŽE

VLAN-ovi su tehnologija koja omogućava logičku segmentaciju mreže, omogućavajući administratorima da fizičku mrežu podele na manje podmreže bez obzira na stvarni fizički raspored uređaja.

To znači da uređaji unutar jedne mreže mogu biti grupisani u različite segmente (VLAN-ove) na osnovu funkcije, odeljenja ili bezbednosnih zahteva.

Primer VLAN konfiguracije:

- **VLAN 10:** Poslovna mreža za zaposlene (192.168.10.0/24)
- **VLAN 20:** Proizvodna mreža koja sadrži IoT uređaje (192.168.20.0/24)
- **VLAN 30:** Gostujuća mreža za posetioce (192.168.30.0/24)
- **VLAN 40:** Administrativna mreža sa kontrolisanim pristupom do ključnih servera (192.168.40.0/24)

Prednosti korišćenja VLAN-ova za segmentaciju

Korišćenje VLAN-ova donosi brojne prednosti kada je u pitanju upravljanje mrežom i bezbednost:

- **Logička izolacija:** VLAN-ovi omogućavaju logičku izolaciju bez fizičkih promena na mreži.
- **Lakše upravljanje pristupom:** Pravila pristupa mogu biti definisana za svaki VLAN, što pomaže u preciznijoj kontroli saobraćaja.
- **Smanjenje rizika od napada:** U slučaju kompromitovanja jednog VLAN-a, napadač neće moći lako da pristupi drugim zonama.
- **Fleksibilnost:** VLAN-ovi omogućavaju brzo pregrupisanje uređaja bez potrebe za fizičkim premeštanjem ili promenama.

Primer iz prakse: Kompanija može kreirati posebne VLAN-ove za različite poslovne jedinice, omogućavajući tako kontrolisani pristup zajedničkim resursima, kao što su fajl serveri, dok se istovremeno onemogućava pristup osetljivim bazama podataka.

Koraci za implementaciju VLAN-ova

1. **Identifikujte potrebe za segmentacijom:** Procena poslovnih jedinica i aplikacija koje bi mogle imati koristi od logičke izolacije.
2. **Dodelite IP opsege za svaki VLAN:** Na primer, VLAN 10 (poslovna mreža) može koristiti opseg 192.168.10.0/24, dok će VLAN 20 (IoT mreža) koristiti opseg 192.168.20.0/24.
3. **Konfigurišite switch uređaje:** Postavite VLAN-ove na mrežnim uređajima tako da svaki port switcha bude dodeljen specifičnom VLAN-u ili postavljen na trunk mod, ako je potrebno više VLAN-ova na jednom portu.
4. **Testirajte izolaciju između VLAN-ova:** Proverite da uređaji u različitim VLAN-ovima ne mogu međusobno komunicirati osim u slučajevima gde su pravila pristupa postavljena.
5. **Primena i praćenje:** Nakon implementacije, pratite saobraćaj i prilagođavajte pravila pristupa prema poslovnim potrebama i bezbednosnim rizicima.

Pristup između VLAN-ova: Primena rutiranja i pravila pristupa

Iako VLAN-ovi obezbeđuju logičku izolaciju, postoji mogućnost da se omogući komunikacija između određenih VLAN-ova kada je to potrebno za poslovne procese. To se postiže kroz:

- Rutiranje između VLAN-ova: Mnogi moderni switch uređaji imaju ugrađenu funkciju rutiranja koja omogućava upravljanje saobraćajem između VLAN-ova.
- Postavljanje Access Control List (ACL) pravila: ACL pravila se koriste za kontrolu tačno određenih tipova saobraćaja između VLAN-ova, čime se ograničava pristup samo na određene resurse ili servise.

Ako radne stanice u VLAN-u 10 treba da imaju pristup aplikaciji na serverskom VLAN-u 40, ACL može biti podešen tako da dozvoli samo određeni saobraćaj (npr. RDP ili HTTP/HTTPS) između ta dva VLAN-a, dok će ostatak komunikacije biti blokiran.

Alati za upravljanje VLAN-ovima

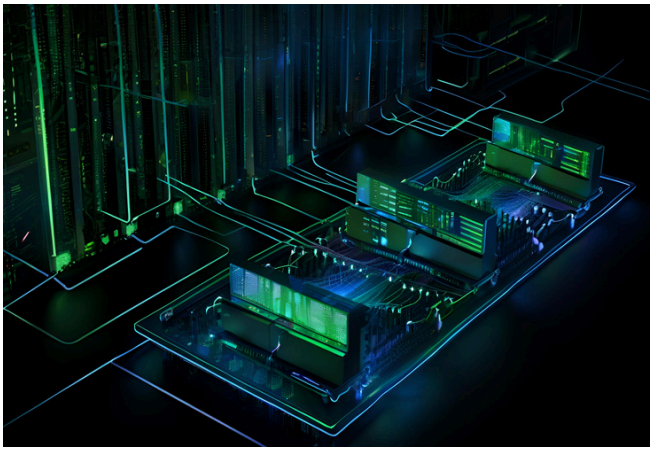
1. **Palo Alto Networks firewall:** Omogućavaju postavljanje polisa kontrole pristupa između VLAN-ova sa visokom preciznošću.
2. **Cisco Catalyst Switches:** Pružaju visok nivo kontrole nad VLAN-ovima, uključujući napredne opcije za rutiranje i bezbednosna pravila.
3. **Open-source alati:** Alati kao što su pfSense ili OPNSense, koji omogućavaju rutiranje i bezbednosnu kontrolu između VLAN-ova u malim i srednje velikim mrežama.

IMPLEMENTACIJA I PRAĆENJE PRAVILA PRISTUPA I BEZBEDNOSNIH POLISA

Uloga pravila pristupa u segmentaciji mreže

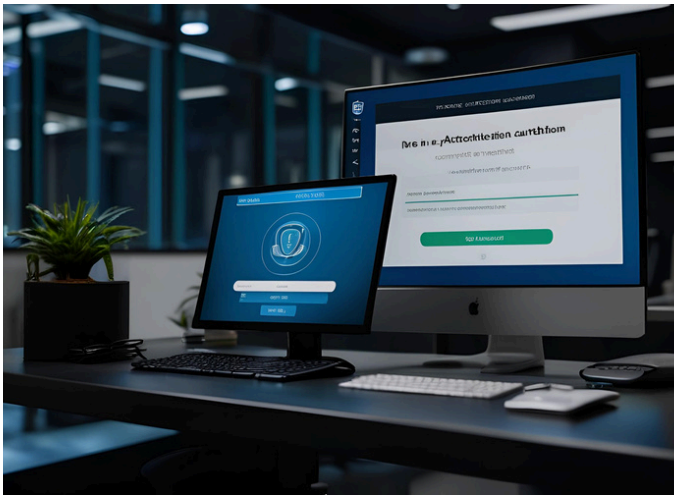
Pravila pristupa čine osnovu bezbednosti segmentisane mreže. Njihova svrha je da definišu dozvoljeni i zabranjeni saobraćaj između različitih delova mreže, omogućavajući organizaciji kontrolu nad time ko i šta može pristupiti osetljivim resursima.

Primer: U scenariju sa nekoliko VLAN-ova, pravila pristupa mogu ograničiti saobraćaj između korisničkih radnih stanica i serverskih resursa, osiguravajući da samo ovlašćeni korisnici mogu pristupiti određenim aplikacijama ili podacima.



Ključni principi za definisanje pravila pristupa

- **Princip najmanjeg pristupa:** Pravilo treba da omogući samo minimum neophodnog pristupa. Na primer, zaposlenima koji rade u prodaji ne treba omogućiti pristup serverskoj zoni sa finansijskim podacima.
- **Segmentacija na osnovu rizika:** Pristup između segmenata sa višim i nižim nivoima rizika treba da bude pažljivo kontrolisan. Na primer, IoT uređaji koji se nalaze u niskobezbednosnoj zoni treba da imaju ograničen pristup mrežnim resursima.
- **Pravila po uzorku specifičnih servisa:** Pravila pristupa mogu biti konfigurisana tako da dopuštaju samo određene servise (npr. samo HTTP i HTTPS za web servere), čime se dodatno smanjuje rizik od napada.



Koraci za implementaciju pravila pristupa

1. **Identifikacija poslovnih potreba:** Razumevanje zahteva za pristup unutar i između različitih segmenata.
2. **Postavljanje Access Control List (ACL) pravila:** Postavite ACL-ove na firewall uređaje kako biste ograničili saobraćaj između različitih zona i VLAN-ova.
3. **Primena dvofaktorske autentifikacije (2FA):** Za kritične resurse i zone, dodajte 2FA kako biste osigurali da samo ovlašćeni korisnici imaju pristup.
4. **Redovno ažuriranje i revizija:** Pravila treba da budu prilagođena razvoju poslovnih potreba i pretnji. Obezbedite redovno ažuriranje kako bi se izbegli zastareli ili nebezbedni pristupi.
5. **Testiranje i praćenje**: Testirajte pravila pristupa kako biste se uverili da su pravilno primenjena i da ne ometaju normalan rad poslovnih procesa.

Uloga alata za praćenje i nadzor bezbednosnih polisa

Alati za monitoring omogućavaju administratorima da prate kako se pravila pristupa primenjuju i da identifikuju sumnjiv saobraćaj ili neovlašćen pristup. Redovno praćenje takođe pomaže u bržem odgovoru na potencijalne pretnje.

Alati za praćenje i nadzor bezbednosnih polisa

- **SIEM sistemi (npr. Splunk, ManageEngine Log360):** Prikupljaju i analiziraju podatke o aktivnostima na mreži, pružajući uvid u sumnjive događaje i aktivnosti.
- **Intrusion Detection Systems (IDS) i Intrusion Prevention Systems (IPS):** Prate mrežni saobraćaj u realnom vremenu i automatski blokiraju sumnjive aktivnosti prema unapred definisanim pravilima.
- **Network Traffic Analysis (npr. NetFlow Analyzer):** Alati za analizu mrežnog saobraćaja omogućavaju detaljno praćenje komunikacije između zona, identifikaciju anomalija i brzi odgovor na pretnje.

Najbolje prakse za praćenje i prilagođavanje pravila pristupa

- **Redovno revidiranje i ažuriranje pravila:** Pravila bi trebalo revidirati najmanje kvartalno kako bi se osiguralo da su u skladu sa trenutnim bezbednosnim standardima i poslovnim potrebama.
- **Praćenje ključnih bezbednosnih metrika:** Uključite metrike kao što su broj blokiranih pristupa, neovlašćenih pokušaja i odstupanja od uobičajenog saobraćaja.
- **Analiza logova i dnevnika aktivnosti:** SIEM i drugi alati omogućavaju analizu logova kako bi se identifikovale eventualne pretnje i prilagodila pravila.
- **Trening i obuka zaposlenih:** Obučite administratore i IT osoblje da prepoznaju potencijalne pretnje i prilagode pristupne polise kada je to potrebno.

PRILAGOĐAVANJE I OPTIMIZACIJA SEGMENTACIJE MREŽE

Segmentacija mreže nije jednokratna aktivnost; kako se poslovne potrebe, infrastruktura i bezbednosne pretnje razvijaju, važno je da mrežna segmentacija evoluira kako bi ostala efikasna i bezbedna. Prilagođavanje i optimizacija segmentacije omogućavaju organizacijama da:

- **Smanje bezbednosne rizike:** Priagođavanje novih polisa pristupa može pomoći u smanjenju napada na segmentisanu mrežu.
- **Poboljšaju performanse mreže:** Prilagođena segmentacija optimizuje mrežni saobraćaj i smanjuje opterećenje, što može poboljšati performanse.
- **Odgovore na poslovne promene:** Različiti sektori ili odeljenja mogu zahtevati različite mrežne resurse tokom vremena, što prilagođena segmentacija može omogućiti.

Proces prilagođavanja segmentacije mreže

1. **Analiza trenutnih mrežnih segmenata:** Identifikujte da li svi segmenti i pravila i dalje ispunjavaju poslovne potrebe i bezbednosne zahteve. Pregledajte mrežni saobraćaj i upotrebu resursa kako biste uočili neiskorišćene ili nepotrebno opterećene segmente.
2. **Identifikacija promena u infrastrukturi:** Procenite da li su novi resursi, servisi, ili korisnici uvedeni u mrežu, kao i da li je potrebno redefinisati segmente kako bi oni bili adekvatno izolovani.
3. **Unapređenje pravila pristupa:** Ažurirajte ACL-ove i pravila za svaki segment na osnovu novih bezbednosnih standarda ili promena u poslovnim potrebama. Na primer, segment za radne stanice možda više ne treba pristup određenim serverskim resursima.
4. **Testiranje segmentacije:** Pre nego što implementirate promene, testirajte nova pravila i segmente na sandbox ili test okruženju kako biste osigurali da ne narušavaju poslovne procese.
5. **Pracenje uticaja i optimizacija:** Nakon primene novih pravila, pratite performanse mreže i korisničko iskustvo. Na osnovu podataka o performansama i bezbednosti, dodatno prilagodite segmentaciju.

Automatizacija i alati za optimizaciju segmentacije

Za efikasnu segmentaciju, korišćenje alata koji omogućavaju automatizaciju i upravljanje može značajno smanjiti potrebu za ručnim intervencijama i omogućiti bržu optimizaciju.

Preporučeni alati za optimizaciju segmentacije:

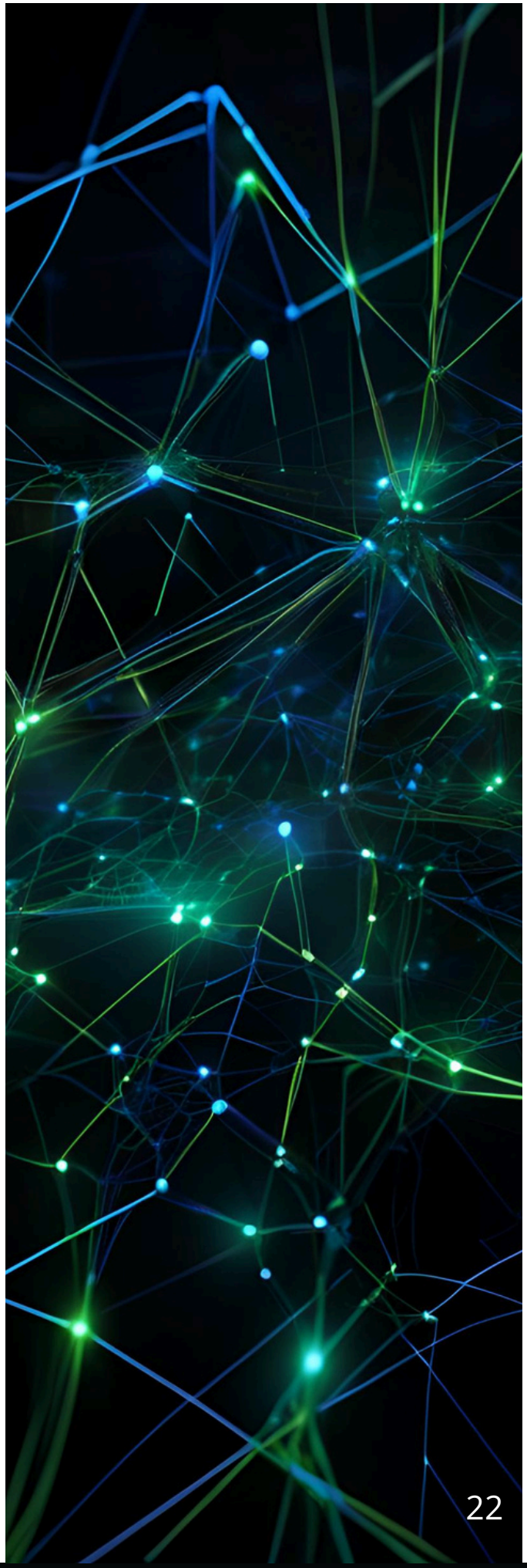
- **Alati za mrežnu automatizaciju:** Omogućavaju brzu i konzistentnu primenu pravila kroz automatsku konfiguraciju uređaja i sistema. Primeri: Ansible, Puppet.
- **SDN rešenja:** Alati kao što su Cisco ACI ili VMware NSX omogućavaju centralizovano upravljanje segmentacijom i brze promene kroz softverske definicije mreže.
- **Network Access Control (NAC) sistemi:** NAC sistemi automatski prilagođavaju pristup korisnika na osnovu unapred definisanih bezbednosnih polisa, omogućavajući segmentaciju zasnovanu na identitetu i uređajima.

Primer:

Organizacija koja koristi SDN može brzo prilagoditi segmente na osnovu potreba, kreirati dodatne segmente za privremene projekte ili omogućiti izolaciju kritičnih resursa u hitnim situacijama.

Najbolje prakse za održavanje i optimizaciju segmentacije

- **Periodične provere i revizije:** Redovno revidirajte sve mrežne segmente i pravila pristupa. Ovo bi trebalo uključiti mesečne ili kvartalne provere kako bi se osiguralo da su sva pravila u skladu sa promenama u poslovnim zahtevima.
- **Usklađivanje sa najnovijim bezbednosnim standardima:** Segmentacija bi trebalo da se prilagodi prema industrijskim standardima, kao što su Zero Trust ili NIST, koji pružaju smernice za optimalnu segmentaciju i pristupnu kontrolu.
- **Simulacija i testiranje pretnji:** Sprovođenje redovnih simulacija pretnji može pomoći u otkrivanju potencijalnih slabih tačaka u segmentaciji, čime ćete predupredити bezbednosne rizike.
- **Obuka osoblja i izgradnja bezbednosne svesti:** Učinite bezbednosna pravila vidljivim zaposlenima, posebno onima u IT i administrativnim sektorima, kako bi segmentacija bila efikasnija uz doslednu primenu od strane korisnika.



NAJČEŠĆI IZAZOVI U IMPLEMENTACIJI I ODRŽAVANJU SEGMENTACIJE

Kompleksnost implementacije

Izazov: Implementacija segmentacije u mrežama, posebno onim velikim i složenim, može biti izuzetno zahtevna. Ova složenost često dovodi do problema sa kompatibilnošću različitih tehnologija i može da zahteva sveobuhvatno planiranje i obuku osoblja.

Rešenje: Počnite sa osnovnom segmentacijom i postepeno razvijajte složenije segmente. Koristite dokumentaciju i alate za mapiranje mreže kako biste olakšali planiranje. Implementacija korak po korak može smanjiti greške i omogućiti lakše prilagođavanje novih segmenata.

Nedovoljna vidljivost u mreži

Izazov: Bez jasne vidljivosti nad mrežnim segmentima, može doći do previda bezbednosnih rizika. Mnoge kompanije nemaju sveobuhvatan uvid u saobraćaj između segmenata, što može otežati prepoznavanje pretnji ili anomalija.

Rešenje: Korišćenje SIEM (Security Information and Event Management) sistema i drugih alata za praćenje mrežnog saobraćaja može pomoći u identifikaciji sumnjivih aktivnosti.

Održavanje efikasnih pravila pristupa

Izazov: Kreiranje i održavanje preciznih pravila pristupa može biti kompleksno. Previše složena pravila mogu dovesti do grešaka ili propusta koji otvaraju potencijalne bezbednosne rizike. Istovremeno, pravila koja nisu dovoljno stroga mogu omogućiti neovlašćen pristup.

Rešenje: Koristite kontrolne liste i automatizovane alate za upravljanje pristupnim kontrolama. Pravila pristupa trebalo bi periodično revidirati i optimizovati na osnovu promena u mreži i poslovnim potrebama. Automatizacija kroz alate kao što su NAC (Network Access Control) može značajno olakšati upravljanje pravilima.

Balansiranje bezbednosti i performansi

Izazov: Efikasna segmentacija često podrazumeva stroga pravila pristupa, što može negativno uticati na performanse mreže i produktivnost korisnika. Na primer, suviše restriktivna pravila mogu usporiti pristup aplikacijama ili uslugama.

Rešenje: Redovno merenje performansi segmentisane mreže omogućava prilagođavanje pravila prema potrebama korisnika i ključnim poslovnim procesima. Testirajte pravila pre implementacije i redovno revidirajte da biste osigurali optimalnu ravnotežu između bezbednosti i performansi.

Resursi i budžet

Izazov: Implementacija segmentacije mreže, naročito u velikim organizacijama, zahteva dodatne resurse i budžet. Nabavka novih uređaja, softverskih rešenja, i obuka osoblja mogu stvoriti finansijski i operativni pritisak.

Rešenje: Za početak, usmerite budžet na najkritičnije segmente mreže, kao što su serverski i administrativni segmenti, koji zahtevaju najviši nivo zaštite. Postepena implementacija omogućava efikasnije korišćenje resursa i budžeta, a upravljanje kroz cloud i SDN tehnologije može dodatno smanjiti troškove.

ZAKLJUČCI I SMERNICE ZA DALJE KORAKE

Ključni zaključci

Mrežna segmentacija pruža osnovu za naprednu bezbednost, kontrolu i otpornost u svakodnevnim operacijama i u slučaju potencijalnih pretnji. Kroz pažljivo planiranje i doslednu primenu, segmentacija mreže:

- **Smanjuje opseg napada:** Izolacijom osetljivih resursa od preostalih delova mreže, organizacija smanjuje šanse za lateralno kretanje napadača i omogućava brže otkrivanje pretnji.
- **Poboljšava kontrolu pristupa:** Definisanje pravila pristupa za različite segmente omogućava organizaciji da precizno kontroliše ko može pristupiti određenim podacima i resursima.
- **Optimizuje performanse mreže:** Segmentacijom se smanjuje opterećenje u kritičnim mrežnim delovima, što vodi ka bržem pristupu resursima i efikasnijem korišćenju infrastrukture.

Smernice za održavanje segmentacije mreže

Efikasna segmentacija mreže zahteva kontinuirano održavanje i prilagođavanje kako bi ostala relevantna i bezbedna. Preporučujemo sledeće korake za održavanje segmentacije:

- **Periodična analiza i revizija:** Uvedite redovne revizije mrežne segmentacije, obavezno proveravajući da svi segmenti ispunjavaju trenutne poslovne i bezbednosne zahteve.
- **Ažuriranje pravila i protokola:** Pravila pristupa, ACL-ove i firewall konfiguracije treba ažurirati u skladu sa novim bezbednosnim standardima i pretnjama koje se pojavljuju.
- **Primena Zero Trust principa:** Kroz postepeno usvajanje Zero Trust modela, organizacije mogu dodatno unaprediti bezbednost omogućavanjem pristupa na osnovu specifičnog identiteta korisnika i uređaja, bez implicitnog poverenja.

Smernice za dalju optimizaciju segmentacije

Nakon početne implementacije, razmotrite dodatne optimizacije koje uključuju napredne tehnologije i pristupe:

- **Korišćenje AI i mašinskog učenja:** Ovi alati mogu pomoći u prepoznavanju anomalija u saobraćaju i automatskom prilagođavanju pravila pristupa.
- **Implementacija mikrosegmentacije:** Mikrosegmentacija na nivou aplikacija omogućava dodatnu bezbednost, posebno za kompanije koje koriste oblak ili imaju kompleksnu IT infrastrukturu.
- **Kontinuirana obuka zaposlenih:** Obuka i podizanje svesti zaposlenih o bezbednosnim praksama značajno doprinosi efektivnosti segmentacije.

Sledeći koraci za implementaciju segmentacije mreže

Za kompanije koje tek započinju put segmentacije mreže, preporučujemo sledeće korake:

- **Počnite sa osnovnim segmentima:** Identifikujte ključne segmente kao što su korisničke radne stanice, serverski resursi, IoT uređaji i administrativni segment. Implementirajte osnovna pravila pristupa između njih.
- **Pratite i prilagođavajte:** Pratite mrežni saobraćaj i obavljajte početne optimizacije. Na osnovu dobijenih podataka, prilagodite konfiguraciju pravila kako biste postigli optimalnu bezbednost.
- **Razvijajte strategiju za dugoročnu optimizaciju:** Pripremite plan za napredne pristupe segmentaciji, kao što su automatizacija, upotreba NAC sistema i integracija sa SIEM alatima za praćenje.

Segmentacija mreže je proces koji značajno unapređuje bezbednost i performanse mreže, ali zahteva kontinuirano praćenje i prilagođavanje. Korisnicima se savetuje da posvete vreme planiranju i postepenom uvođenju segmentacije, kao i da obezbede potrebne resurse za održavanje bezbednosnih polisa.

Kontinuirano ulaganje u optimizaciju segmentacije mreže donosi značajne prednosti u zaštiti podataka i resursa, omogućavajući organizaciji da ostane otporna na sve sofisticiranije pretnje u sajber prostoru.

O NET++ TECHNOLOGY

Net++ technology brine o bezbednosti vaših mreža i podataka. Naš tim stručnjaka pomaže preduzećima da zaštite svoje sisteme od sajber pretnji i da postignu sigurnost u poslovanju.

Nudimo:

- Implementaciju i podršku: Postavljamo i prilagođavamo sisteme kako bi vaša mreža bila zaštićena, a naši stručnjaci su tu za podršku i održavanje.
- Obuku i podizanje svesti o sajber bezbednosti: Radimo obuke za zaposlene i simulacije phishing za bolje razumevanje i sprečavanje pretnji.
- Proaktivnu zaštitu: Pomažemo vam da prepoznate pretnje pre nego što postanu problem, koristeći najnoviju tehnologiju i najbolje prakse.

Naša misija je da vam pružimo osećaj sigurnosti i omogućimo da se usredsredite na poslovanje, dok mi brinemo o bezbednosti.

KONTAKTIRAJTE NAS

Telefon +381 11 3699 967
Website www.netpp.rs
Email office@netpp.rs
Adresa Otokara Keršovanija 11/39, Beograd