STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**FIREWALL**

ZÁKLADY A JEHO TYPY

**ADAM JÁN VILÁGI**

2024

Obsah

Obsah 1

Anotácia 2

1 Úvod do Firewallov 3

1.1 Definícia Firewallu 4

1.2 História Firewallu 4

2 Typy Firewallu 4

2.1 Sieťový Firewall 5

2.2 Aplikačný firewall 5

2.3 Cloudový firewall 5

3 Funkcie Firewallu 5

3.1 Schválenie/Blokovanie 6

3.2 Network Address Translation (NAT) 6

3.2.1 Implementácia NAT 6

3.3 Zaznamenávanie a generovanie správ 6

3.3.1 Zaznamenávanie správ 6

3.4 Generovanie správ 7

4 Postup pre správnu ochranu 7

4.1 Pravidelné aktualizácie 8

4.2 Zavedenie pravidiel 8

4.3 Technické opatrenia 8

4.3.1 Segmentácia siete 8

4.3.2 Monitorovanie prenosu 8

4.3.3 Kontrola prístupu: 8

5 Záver 9

Zoznam použitej literatúry 10

Anotácia

V tejto práci by som chcel poukázať na to ako funguje Firewall a aké sú jeho typy, čím sa posnažím poukázať na jeho implementácie v dnešných počítačových sieťach. Túto tému som si zvolil kvôli jej zásadnému významu v oblasti počítačovej bezpečnosti a myslím si že by mal mať každý aspoň základný prehľad o tom ako tento Firewall funguje, hlavne v zrozumiteľnej forme

**Annotation**

In this paper, I aim to illustrate how a firewall operates and what its types are, intending to highlight its implementations in contemporary computer networks. I chose this topic due to its fundamental significance in the field of computer security, believing that everyone should have at least a basic understanding of how this firewall functions, particularly in an understandable manner.

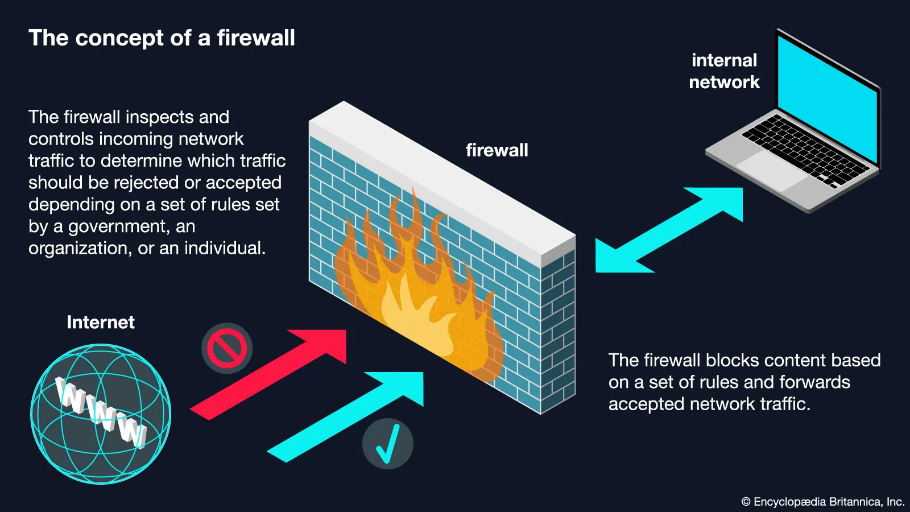
1. Úvod do Firewallov

Firewall je veľmi dôležitý prvok v oblasti počítačovej bezpečnosti, ktorý slúži na ochranu počítačových sietí pred neoprávneným prístupom a škodlivým softvérom. Jeho účelom je monitorovať a kontrolovať tok dát medzi sieťami s rôznymi úrovňami dôveryhodnosti, čím prispieva k zabezpečeniu dôvery, integrity a dostupnosti informácií

* 1. Definícia Firewallu

Firewall chráni a  monitoruje komunikáciu medzi sieťami a zabraňuje neopravnému prístupu k citlivým dátam alebo ich službám. Identifikuje a blokuje škodlivý alebo nebezpečný obsah, ako sú vírusy, malvérové programy a iné formy malvéru. Firewall taktiež môže filtrovať sieťový tok na základe udaných pravidiel, čo umožňuje organizácii alebo používateľovi kontrolovať, ktoré typy komunikácii sú blokované alebo povolené.

* 1. História Firewallu

Vývoj firewallu sa začal niekedy v období 80 rokoch 20 storočia za účelom chránenia toku siete. V tom období to bol skôr primitívny firewall s jednoduchými pravidlami, ale bol schopný filtrovať sieť celkom dobre. Časom o pár desiatok rokov sa objavili lepšie, komerčné riešenia s pokročilejšími funkciami a možnosťou rôznej konfigurácie. Neskôr sa kvôli počtu narážajúcich útokov vyvinuli aj rôzne nove typy firewallu, ako je aplikačný firewall alebo dokonca cloudový. Celkový vývoj firewallu je úzko spojený s rastúcou dôležitosťou bezpečnosti na internete. Od svojich skromných začiatkov sa firewall stal nevyhnutným nástrojom pre zabezpečenie sieti a dnes už ho má skoro každé zariadene.

Obr. 1 Koncept Firewallu

1. Typy Firewallu

Tu poukážem na to aké máme typy firewallu a na čo slúžia, každý sa niečím líši s slúži na niečo iné.

* 1. Sieťový Firewall

Sieťový firewall je zameraný na filtrovanie sieťového toku na základe IP adries a portov. Existujú dva hlavné typy sieťových firewallov: stateful a stateless. Stateful firewall sleduje stav sieťovej komunikácie a rozhoduje na základe predchádzajúcich paketov. Stateless firewall rozhoduje o povolení alebo blokovaní paketov na základe statických pravidiel. Sieťový firewall je často umiestnený medzi vnútornou a vonkajšou sieťou a slúži na ochranu vnútorných zariadení pred vonkajšími hrozbami.

* 1. Aplikačný firewall

sad Aplikačný firewall operuje na vyššej úrovni sieťovej architektúry a je schopný filtrovať sieťový tok na základe konkrétnych aplikácií alebo služieb. Tento typ firewallu môže monitorovať obsah prenášaný cez aplikácie a identifikovať škodlivé alebo nebezpečné aktivity. Aplikačné firewally sú často používané na ochranu webových aplikácií a emailových serverov pred rôznymi formami útokov, ako sú napríklad SQL injection alebo útoky typu cross-site scripting.

* 1. Cloudový firewall

Cloudový firewall je navrhnutý špeciálne pre ochranu cloudových prostredí a služieb. Poskytuje možnosti konfigurácie a ochrany pre virtuálne servery, siete a služby hostované v cloudových prostrediach. Cloudové firewally môžu byť integrované s inými cloudovými nástrojmi pre riadenie bezpečnosti a sú často súčasťou služieb poskytovaných poskytovateľmi cloudových služieb.

1. Funkcie Firewallu

Firewall je veľmi dôležitý prvok v počítačovej bezpečnosti, ktorý zabezpečuje kontrolu a reguláciu toku dát medzi sieťami, pričom sa zameriava na zabezpečenie dôvernosti, integrity a dostupnosti informácií.

* 1. Schválenie/Blokovanie

Tieto základné funkcie firewallu umožňujú určovať, či sa sieťový tok dát povolí alebo zablokuje na základe nastavených pravidiel a politík bezpečnosti. Povolením vybraných tokov dát sa zabezpečuje neprerušená komunikácia medzi sieťami, zatiaľ čo blokovaním nežiaducich tokov sa chráni sieť pred škodlivými aktivitami a neoprávneným prístupom.

* 1. Network Address Translation (NAT)

NAT je technika, ktorá mení IP adresy v paketoch prenášaných cez sieť. Hlavným cieľom NAT je umožniť viacerým zariadeniam v sieti používať jednu verejnú IP adresu na komunikáciu s internetom. Týmto spôsobom môžu zariadenia v internej sieti, ktoré majú pridelené lokálne IP adresy, komunikovať s vonkajším svetom cez jednu alebo viac verejných IP adries.

* + 1. Implementácia NAT

Implementácia NAT môže byť realizovaná rôznymi spôsobmi. Siewteový firewall môže implementovať NAT ako súčasť svojich funkcií, čím umožní prevádzku viacerých zariadení za jedným verejným IP adresovaním. Aplikačný firewall môže tiež podporovať NAT, aby umožnil transparentnú komunikáciu medzi vnútornými a vonkajšími zariadeniami v sieti. Cloudové firewally môžu mať vstavanú podporu NAT, ktorá umožňuje správu IP adries a komunikáciu v rámci cloudových infraštruktúr.

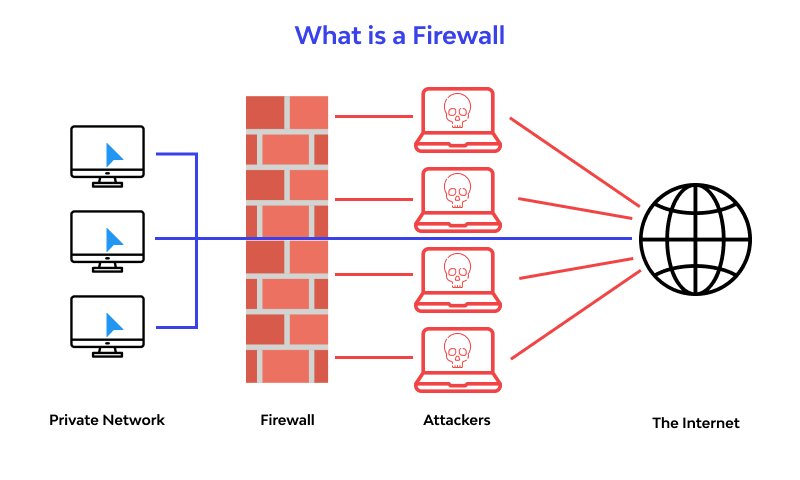
* 1. Zaznamenávanie a generovanie správ

Logging a reporting, alebo teda zaznamenávanie a generovanie správ sú dve kritické súčasti bezpečnosti a správy sietí.

* + 1. Zaznamenávanie správ

Zaznamenávanie alebo inak logging udalostí a aktivít v sieti je veľmi dôležité pre monitorovanie bezpečnostných dier, incidentov alebo identifikáciu potenciálnych hrozieb. Logovacie záznamy obsahujú informácie o prístupoch k sieťovým zdrojom, úspešných a neúspešných prihláseniach, sieťových aktivitách a iných udalostiach v sieti. Dôležité je, aby boli logovacie záznamy vytvárané neustále, zabezpečené a dostupné pre neskoršiu analýzu a vyšetrovanie bezpečnostných incidentov.

* 1. Generovanie správ

Generovanie správ založených na logovacích údajoch umožňuje administrátorom sledovať a analyzovať bezpečnostné udalosti v sieti. Tieto správy môžu obsahovať informácie o útokoch, pokusoch o neoprávnený prístup, anomáliách v sieti, prístupových právach a iných bezpečnostných udalostiach. Správy poskytujú administrátorom holistický pohľad na bezpečnostnú situáciu v sieti a umožňujú im prijímať informované rozhodnutia týkajúce sa riadenia bezpečnosti a reakcie na incidenty. 

Obr. 1 Čo je Firewall

1. Postup pre správnu ochranu

Správne nastavenie fierwallu je vo svete internetu veľmi dôležité, dokáže to zachrániť mnoho citlivých dát.

* 1. Pravidelné aktualizácie

Pravidelné aktualizovanie softvéru a firmvéru firewallu je hlavné pre zabezpečenie ochrany pred najväčšími hrozbami. Aktualizácie operačného systému často obsahujú opravy pre známe zraniteľnosti, čím znižujú riziko, že budú tieto diery v systéme zneužité útočníkmi. Dôležité je mať zavedený systém, ktorý automaticky kontroluje a aplikuje tieto aktualizácie.

* 1. Zavedenie pravidiel

Zavedenie jasných a prísnych bezpečnostných pravidiel je nevyhnutné pre efektívnu ochranu. Tieto pravidlá by mali definovať, aký sieťový prenos je povolený a aký je blokovaný, na základe bezpečnostných požiadaviek používateľa. Implementácia týchto politík pomáha zabezpečiť konzistentnú ochranu naprieč všetkými časťami siete. Pravidlá by mali byť pravidelne kontrolované a aktualizované podľa nových hrozieb a technologických zmien.

* 1. Technické opatrenia

Technické opatrenia sú nevyhnutné na posilnenie bezpečnosti firewallu a siete ako celku. Medzi hlavné opatrenia patria tieto.

* + 1. Segmentácia siete

Rozdelenie siete na menšie, izolované segmenty môže zlepšiť bezpečnosť tým, že obmedzí potenciálne narušenia na malú časť siete. Tento prístup znižuje riziko, že útočník získa prístup k citlivým údajom alebo kritickým systémom v prípade prieniku do siete.

* + 1. Monitorovanie prenosu

Neustále monitorovanie sieťového prenosu pomáha včas identifikovať a reagovať na podozrivé aktivity. Použitie nástrojov pre detekciu a prevenciu narušení (IDPS) môže poskytovať ďalšie vrstvy ochrany tým, že automaticky reagujú na detegované hrozby.

* + 1. Kontrola prístupu:

Implementácia striktných kontrol prístupu zabezpečuje, že iba autorizovaní používatelia a zariadenia majú prístup k určitej časti siete. Tento prístup pomáha minimalizovať riziko interných hrozieb.

Graf. 1 Týždenné útoky na organizáciu podľa regiónu

1. Záver

Podľa môjho názoru sú firewally nevyhnutnou súčasťou modernej kybernetickej bezpečnosti. Ich schopnosť chrániť siete pred rôznymi hrozbami je kľúčová pre udržanie integrity a bezpečnosti dát. Firewally umožňujú kontrolovať prístup, monitorovať sieťový prenos a rýchlo reagovať na potenciálne hrozby, čím poskytujú silnú ochranu.

Tému firewall som si vybral kvôli ich zásadnému významu. Správna konfigurácia a pravidelné aktualizácie sú nevyhnutné pre efektívnu ochranu. Verím, že hlbšie pochopenie ich fungovania môže výrazne prispieť k lepšej ochrane sietí a dát. Každý, kto pracuje s počítačovými sieťami, by mal mať aspoň základné vedomosti o firewalle a jeho implementácii.

Zoznam použitej literatúry

1. ANNASOFT, WAF – WEB APPLICATION FIREWALL, [cit. 28.4.2024]  [online] Dostupné na: https://www.anasoft.com/sk/home/riesenia/IT-Security/WAF-Web-Application-Firewall
2. The role and security of firewalls in cyber-physical cloud computing,[cit. 12.3.2024]  [online] Dostupné na:<https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-016-0042-3>
3. Stateful vs. stateless firewalls: Understanding the differences, [cit. 21.3.2024]  [online] Dostupné na: [https://www.techtarget.com/searchsecurity/answer/How-do-stateful-inspection-and-packet-filtering-firewalls-differ?\_gl=1\*s1su8y\*\_ga\*MTA4OTc0MTQzNy4xNzE2NTM0MjQ2\*\_ga\_TQKE4GS5P9\*MTcxNjUzNDI0Ni4xLjEuMTcxNjUzNTIyMy4wLjAuMA..](https://www.techtarget.com/searchsecurity/answer/How-do-stateful-inspection-and-packet-filtering-firewalls-differ?_gl=1*s1su8y*_ga*MTA4OTc0MTQzNy4xNzE2NTM0MjQ2*_ga_TQKE4GS5P9*MTcxNjUzNDI0Ni4xLjEuMTcxNjUzNTIyMy4wLjAuMA..)
4. What are next generation firewalls? How the cloud and complexity affect them, [cit. 20.3.2024]  [online] Dostupné na: [https://www.csoonline.com/article/566153/what-are-next-generation-firewalls-how-the-cloud-and-complexity-affect-them.html](https://www.csoonline.com/article/566153/what-are-next-generation-firewalls-how-the-cloud-and-complexity-affect-them.html%20)
5. Log and Monitor Data Center Traffic [cit. 23.4.2024]  [online] Dostupné na: <https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/log-and-monitor-data-center-traffic>
6. Advanced Firewall Techniques [cit. 1.3.2024]  [online] Dostupné na: <https://www.linkedin.com/pulse/advanced-firewall-techniques-proinfinc>
7. All You Need to Know About Network Security, Firewalls, and VPNs [cit. 10.2.2024]  [online] Dostupné na: <https://www.eccu.edu/blog/cybersecurity/network-security-firewalls-vpns/>
8. What Are the 5 Main Types of Firewall? [cit. 10.2.2024]  [online] Dostupné na: <https://www.makeuseof.com/types-of-firewalls/>
9. Firewall [cit. 10.2.2024]  [online] Dostupné na:< <https://www.eset.com/sk/firewall-ochrana/>>
10. Introdcution of Firewall in Computer Network [cit. 8.2.2024]  [online] Dostupné na:<https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/>
11. Čo je to brána firewall? [cit. 6.2.2024]  [online] Dostupné na:<https://www.mcafee.com/sk-sk/antivirus/firewall.html>
12. Types of Firewalls Defined and Explained [cit. 14.4.2024] ]  [online] Dostupné na:<https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls>
13. Fireawalls defined, explained, and explored [cit. 11.1.2024] ]  [online] Dostupné na:<https://www.forcepoint.com/cyber-edu/firewall>