



ТЕХНИЧЕСКИ УНИВЕРСИТЕТ —
СОФИЯ

ФАКУЛТЕТ КОМПЮТЪРНИ СИСТЕМИ И
ТЕХНОЛОГИИ

Курсова работа

Дисциплина: „Операционни системи ”

тема: “Proxy server - анализ и употреба”

Изготвил:

Владислав Валентинов Атанасов

Фак. № 121222190

Група: 39

III курс, КСИ

e-mail: vladatanasov@tu-sofia.bg

Ръководител:

доц. Невен Николов

София, 2024

СЪДЪРЖАНИЕ

1. Увод
 - 1.1. Значение на мрежовите технологии
 - 1.2. Роля на прокси сървърите в интернет комуникациите
2. Какво е Proxy Server?
 - 2.1. Дефиниция и основни функции
 - 2.2. Видове прокси сървъри
3. Как работи Proxy Server?
 - 3.1. Основни принципи на работа
 - 3.2. Технологии и протоколи, използвани от прокси сървъри
 - 3.3. Load Balancing и Distributed Computing
4. Анализ на предимствата и недостатъците на Proxy Server
 - 4.1. Предимства
 - 4.2. Недостатъци
5. Употреба на Proxy Server в различни сфери
 - 5.1. Корпоративна среда
 - 5.2. Индивидуална употреба
 - 5.3. Други приложения
6. Сравнение между Proxy Server и VPN
 - 6.1. Общи характеристики
 - 6.2. Разлики в сигурността и функционалността
 - 6.3. Приложения и подходящ избор
7. Съвременни тенденции и развитие на Proxy Server технологиите
 - 7.1. Актуални предизвикателства в сигурността
 - 7.2. Интеграция с облачни услуги
 - 7.3. Роля на прокси сървърите в ерата на IoT
8. Заключение
 - 8.1. Значение на прокси сървърите в съвременната мрежова среда
 - 8.2. Бъдещи перспективи за използването им
9. Използвана литература

1. Увод

1.1. Значение на мрежовите технологии

В съвременния свят комуникациите чрез интернет пространството играят основна роля в ежедневието ни, като свързват хора, устройства и информация с невероятна бързина и мащаб. В тази динамична среда, сигурността, ефективността и достъпът до данни се превръщат в ключови аспекти за успешното функциониране на мрежите. За да се отговори на тези изисквания, се разработват различни технологии, които подпомагат управлението на информацията и подобряват взаимодействието между потребителите и интернет ресурсите. Сред тези технологии прокси сървърите заемат важно място, предоставяйки възможности за защита на личните данни, оптимизация на мрежовия трафик и управление на достъпа.

1.2. Роля на прокси сървърите в интернет комуникациите

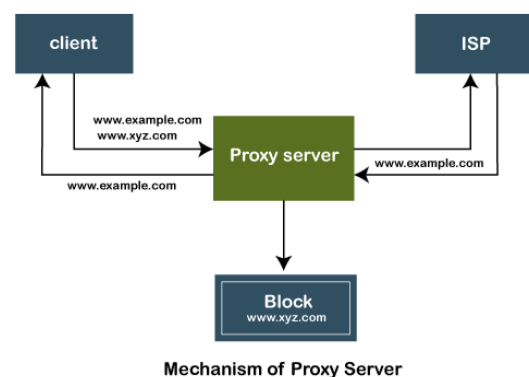
Прокси сървърите изпълняват уникална роля в посредничеството между крайните потребители и онлайн ресурсите. Чрез тяхното използване се постига по-голям контрол върху потока на информация, както и възможност за адресиране на редица проблеми, свързани с поверителността и сигурността в глобалната мрежа. Тази технология намира приложение както в ежедневната работа на отделния потребител също така и в по-широки корпоративни контексти, където управлението на мрежовия трафик и защитата на данни са критично важни.

Тази работа има за цел да разгледа концепцията за прокси сървърите, техните функции и приложения в различни сфери. Ще бъдат анализирани техните предимства и недостатъци, както и значението им за модерната интернет инфраструктура. По този начин ще се подчертае значимостта на прокси сървърите като инструмент за ефективно и сигурно използване на мрежовите ресурси.

2. Какво е Proxy Server?

2.1. Дефиниция и основни функции

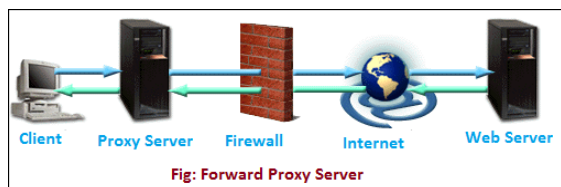
Прoxy сървърът представлява междинен сървър, който действа като посредник между потребителя и интернет ресурсите, до които той се опитва да получи достъп. Основната му функция е да приема заявки от потребителя и да ги препраща към съответния уебсайт, услуга или сървър, като същевременно връща резултата обратно към заявителя.



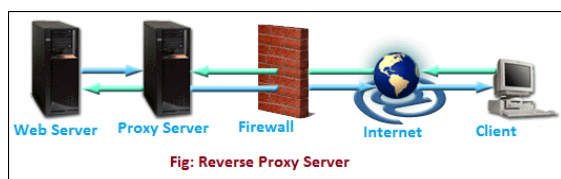
Този процес не само опростява взаимодействието с различни онлайн ресурсите, но и добавя слой от анонимност, защита и управление на трафика. Proxy сървърите често се използват за оптимизация на работата на мрежите, контрол върху достъпа до определени ресурси или заобикаляне на географски ограничения. Освен това те могат да играят важна роля в кеширането на съдържание, намалявайки натоварването върху мрежовите ресурси.

2.2. Видове прокси сървъри

Разнообразието от видове прокси сървъри е значително и всяка категория има свои специфични приложения и характеристики. Forward proxy, например, се използва основно за достъп на потребители до интернет, като скрива техния IP адрес и осигурява анонимност. Това е най-често срещаният тип прокси, който често се използва за лична защита и достъп до ограничено съдържание.



Обратният прокси (Reverse proxy), от друга страна, служи за защита на сървърите, към които потребителите се опитват да се свържат. Този тип прокси е разположен пред уеб сървърите и филтрира трафика, като по този начин подобрява сигурността, балансира натоварването и осигурява по-добра производителност на приложенията.



Една от по-специфичните категории е Transparent proxy, който не скрива по никакъв начин идентичността на потребителя, но предлага оптимизация на мрежовия трафик чрез кеширане и филтриране на съдържание. Този тип прокси често се използва в корпоративни мрежи за наблюдение и управление на интернет достъпа. Анонимните прокси сървъри предоставят допълнително ниво на защита, като скриват IP адреса на потребителя и предотвратяват проследяването на неговата онлайн активност. Високоанонимните прокси, известни още като Elite proxies, не само скриват идентичността на потребителя, но и не разкриват на целевите сървъри, че заявката е преминала през прокси. Това ги прави особено подходящи за потребители, които изискват максимална степен на конфиденциалност.

Всеки от тези видове прокси сървъри има своя уникална роля в контекста на съвременните мрежови приложения. Те се използват в зависимост от нуждите на потребителите и мрежовата среда, в която се прилагат, като осигуряват широк спектър от функционалности и ползи за управление на интернет трафика и повишаване на сигурността.

3. Как работи Proxy Server?

3.1. Основни принципи на работа

Прокси сървърът действа като посредник между клиента и целевия сървър, като изпълнява функциите на филтър, преводач и кеширащ механизъм. Когато потребителят изпрати заявка за достъп до определен ресурс, заявката първо преминава през прокси сървъра, който обработва информацията и решава дали да я препрати към съответния ресурс или да върне кеширана версия на съдържанието. Тази обработка включва анализ на заявката, идентифициране на достъпните ресурси и изпълнение на конфигурираните правила, които могат да ограничават или позволяват определени действия. Резултатът се връща обратно към потребителя, като често се включва допълнителна оптимизация или защита на данните.

Основният принцип на работа на прокси сървърите е пренасочването на мрежовия трафик. Когато потребителят прави заявка, неговият IP адрес се заменя с IP адреса на прокси сървъра, което осигурява определено ниво на анонимност. В зависимост от типа на прокси, заявката може да бъде кеширана, за да се ускори достъпът при следващо търсене на същото съдържание, или модифицирана, за да се отговори на специфични мрежови изисквания, например филтриране на данни или компресия на съдържанието.

3.2. Технологии и протоколи, използвани от прокси сървъри

Технологиите и протоколите, използвани от прокси сървърите, играят критична роля за тяхната функционалност. HTTP proxy сървърите, например, работят с протокола HTTP и се използват за управление на уеб трафик, като осигуряват кеширане, филтриране и анонимност при посещаване на уебсайтове. HTTPS proxy добавя поддръжка за криптирани връзки, което гарантира сигурността на данните, преминаващи през сървъра. SOCKS proxy, който работи на по-ниско ниво от OSI модела, е универсално решение, подходящо за работа с различни протоколи, включително HTTP, FTP и SMTP, като

предлага повече гъвкавост, но често е по-бавен.

Сред другите ключови технологии, използвани от прокси сървърите, е кеширащият механизъм, който позволява временно съхранение на данни. Тази функция е особено полезна за намаляване на натоварването върху целевите сървъри и ускоряване на достъпа до често използвано съдържание. Освен това проху сървърите често използват SSL/TLS за да могат да криптират връзките, което е допълнителен слой защита при обработка на чувствителна информация.

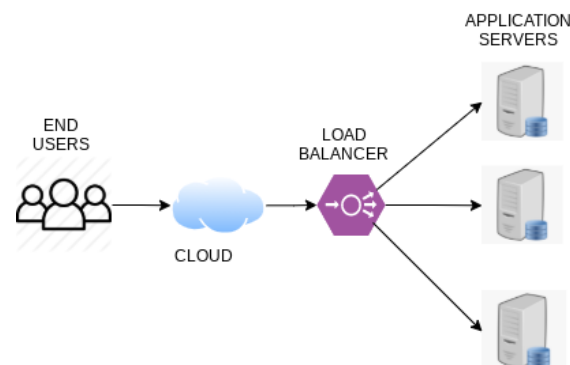
Важна част от работата на прокси сървърите е и поддръжката на протоколи за автентикация и контрол на достъпа, като LDAP или RADIUS. Те се използват в корпоративни среди за гарантиране, че само оторизирани потребители имат достъп до мрежови ресурси. Тези технологии допринасят за ефективността и сигурността на прокси сървърите, като ги правят незаменими инструменти в управлението на съвременните мрежи.

3.3. Load Balancing и Distributed Computing

Проху сървърите често играят ключова роля в механизмите за баланс на натоварването (load balancing) и разпределените изчисления (distributed computing), които са от съществено значение за съвременните мрежи и приложения.

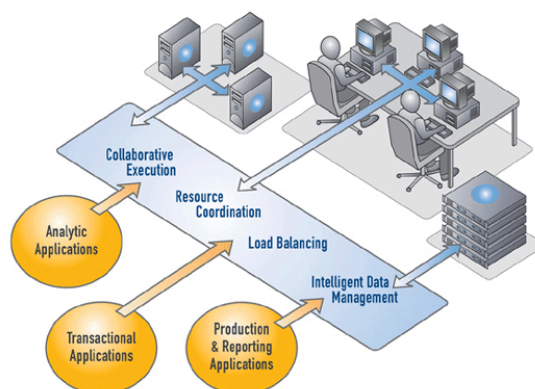
Load balancing е техника, при която проху сървърът разпределя входящия трафик между множество сървъри, за да избегне претоварване и да осигури равномерно разпределение на ресурсите. Това се постига чрез използване на алгоритми, като Round Robin (заявките се разпределят последователно), Least Connections (заявката се насочва към сървъра с най-малко активни връзки) или Weighted Distribution (ресурсите се разпределят въз основа на производителността на сървърите). Проху сървърът следи текущото състояние на сървърите и динамично пренасочва

заявките, за да гарантира оптимално време за отговор и максимална производителност.



Например уеб платформи с висока посещаемост, като онлайн магазини или социални мрежи, проху сървърът използва load balancing, за да насочи потребителския трафик към различни сървъри, което гарантира бързина и стабилност на услугите дори при голям обем от заявки.

Distributed computing (разпределени изчисления) е концепция, при която изчислителните задачи се разпределят между множество устройства или сървъри, свързани в мрежа. Проху сървърите често служат като координационен механизъм в такива системи, като осигуряват интелигентно разпределение на заявките и управление на ресурси. Те позволяват на отделните сървъри или клъстери да работят заедно по изпълнението на сложни задачи, като големи изчисления, анализ на данни или обработка на мултимедийно съдържание.



Чрез load balancing и distributed computing, прокси сървърите подпомагат изграждането на мащабируеми, устойчиви и

ефективни мрежови инфраструктури. Те осигуряват равномерно разпределение на натоварването, предотвратяват затруднения в трафика и минимизират риска от сринове, което е особено важно за критични приложения като финансови услуги, здравеопазване или облачни платформи.

4. Анализ на предимствата и недостатъците на Proxy Server

4.1. Предимства

Едно от най-значимите предимства на проху сървърите е подобряването на сигурността. Те служат като междинна точка между потребителя и интернет ресурсите, което намалява риска от директен достъп на злонамерени лица до устройството на потребителя. Чрез скриване на IP адреса проху сървърите осигуряват основна анонимност, която е особено важна за защита на личните данни и предотвратяване на кибератаки.

Оптимизацията на мрежовия трафик е друга важна функция. Кеширането на данни позволява на проху сървърите да съхраняват често използвана информация, така че последващите заявки да бъдат обслужвани по-бързо. Това не само намалява времето за достъп, но и облекчава натоварването върху целевите сървъри, което е критично за корпоративни мрежи и уеб платформи с голям обем на трафика.

Друго предимство е възможността за заобикаляне на географски ограничения. Проху сървърите позволяват достъп до съдържание, което е ограничено в определени региони, като пренасочват заявките през сървъри в други държави. Това е особено полезно за потребители, които искат да получат достъп до стрийминг услуги, новинарски платформи или социални мрежи, блокирани в тяхната страна.

На корпоративно ниво проху сървърите осигуряват контрол върху достъпа до интернет. Те могат да бъдат конфигурирани така, че да ограничават достъпа до нежелани сайтове, което подобрява продуктивността на служителите и минимизира риска от злонамерен софтуер.

Освен това проху сървърите могат да се използват за наблюдение на трафика, като предоставят ценна информация за анализа на мрежовата активност.

4.2. Недостатъци

Въпреки множеството си предимства, проху сървърите имат и своите ограничения. Един от основните недостатъци е тяхната ограничена сигурност в сравнение с други технологии, като VPN. Докато проху сървърите скриват IP адреса, те не криптират данните, преминаващи през тях. Това означава, че информацията може да бъде прихваната от злонамерени лица, особено ако се използва прокси без подходяща защита.

Друго ограничение е зависимостта от конфигурацията и надеждността на проху сървъра. Неправилно конфигуриран сървър може да изложи потребителските данни на риск или да доведе до понижаване на производителността. Освен това публичните проху сървъри често са по-бавни, тъй като се използват от множество потребители, което увеличава времето за отговор и намалява ефективността.

Необходимо е също така да се отбележи, че проху сървърите могат да бъдат използвани за злонамерени цели. Злоупотребата с тях за достъп до незаконно съдържание или за избягване на правила и ограничения представлява сериозен етичен и правен проблем. Освен това някои публични проксита могат да бъдат управлявани от недоброжелателни оператори, които събират и злоупотребяват с данните на потребителите.

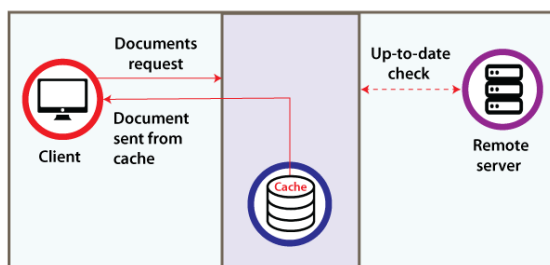
На корпоративно ниво проху сървърите изискват постоянна поддръжка и актуализация, за да бъдат ефективни. Технологиите и методите за заобикаляне на проксита постоянно се развиват, което изисква от мрежовите администратори да следят новите заплахи и да предприемат мерки за защита. Това увеличава оперативните разходи и изисква специализиран персонал.

5. Употреба на Proxy Server в различни сфери

5.1. Корпоративна среда

В бизнеса проху сървърите са основен инструмент за управление на мрежовия трафик и подобряване на сигурността. Компаниите често използват проху сървъри за ограничаване на достъпа на служителите до несвързани с работата уебсайтове, което повишава продуктивността и намалява риска от случайно изтегляне на зловреден софтуер. През проху сървърите може да се осъществява мониторинг на мрежовата активност, което позволява на администраторите да анализират поведението на потребителите и да оптимизират ресурсите.

Едно от ключовите приложения в корпоративната среда е кеширането на съдържание. Това помага за намаляване на времето за достъп до често използвани ресурси и облекчава натоварването върху мрежата, което е от съществено значение за големи организации. Също така, в условия на висока конкуренция проху сървърите се използват за защита на корпоративните данни чрез reverse проху решения, които филтрират входящия трафик и блокират злонамерени атаки, като DDoS.



5.2. Индивидуална употреба

Индивидуалните потребители също се възползват от множество функционалности на проху сървърите, най-вече за повишаване на онлайн сигурността и заобикаляне на ограничения. Много хора използват проху сървъри, за да скрият своя IP адрес и по този начин да увеличат нивото на анонимност при сърфиране в интернет. Това е особено важно при достъп до публични

Wi-Fi мрежи, където рискът от прихващане на данни е по-висок.

Друга често срещана употреба е заобикалянето на географски ограничения, например при достъп до стрийминг платформи, които предоставят съдържание само за определени региони. Потребителите могат да използват проху сървъри, разположени в други държави, за да получат достъп до желаните услуги.

Индивидуалните потребители, които изискват висока скорост и сигурност, често прибягват до платени проху сървъри, които предоставят допълнителни функции като криптиране и специализирана поддръжка. В същото време някои потребители избират публични проксите за краткосрочна употреба, въпреки че те са по-несигурни и бавни.

5.3. Други приложения

Освен в корпоративната и индивидуалната сфера, проху сървърите се използват в редица специфични приложения. Те играят важна роля в електронната търговия и дигиталния маркетинг, където са необходими за извършване на уеб скрапинг – техника за събиране на данни от уебсайтове. Проху сървърите позволяват събиране на информация, като ценови данни или анализ на конкуренцията, без риск от блокиране на достъпа от целевия сайт.

В сферата на образованието проху сървърите често се използват в учебни заведения за ограничаване на достъпа на учениците до нежелано съдържание и за защита на мрежите от външни заплахи. В научноизследователската дейност те осигуряват достъп до специализирани онлайн ресурси, които може да са ограничени до определени географски региони или институции.

В държавната администрация проху сървърите често се използват за повишаване на сигурността на чувствителни данни и за наблюдение на интернет активността с цел предотвратяване на киберзаплахи. Освен това те се прилагат в правоприлагането за

извършване на разследвания в интернет, като скриват източника на заявките.

Proху сървърите са незаменим компонент и в IoT (Internet of Things) мрежите. Те осигуряват ефективно управление на свързаните устройства, като оптимизират трафика и защитават данните, преминаващи през тях. В контекста на нарастващото използване на свързани устройства, тази роля на проху сървърите става все по-значима.

Чрез множеството си приложения проху сървърите демонстрират своята универсалност и значимост в различни аспекти на съвременния дигитален свят. Независимо от мащаба на потребителската база или специфичността на изискванията, те остават ключов инструмент за подобряване сигурността, производителността и функционалността на мрежите.

6. Сравнение между Proxy Server и VPN

Proху сървърите и виртуалните частни мрежи (VPN) са популярни технологии за управление на интернет връзките, осигуряване на анонимност и оптимизиране на достъпа до ресурси. Макар че те често се използват с подобни цели, разликите в тяхната архитектура, функционалност и приложение ги правят подходящи за различни ситуации. Разглеждането на общите им характеристики, както и на техните различия, е от съществено значение за правилния избор в зависимост от конкретните нужди.

6.1. Общи характеристики

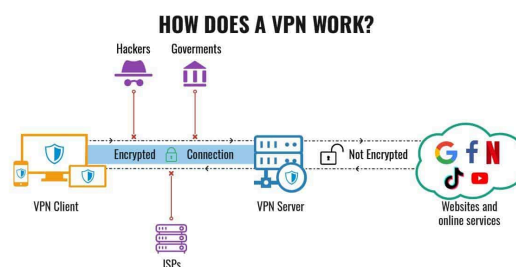
И проху сървърите, и VPN осигуряват посредничество между клиента и целевите сървъри, което позволява пренасочване на трафика през трета страна. И двете технологии могат да скрият реалния IP адрес на потребителя, предоставяйки основно ниво на анонимност. Те също така могат да бъдат използвани за заобикаляне на географски ограничения или блокировки, предоставяйки достъп до съдържание, което иначе би било недостъпно.

Както проху сървърите, така и VPN предлагат функционалности за контрол на трафика, които са полезни както в индивидуален, така и в корпоративен контекст. Например, те могат да бъдат конфигурирани за ограничаване на достъпа до определени ресурси или за предоставяне на защита срещу нежелан мрежов трафик.

6.2. Разлики в сигурността и функционалността

Основната разлика между проху сървърите и VPN е нивото на сигурност, което те предлагат. Proху сървърите обикновено не криптират трафика, преминаващ през тях, което ги прави уязвими към прихващане на данни от трети страни. От друга страна, VPN осигуряват силно криптиране чрез протоколи като OpenVPN, IPSec или WireGuard, което гарантира защита на информацията, включително в несигурни мрежи като обществени Wi-Fi точки.

Функционалността също се различава. Proху сървърите обикновено са ограничени до определени приложения или типове трафик, например уеб браузъри или стрийминг услуги, докато VPN защитават целия интернет трафик на устройството. Това прави VPN по-универсални в ситуации, изискващи висока степен на защита, като например работа с чувствителни данни.



От гледна точка на скоростта, проху сървърите често са по-бързи, тъй като не извършват сложни криптиращи операции. Това ги прави подходящи за задачи, които не изискват високо ниво на сигурност, като гледане на онлайн съдържание или уеб скрапинг. VPN, поради допълнителния слой на криптиране, може да доведе до забавяне на връзката, особено ако се използват сървъри на голямо разстояние.

6.3. Приложения и подходящ избор

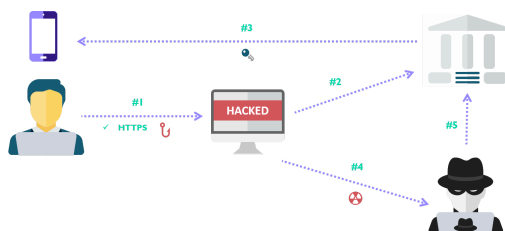
Proxu сървърите са предпочитан избор в ситуации, където бързината и лесната конфигурация са от значение. Те са подходящи за потребители, които искат да заобиколят географски ограничения, да ограничат достъпа до определени уебсайтове или да управляват корпоративен интернет трафик. Освен това, те са широко използвани в автоматизирани системи за събиране на данни и анализ на уебсайтове.

VPN от своя страна са идеалният избор за осигуряване на високо ниво на сигурност и поверителност. Те са подходящи за потребители, които работят с чувствителна информация, като например при работа отдалечено или в случаи на достъп до корпоративни мрежи. VPN също така предоставят по-добра защита срещу интернет доставчици или правителствени структури, които може да наблюдават трафика.

В крайна сметка изборът между проху сървър и VPN зависи от конкретните изисквания. Ако сигурността и поверителността са основен приоритет, VPN е по-добрият вариант. Ако обаче се търси бързо и лесно решение за конкретни задачи, проху сървърът може да бъде по-подходящият избор.

7. Съвременни тенденции и развитие на Proxy Server технологиите

Proxu сървърите продължават да се развиват, за да отговорят на променящите се изисквания на съвременния дигитален свят. Разширяването на интернет инфраструктурата, нарастващата сложност на киберзаплахите и интеграцията с нови технологии, като облачни услуги и Internet of Things (IoT), създават нови възможности и предизвикателства за тази технология.



7.1. Актуални предизвикателства в сигурността

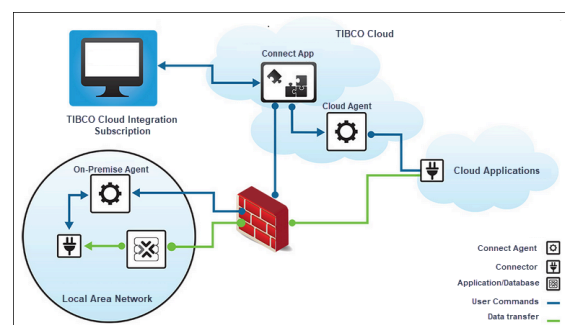
С нарастването на кибератаките проху сървърите са изправени пред значителни предизвикателства, свързани със сигурността. Злонамерени атаки, като например експлойти на уязвимости в конфигурацията на проху сървъри или използването на публични проксита за злонамерени дейности, изискват по-напреднали механизми за защита.

Една от основните области за развитие е усъвършенстването на методите за откриване и блокиране на зловреден трафик. Proxu сървърите все по-често интегрират изкуствен интелект и машинно обучение, за да идентифицират необичайни модели на мрежова активност и да предотвратяват атаки в реално време.

Освен това се увеличава използването на прокси решения, които комбинират традиционните функции със съвременни технологии за криптиране, за да защитят потребителските данни. Протоколи като HTTPS Proxu и SOCKS5 се развиват, за да осигурят по-високо ниво на сигурност и съвместимост с различни приложения.

7.2. Интеграция с облачни услуги

С нарастването на облачните технологии проху сървърите намират нова роля в осигуряването на достъп и защита в този контекст. Облачните проксита, които се хостват като част от облачната инфраструктура, предлагат гъвкавост и мащабируемост, които са недостъпни за традиционните локални решения.



Тези сървъри играят ключова роля в управление на достъпа до облачни

платформи, като осигуряват филтриране на трафика и криптиране на данните. Те са особено полезни за организации, които се нуждаят от защита на чувствителна информация при работа с публични или хибридни облаци.

Освен това облачните проху сървъри позволяват интеграция с други услуги, като например системи за идентификация (identity management) и инструменти за анализ на мрежовия трафик. Тази интеграция подобрява управляемостта и сигурността на корпоративните мрежи, като същевременно намалява разходите за инфраструктура.

7.3. Роля на прокси сървърите в ерата на IoT

С нарастването на IoT устройствата проху сървърите се адаптират, за да отговорят на специфичните изисквания на тези мрежи. IoT устройства често са уязвими към кибератаки поради ограничените им възможности за обработка на данни и липсата на съвременни защити. Проху сървърите могат да действат като междинен слой, който осигурява допълнителна защита и управление на мрежовия трафик.

В IoT средата проху сървърите се използват за оптимизация на трафика, като групират и пренасочват заявките от множество устройства. Това намалява натоварването върху мрежата и позволява по-ефективно управление на ресурсите. Освен това те осигуряват защитна бариера срещу неоторизиран достъп до IoT устройствата, предотвратявайки атаки като ботнет експлойти и прихващане на данни.

Едно от значимите приложения на проху сървърите в IoT е обработката на данни в реално време. Те позволяват на устройствата да изпращат събрана информация към облака или центрове за данни чрез сигурни и оптимизирани канали. Това е особено важно в индустрии като здравеопазването, където IoT устройствата трябва да обработват чувствителни данни в условия на висока сигурност.

Проху сървърите са ключов елемент в изграждането на мащабируеми и сигурни мрежи в ерата на IoT. Те не само защитават устройствата, но и улесняват интеграцията им с по-широки инфраструктури, като предоставят критично значение за бъдещето на свързаните технологии.

8. Заключение

Проху сървърите са ключов елемент в съвременната мрежова архитектура, като предоставят решения за множество предизвикателства в интернет комуникациите. Чрез разнообразните си приложения те осигуряват сигурност, управление на трафика и ефективно използване на мрежовите ресурси. Тяхното значение се увеличава с разширяването на облачните технологии, растящия брой IoT устройства и нарастващите изисквания за киберсигурност.

Въпреки че проху сървърите не винаги предлагат същото ниво на защита като VPN, тяхната ефективност и гъвкавост ги правят незаменим инструмент в много контексти – от корпоративните мрежи до личната употреба. Развитието на технологии за разпределено изчисление и баланс на натоварването демонстрират как проху сървърите могат да се адаптират и надграждат, за да отговорят на бъдещите нужди на мрежовите среди.

С напредъка в изкуствения интелект и машинното обучение, проху решенията могат да станат още по-интелигентни и ефективни. Това подчертава тяхната роля не само като инструмент за подобрене на мрежовата работа, но и като основа за сигурни и устойчиви дигитални екосистеми. В бъдеще, интеграцията на проху технологии с нови направления в IT ще осигури още по-широки възможности за използване в глобалната дигитална трансформация.

9. Използвана литература

<https://www.pcmag.com/explainers/what-is-a-proxy-server-and-do-you-need-one>

<https://www.javatpoint.com/what-is-a-proxy-server-and-how-does-it-work>

<https://www.onespan.com/blog/how-attackers-bypass-modern-two-factor-authentication-and-how-protect-your-users>

<https://www.comparitech.com/blog/vpn-privacy/vpn-tunneling/>

<https://www.techopedia.com/definition/4200/proxy-server>

<https://softwarelab.org/blog/what-is-a-proxy-server/>

<https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/>