MJI

Media Jurnal Informatika
Vol. 16, no.1, Juni 2024
http://jurnal.unsur.ac.id/mjinformatika

p-issn : 2088-2114
e-issn : 2477-2542

Perlindungan Port dari Pemindaian NMAP dan Meningkatkan Efisiensi IPv4 dengan MikroTik dan Nginx

Juri Pebrianto
Universitas Pamulang
juripebrianto@gmail.com

Abstract

In addition to attempting to safeguard web hosting servers from NMAP port scan attacks, this research addresses the issue of IPv4 addresses being scarcer and more efficiently used and utilizing the Reverse Proxy method to protect against port scanning and the Enhanced Explicit Port Forwarding method from MikroTik to maximize IPv4 usage efficiency. This study suggests combining the two to increase infrastructure efficiency, particularly web hosting servers. Utilizing MikroTik port redirection yields the following results: Up to 254 private IP addresses can be handled by a single public or static IPv4 address. While the implementation of Nginx as a reverse proxy requires one IPv4 address to convert it into a web service that can be accessed via DNS, Nginx's reverse proxy capability makes the IPv4 and port generated by MikroTik invisible from the outside. IPs or local IPs using different ports must be used as the address of a web hosting server or IoT device. The port that the Nginx server is on, not the primary server, will be displayed in the results of an Nmap port scan if an attack or port scan is conducted on a domain running Nginx. This method requires just two IPv4 addresses to manage many devices, including those needed for web services (such as those in this study) and other devices that need their IPv4 address to avoid port scans with NMAP revealing a domain's valid address.

Keywords*: Infrastructure Security, NMAP* Scan *Protection, IPv4 Efficiency, MikroTik, Nginx Reverse Proxy*

Abstrak

Penelitian ini merespons masalah semakin terbatasnya alamat IPv4 dan upaya untuk meningkatkan efisiensi penggunaannya, serta melindungi server web hosting dari serangan NMAP port scan. Menggunakan metode Enhanced Explicit Port Forwarding Dari MikroTik untuk efisiensi penggunaan IPv4 dan metode Reverse Proxy untuk pengamanan dari port scan. Penelitian ini mengusulkan pendekatan yang mengintegrasikan keduanya untuk meningkatkan efisiensi infrastruktur, terutama pada server web hosting. Hasil penggunaan pengalihan port MikroTik menunjukkan bahwa hanya diperlukan satu alamat IPv4 publik/stais yang didedikasikan untuk menangani hingga 254 IP private atau IP Lokal dengan menggunakan port yang berbeda untuk nantinya dijadikan sebagai alamat server web hosting atau perangkat IoT, sedangkan implementasi Nginx sebagai Reverse Proxy memerlukan satu alamat IPv4 untuk mengkonversinya menjadi layanan web yang dapat diakses melalui DNS serta kemampuan Reverse Proxy Nginx menjadikan IPv4 dan port yang dihasilkan MikroTik tidak terlihat dari luar. Jika terjadi serangan atau dilakukan port scan pada domain yang ada pada Nginx, hasil port scan NMAP akan menunjukan port yang ada pada server Nginx berada, bukan server utama. Dengan pendekatan ini, hanya diperlukan dua alamat IPv4 untuk menangani sejumlah besar perangkat, baik untuk layanan web (seperti dalam penelitian ini) maupun perangkat lain yang memerlukan alamat IPv4 terpisah serta menghalau terjadinya port scan menggunakan NMAP untuk mengetahui alamat asli dari sebuah domain.
Kata kunci: *Keamanan Infrastruktur, Perlindungan Pemindaian NMAP, Efisiensi IPv4, MikroTik, Nginx Reverse Proxy*

I. PENDAHULUAN

Dalam era kemajuan teknologi informasi, infrastruktur jaringan memainkan peran yang sangat penting dalam menghubungkan perangkat dan layanan secara global. Namun, pertumbuhan yang pesat penggunaan perangkat yang membutuhkan akses menggunakan IP publik/statis menyebabkan alamat IP publik versi 4 (IPv4) mendekati batas kapasitasnya, ditambah dengan adanya prediksi bahwa akan ada hingga 50 miliar perangkat yang terhubung ke Internet pada tahun 2025 [1]. IPv4 adalah alamat protokol internet yang merupakan alamat 32-bit dan masalah sementara ini kita telah melihat ada lebih sedikit alamat IP sehingga di masa depan mereka akan tidak akan bisa bertahan terlalu lama [2]. Pertumbuhan internet yang pesat telah menghabiskan alokasi alamat IPv4 dari Internet Assigned Numbers Authority (IANA) [3]. Laporan statistik yang dikeluarkan oleh Regional Internet Registry (RIR) pada 7 May 2024 terkait “Internet Number Resource Report Q1 March 2024” menunjukkan bahwa sisa ruang alamat IPv4 yang tersedia di masing-masing RIR sangat terbatas. Dokumen "Number Resource Status Report (NRO) Q1-2024" mengungkapkan detail sebagai berikut:

- AFRINIC: 0.068 blok /8 (sekitar 1.140.851 alamat IPv4)
- APNIC: 0.14 blok /8 (sekitar 2.348.810 alamat IPv4)
- ARIN: 0 blok /8
- LACNIC: 0 blok /8

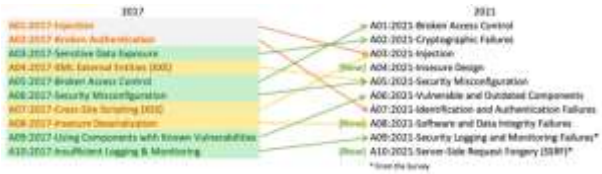
- RIPE NCC: 0 blok /8

Blok /8 mewakili 16.777.216 alamat IPv4. Total sisa alamat IPv4 yang tersedia secara global adalah sekitar 3.489.661 alamat IPv4, dari total keseluruhan 4.294.967.296 alamat IPv4 yang ada. Dengan demikian, sekitar 99.92% alamat IPv4 telah digunakan, menyisakan hanya sekitar 0.08% yang masih tersedia. Hal ini menunjukkan bahwa hampir semua blok IPv4 yang dapat dialokasikan telah digunakan, dengan hanya sedikit yang tersisa terutama di APNIC dan AFRINIC [13].

Organisasi, perusahaan, dan individu yang ingin menjalankan layanan, perangkat atau server dalam infrastruktur jaringan mereka, kini dihadapkan pada kesulitan dalam mendapatkan alokasi alamat IP yang memadai. Keterbatasan ini menjadi kendala signifikan dalam pengelolaan infrastruktur jaringan yang efisien karena saat ini menjelang habisnya IPv4, masih banyak infrastruktur yang ketergantungan bahkan tidak dapat diubah dengan mudah ke IPv6 karena banyak aspek yang tidak dapatnya dimigrasikan dengan mudah, contohnya adalah server hosting, tidak mudah mengganti alamat jaringan (IP) yang sudah didaftarkan ke dalam DNS (domain name system) sehingga untuk melakukan perubahan di dalamnya harus melakukan maintenance yang krusial seperti mematikan server atau perangkat.

Terbatasnya sisa kuota dari IPv4 dapat ditanggulangi menggunakan teknologi Network Address Translation (NAT) yang bekerja dengan cara menutupi alamat IP private/lokal dengan alamat IP publik/statis, sehingga perangkat lokal dapat mengakses internet dan layanan Internet dengan bantuan alamat IP publik yang diberikan oleh router MikroTik [4], solusi ini dikenal sebagai Enhanced Explicit Port Forwarding (EEPF) [5], namun tantangannya adalah perlu adanya mekanisme yang dapat menjembatani antara IP NAT dengan exposure akses dari external. MikroTik adalah sebuah sistem operasi berbasis Linux yang diciptakan khusus untuk kebutuhan jaringan, telah menjadi salah satu elemen penting dalam pengelolaan infrastruktur jaringan modern [6][7]. Nginx (engine-X) hadir untuk menjawab tantangan terkait EEPF tersebut, karena pada umumnya, Nginx untuk digunakan untuk membentuk kluster server dan platform internal mereka melalui Reverse Proxy Nginx [8].

Topologi atau mekanisme terkait EEPF membutuhkan alokasi IP privat/lokal serta port asli yang diteruskan/forwarding ke Dan Dari MikroTik, alhasil dengan IP public/statis yang sama namun memiliki banyak port, hal ini menjadi kurang baik karena port-port yang digunakan menjadi terekspos, tantangan dalam menjaga keamanannya pun menjadi semakin besar, karena penggunaan mekanisme keamanan jaringan dalam jaringan komunikasi seperti Firewall dan Intrusion Detection System (IDS), menjadi harus diprioritaskan dan dipertimbangkan lebih [9]. Serangan-serangan siber yang paling banyak terjadi adalah pada web server atau hosting, terutama terkait dengan serangan port scan NMAP (Network Mapper) yang menimbulkan resiko keamanan. Kembali kepada permasalahan yang disebutkan sebelumnya, terkait mekanisme EEPF yang menuntut penggunaan port di setiap servis pengalihannya (port-forward) yang jika itu dilakukan port scan akan terlihat semua port yang digunakan, baik port tersebut untuk aplikasi atau perangkat yang bersifat public atau internal/privat. Menurut laporan OWASP terkait kategori risiko yang paling signifikan terjadi disajikan pada gambar 1.



Gambar 1: Laporan OWASP - 10 Risiko Keamanan Aplikasi Web Teratas

Pada Gambar 1 OWASP (The Open Worldwide Application Security Project) menjelaskan bahwa hal-hal yang dapat terjadi terkait kerusakan pada web server, antara lain, adalah kendali akses yang rusak (Broken Access Control). Sebanyak 94% aplikasi diuji menunjukkan adanya beberapa bentuk kendali akses yang rusak, dengan 34 Common Weakness Enumerations (CWEs) terkait yang memiliki frekuensi lebih tinggi daripada kategori lainnya. Injeksi, yang mencakup 94% aplikasi diuji untuk beberapa bentuk injeksi, memiliki 33 CWEs terkait dengan kategori ini yang memiliki frekuensi kedua tertinggi. Konfigurasi Keamanan yang Salah (Security Misconfiguration) terdapat pada 90% aplikasi yang diuji, menunjukkan beberapa bentuk konfigurasi keamanan yang salah. Data ini menegaskan bahwa risiko keamanan aplikasi web memberikan kontribusi signifikan terhadap serangan pada web server atau hosting. Oleh karena itu, penanganan aspek-aspek ini menjadi sangat penting untuk menjaga keamanan infrastruktur terutama pada jalan masuk awal (port sniffing) [10].

NMAP scan adalah alat paling ampuh untuk pengendusan jaringan [11] serta pemindai keamanan yang digunakan untuk menemukan port terbuka dan layanan yang berjalan pada port tersebut di jaringan komputer [12] ditambah efisiensi pemindaian beberapa alamat IP target dengan NMAP dapat ditingkatkan [13]. Port scan adalah langkah awal dari serangan siber [14], dengan menggunakan NMAP, seorang penyerang dapat mendapatkan gambaran yang mendalam tentang layanan yang berjalan di server target, termasuk versi layanan dan sistem operasi yang digunakan oleh host tersebut [15] serta port scan adalah masalah terus-menerus pada jaringan komunikasi kontemporer dan biasanya digunakan sebagai alat pengintai serangan, mereka juga dapat membuat masalah dengan kinerja dan throughput aplikasi [16]. Serangan ini dapat memberikan informasi strategis tentang port service yang terbuka atau digunakan pada sebuah server, khususnya server web. NMAP memulai prosesnya dengan mengonversi nama host ke alamat IPv4 melalui resolusi nama DNS [11] lalu mengecek tiap-tiap layanan atau service, dengan kata lain melacak port pada komputer target. NMAP, sebagai alat pemindaian yang umum digunakan, dapat memberikan informasi krusial yang dapat dianalisis untuk mendukung serangan selanjutnya [17]

Penelitian ini akan memberikan penekanan pada solusi inovatif yang diusulkan untuk mengatasi dua permasalahan utama, yaitu efisiensi penggunaan alamat IPv4 dengan metode EEPF dan perlindungan terhadap

serangan port scan NMAP menggunakan metode Reverse Proxy. Pendekatan ini tidak hanya meningkatkan optimalisasi penggunaan alamat IPv4, tetapi juga memperkuat pertahanan terhadap serangan dari port scan NMAP, sehingga menjaga keamanan infrastruktur secara holistik. Solusi yang diusulkan akan mengintegrasikan teknologi terkini, seperti pengalihan port menggunakan MikroTik dan Nginx sebagai Reverse Proxy (peladen proksi atau server pewali), untuk mencapai efisiensi dan keamanan yang optimal dalam mengelola infrastruktur jaringan.

II. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan Enhanced Explicit Port Forwarding (EEPF) dan Reverse Proxy sebagai metode utama. EEPF digunakan untuk mengoptimalkan penggunaan alamat IPv4 dengan menangani port forwarding secara eksplisit, memungkinkan satu alamat IPv4 dapat menangani sejumlah besar perangkat atau layanan dengan port yang berbeda. Pendekatan ini berfokus pada efisiensi dan keamanan infrastruktur jaringan.

Selain itu, metode Reverse Proxy digunakan untuk menyembunyikan identitas IP Dan port sebenarnya dari server utama. Dengan menggunakan Nginx sebagai Reverse Proxy, alamat IP dan port dari Server utama dapat disembunyikan dari luar, meningkatkan lapisan keamanan dan privasi. Kombinasi kedua metode ini diharapkan dapat memberikan solusi yang efektif dalam menghadapi keterbatasan alamat IPv4 dan melindungi server dari potensi serangan NMAP port scan.

Secara rinci, MikroTik berfungsi sebagai alat port forwarding, memungkinkan penggunaan satu alamat IP publik/statis untuk melayani sejumlah perangkat di belakangnya. Nginx, sebagai Reverse Proxy dan garda terdepan, mengubah alamat IP dan port asal dari aliran pengalihan MikroTik. Perubahan ini tidak hanya meningkatkan keamanan komunikasi melalui penerapan SSL, tetapi juga menyederhanakan akses dengan mengganti alamat IP dan port menjadi nama domain yang mudah diingat.

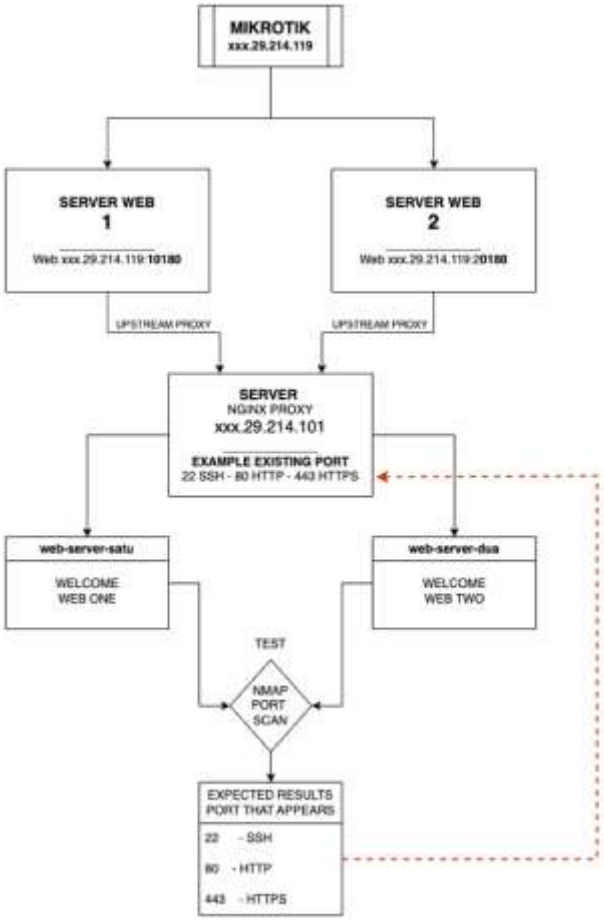
Fase pertama metodologi penelitian mencakup perencanaan topologi jaringan, dengan identifikasi kebutuhan infrastruktur seperti MikroTik, server hosting, atau mesin virtual (VM). Infrastruktur ini akan diberikan alamat IPv4 dan port melalui NAT MikroTik agar dapat diakses melalui Reverse Proxy Nginx.

Fase kedua adalah penerapan Nginx yang bertujuan untuk melindungi alamat IP dan port MikroTik, memastikan akses eksternal, dan meneruskan lalu lintas ke server hosting atau VM yang dituju. Langkah ini diperkuat dengan konfigurasi SSL/TLS untuk meningkatkan keamanan komunikasi HTTP/HTTPS yang ditangani oleh Nginx.

Fase ketiga adalah fase pengujian yang melibatkan simulasi serangan port scan menggunakan NMAP. Hasil pemindaian akan dianalisis untuk mengevaluasi keberhasilan topologi MikroTik dan Nginx. Evaluasi ini akan menilai efektivitas solusi dalam menghadapi serangan dan dampaknya terhadap performa infrastruktur secara keseluruhan.

Metode Enhanced Explicit Port Forwarding (EEPF)

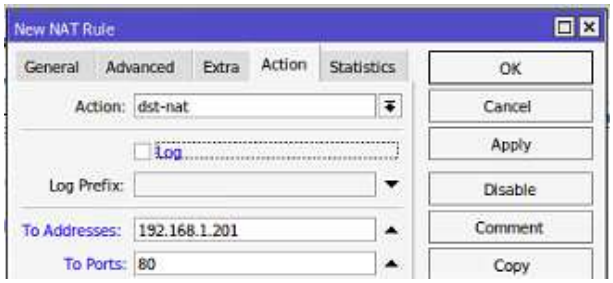
Metode Enhanced Explicit Port Forwarding (EEPF) menjadi landasan utama penelitian ini, sebagaimana tergambarkan secara rinci pada Gambar 2. Dalam konteks visualisasi alur penelitian, gambaran tersebut memberikan langkah-langkah dan proses yang akan diimplementasikan. Fokus utama dari metode ini adalah mengoptimalkan efisiensi penggunaan IPv4 dan meningkatkan tingkat keamanan terhadap serangan port scan NMAP. Melalui langkah-langkah terinci ini, diharapkan dapat tercapai solusi yang efektif dalam mengatasi keterbatasan alamat IPv4 dan menjaga keamanan infrastruktur jaringan.



Gambar 2 : Alur Penelitian: Optimasi IPv4 dan Perlindungan Terhadap NMAP Port Scan

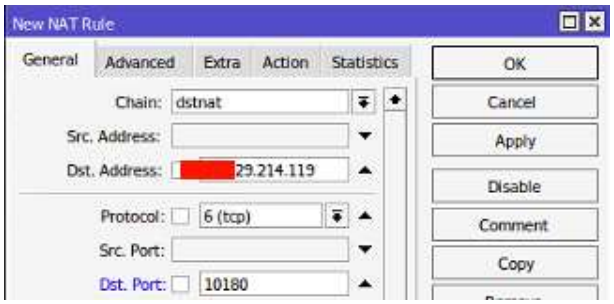
MikroTik berfungsi sebagai perangkat pengatur lalu lintas dan internet dari ISP (internet service provider) serta menggunakan IP public hingga distribusi dan alokasi IP Private ke server hosting atau perangkat lainnya. Pada penelitian ini, IP public/statis yang digunakan untuk keamanan adalah xxx.28.214.119 dan di-assign ke MikroTik. Selanjutnya, kami melakukan simulasi dengan menggunakan dua Virtual Machine/Server sebagai perwujudan Web Server.

Gambar 3 menggambarkan konfigurasi pada MikroTik IP private/lokal untuk Server 1 (192.168.1.201) dengan port 80. Adapun hasil konfigurasi tersebut adalah pengalihan port ke 10180 yang dapat dilihat pada gambar 4.



Gambar 3: Konfigurasi MikroTik IP NAT untuk server satu 192.168.1.201 dan port 80

Setelah IP private/lokal dengan port 80 dikonfigurasikan pada server, maka Server 1 dapat diakses melalui alamat http://xxx.29.214.119:10180.



Gambar 4: Konfigurasi MikroTik untuk pengalihan port IP xxx.29.214.119 ke port 10180

Gambar 4 memperlihatkan langkah-langkah konfigurasi MikroTik yang diperlukan untuk melakukan pengalihan IP private/lokal 192.168.1.201 ke IP public/statis milik MikroTik yaitu xxx.29.214.119 serta melakukan pengalihan port Dari 89 ke port 10180, sesuai dengan konfigurasi pada Server 1. Hal ini dilakukan juga pada Server 2 dengan IP private/lokal 192.168.1.202 ke IP MikroTik dan port 80 ke port 20180

Selanjutnya, Setelah menyiapkan Server 1 dan Server 2 sebagai web server, angkah berikutnya dalam pengembangan infrastruktur jaringan adalah konfigurasi Nginx sebagai Reverse Proxy pada Server 3. Reverse Proxy berfungsi sebagai pintu depan (cloudfront) yang menerima dan mendistribusikan lalu lintas internet ke server internal berdasarkan permintaan.

Gambar 5: Konfigurasi DNS

Gambar 5 menggambarkan konfigurasi DNS yang menciptakan subdomain "server1.domain" dan "server2.domain," diarahkan ke IP xxx.29.214.101. Selanjutnya, Nginx diatur untuk memasukkan Server 1 dan Server 2 dalam strukturnya, meskipun keduanya berbeda server. Hal ini karena pengguna eksternal pada dasarnya mengakses Server 3, yang kemudian melakukan Reverse Proxy ke Server 1 atau Server 2. Konfigurasi ini memungkinkan Nginx mengalihkan lalu lintas secara optimal dan merata ke Server 1 dan Server 2.

Metode Reverse Proxy

Sebagai Reverse Proxy, Server 3 berperan dalam mengonsumsi IP dari Server 1 dan 2. Lebih rinci, Server 3 melibatkan pembungkusan IP asli dari Server 1 dan 2 dengan menggunakan domain, mengamankan identitas IP sebenarnya dari server yang terletak di belakangnya. Dengan demikian, Server 3 bertindak sebagai perantara yang menghubungkan pengguna dengan Server 1 dan 2, memberikan lapisan tambahan untuk keamanan dan privasi.

Gambar 6 : Konfigurasi Nginx untuk server web 1

Gambar 6 berisikan konfigurasi Nginx untuk Server Web 1. Variabel "server_name" digunakan untuk menentukan domain (pada saat ini menggunakan nama domain server1.domain) sedangkan variabel "proxy_pass" menjadi penghubung ke alamat URL server utama yaitu http://xxx.29.214.119:10180.

Konfigurasi ini memiliki tujuan utama, yakni membangun jembatan antara nama domain dengan alamat Server 1 yang Masih berupa IP atau angka-angka. Saat mengakses domain yang telah ditentukan, terjadilah suatu proses dimana server Reverse Proxy (Nginx) menjadi penjaga gerbang yang mengarahkan permintaan kepada server utama. Dalam konteks ini, server Reverse Proxy bertindak sebagai garda terdepan, merahasiakan identitas asli server utama untuk meningkatkan lapisan keamanan.

Konfigurasi serupa diterapkan pada Server 2 dengan alamat domain server2.domain dengan akses ke Server 2 yaitu akses http://xxx.29.214.119:20180. Dengan demikian, Nginx sebagai Reverse Proxy menjelma menjadi elemen penting dalam arsitektur, memastikan keamanan dan kemudahan akses dalam setiap transaksi antara pengguna dan server utama.

Dalam melihat ke belakang, semua metode ini memainkan peran kunci dalam merancang sistem yang dapat mengoptimalkan efisiensi penggunaan IPv4 dan melindungi infrastruktur terhadap serangan port scan NMAP. Pengaturan MikroTik dan Nginx sebagai perangkat lunak Server Reverse Proxy menjadi fondasi yang kokoh untuk mencapai tujuan tersebut. Hasil dan pembahasan selanjutnya akan membawa kita lebih dalam untuk memahami dampak dan implikasi dari metode ini terhadap keamanan jaringan dan kinerja infrastruktur secara keseluruhan. Temuan yang dihasilkan akan memberikan wawasan lebih lanjut dan mendalam terkait efektivitas solusi yang telah diimplementasikan.

III. HASIL PENELITIAN

Dalam penelitian ini, metode Enhanced Explicit Port Forwarding (EEPF) sebagai landasan untuk mengatasi tantangan terkait keterbatasan alamat IPv4. EEPF memungkinkan penggunaan satu alamat IPv4 dengan lebih efisien, memfasilitasi penanganan sejumlah besar perangkat atau layanan melalui pengalihan port yang canggih. Pendekatan ini dirancang untuk meningkatkan

optimasi infrastruktur jaringan, terutama pada server web hosting.

Selain EEPF, penerapan Reverse Proxy sebagai solusi pendukung. Reverse Proxy membantu melindungi server utama dari serangan luar dan memfasilitasi distribusi lalu lintas yang optimal. Selanjutnya, penjelasan dan pengujian NMAP akan memberikan gambaran yang lebih rinci terkait efektivitas metode ini dalam mengamankan server dan mendistribusikan lalu lintas dengan optimal. Mari kita telaah lebih lanjut hasil dan temuan yang ditemukan melalui penggunaan metode ini.

Integrasi Web 1 dan Web 2 dengan Domain:

Pada ambar 10 dan Gambar 11 menandai keberhasilan terbungkusnya Web 1 dan Web 2 dengan domain masing-masing.

Gambar 7: Web 1 sudah terbungkus dengan domain

Gambar 8 : Web 2 sudah terbungkus dengan domain

Gambar 7 dan Gambar 8 menunjukkan bahwa Web 1 dan Web 2 telah berhasil terbungkus dengan domain masing-masing. Integrasi ini memastikan bahwa keduanya dapat diakses melalui domain yang telah ditetapkan DNS, memberikan kemudahan akses dan identifikasi bagi pengguna (mudah diingat). Dengan demikian, pengguna dapat mengunjungi Web 1 dan Web 2 dengan mudah melalui domain yang telah ditentukan tanpa perlu mengingat alamat IP atau port tertentu.

IV. PEMBAHASAN

Pembahasan hasil penelitian ini mengeksplorasi dampak dan implikasi dari penerapan Enhanced Explicit Port Forwarding (EEPF) dalam mengoptimalkan penggunaan alamat IPv4 dan melindungi infrastruktur jaringan dari serangan port scan NMAP. Analisis mendalam akan fokus pada temuan signifikan yang ditemukan selama penelitian, serta relevansinya dalam konteks praktis.

Pengujian NMAP Port Scan pada MikroTik:

Pengujian terhadap Server 1 dan 2 untuk memverifikasi ketersediaan akses sesuai dengan konfigurasi yang telah dibuat. Selanjutnya, pengujian NMAP Port Scan dilakukan pada IP xxx.29.214.119 milik MikroTik menggunakan NMAP dari pentest-tools.com mendapati hasil seperti pada gambar 9.

Gambar 9 : Pengujian NMAP Port Scan pada IP MikroTik

Dalam Gambar 9, kita dapat melihat hasil uji coba NMAP port scan pada IP yang dimiliki oleh MikroTik, lebih spesifiknya menuju Server 1 dan Server 2. Uji coba tersebut mengungkap bahwa port 10180 dan 20180 terdeteksi, terpapar melalui alamat akses xxx.29.214.119:10180 dan xxx.29.214.119:20180.

Penting untuk dicatat bahwa informasi ini terpampang jelas pada port scanner, menunjukkan bahwa konfigurasi berjalan dengan sukses. Meskipun demikian, ada sisi yang perlu diperhatikan: keberhasilan konfigurasi ini, meski memudahkan akses, juga membuka celah keamanan. Dengan terlihatnya informasi tentang port, kerentanan terhadap pengintai menjadi semakin nyata.

Pengujian NMAP Port Scan pada Server Reverse Proxy:

Gambar 10: Pengujian NMAP Port Scan pada IP Server Reverse Proxy

Dalam Gambar 10, terlihat pengujian NMAP Port Scan pada IP Server Reverse Proxy (xxx.29.214.101). Proses ini menggunakan alat yang sama seperti yang dijelaskan pada Gambar 9, dengan hasil pengujian NMAP port scan yang terfokus pada IP Server Reverse Proxy, yang secara spesifik melibatkan Server 1 dan Server 2.

Hasil pengujian menunjukkan bahwa port 10180 dan 20180 tidak terdeteksi, sementara port 80 (http) dan 443 (https) terlihat jelas dalam hasil port scan. Hal ini terjadi karena hanya port-port inilah yang digunakan pada server ini. Dengan demikian, konfigurasi Reverse Proxy berhasil menyembunyikan port yang sebelumnya terbuka pada Server 1 dan Server 2, menambahkan lapisan keamanan terhadap potensi serangan dari luar.

Hasil ini dapat dipahami sebagai indikasi bahwa port-port khusus yang digunakan untuk mengarahkan lalu lintas ke Server 1 (10180) dan Server 2 (20180) tetap aman dan tidak terdeteksi oleh serangan NMAP. Keberhasilan pengujian NMAP port scan pada Server Reverse Proxy menunjukkan tingkat keamanan yang

optimal, menegaskan efektivitas infrastruktur yang diimplementasikan.

Dalam konteks desain penelitian, penempatan target serangan siber pada server cloud front/Server 3 berhasil mengamankan server utama (Server 1 dan 2). Pendekatan ini bertujuan untuk mengoptimalkan operasional berbagai perangkat, termasuk IoT dan Server/Komputer, dengan hasil yang mencerminkan efisiensi dan keamanan yang tinggi. Oleh karena itu, metode penelitian ini bukan hanya memahami efektivitas solusi port forwarding dengan MikroTik dan Nginx sebagai Reverse Proxy dalam meningkatkan keamanan jaringan, tetapi juga mengukur dampaknya terhadap kinerja infrastruktur secara menyeluruh.

V. KESIMPULAN

Hasil dari penerapan Enhanced Explicit Port Forwarding (EEPF) dalam penelitian ini mengindikasikan peningkatan signifikan dalam pengoptimalan penggunaan alamat IPv4. Dengan menggunakan EEPF, satu alamat IPv4 dapat efisien menangani sejumlah besar perangkat atau layanan dengan memanfaatkan port yang berbeda. Ini menciptakan solusi yang lebih efektif dalam mengatasi keterbatasan jumlah alamat IPv4 yang tersedia.

Penerapan EEPF juga memperlihatkan kemampuan untuk mengelola lalu lintas dengan lebih baik, memungkinkan distribusi yang optimal ke berbagai server atau perangkat. Dengan demikian, infrastruktur jaringan dapat beroperasi dengan efisien tanpa kehilangan kualitas layanan.

Dalam pembahasan, EEPF menunjukkan keberhasilan dalam meningkatkan efisiensi penggunaan alamat IPv4, mengurangi kebutuhan akan alamat tambahan, dan mengoptimalkan distribusi lalu lintas. Keberhasilan ini mendukung relevansi dan efektivitas metode Enhanced Explicit Port Forwarding dalam menghadapi permasalahan keterbatasan alamat IPv4 dalam konteks penelitian ini.

Penelitian ini bertujuan untuk meningkatkan keamanan jaringan melalui solusi port forwarding dengan menggunakan MikroTik dan Nginx sebagai Reverse Proxy. Dengan latar belakang meningkatnya ancaman siber dan kebutuhan akan sistem yang efisien, penelitian ini memberikan kontribusi signifikan terhadap pemahaman tentang integrasi solusi tersebut.

Mengoptimalkan IPv4 dan Perlindungan Terhadap NMAP Port Scan:

- Integrasi Web 1 dan Web 2 dengan domain melibatkan konfigurasi Nginx sebagai Reverse Proxy, memastikan akses yang mudah dan intuitif.
- Hasil integrasi menunjukkan bahwa Web 1 dan Web 2 berhasil terhubung dengan domain masing-masing, meningkatkan keterjangkauan dan identifikasi.

Uji Keamanan dengan NMAP Port Scan:

- Pengujian NMAP Port Scan pada IP Server Reverse Proxy (xxx.29.214.101) menunjukkan ketahanan terhadap deteksi port 10180 dan 20180.
- Proses masking IP asli dari Server 1 dan 2 dengan menggunakan domain pada Server Reverse Proxy berhasil, meningkatkan lapisan keamanan.

Optimasi Kinerja Infrastruktur:

- Konsep port forwarding dengan MikroTik dan Nginx sebagai Reverse Proxy memberikan hasil positif dalam optimalisasi operasional dan peningkatan keamanan infrastruktur.
- Hasil pengujian menunjukkan bahwa konfigurasi ini dapat diandalkan, menjaga ketersediaan layanan dan keamanan jaringan.

Pengembangan lebih lanjut dari penelitian ini dapat mempertimbangkan beberapa aspek:

- Melibatkan uji coba pada skala yang lebih besar untuk mengidentifikasi kinerja dan keamanan dalam skenario produksi yang lebih kompleks, sebagai contoh menguji lebih dari 100 perangkat atau server atau maksimalkan dengan kuota dari NAT MikroTik yaitu 254 perangkat atau server.
- Mengeksplorasi solusi dan pemulihan mitigasi risiko jika terjadi kegagalan sistem, baik dari MikroTik ataupun Nginx sebagai Reverse Proxy.

Dengan implementasi dan pemahaman yang matang, solusi Port-forwarding dengan MikroTik dan Reverse Proxy Dari Nginx dapat menjadi fondasi yang kuat untuk menghadapi tantangan keamanan jaringan dan meningkatkan kinerja infrastruktur secara keseluruhan.

VI. REFERENSI

[1] Farhan, L., Hameed, R. S., Ahmed, A. S., Fadel, A. H., Gheth, W., Alzubaidi, L., ... & Al-Amidie, M. (2021). Energy efficiency for green internet of things (IoT) networks: A survey. Network, 1(3), 279-314.

[2] Jain, A., Singh, M., & Bhambri, P. (2021, August). Performance evaluation of IPv4-IPv6 tunneling procedure using IoT. In Journal of Physics: Conference Series (Vol. 1950, No. 1, p. 012010). IOP Publishing.

[3] Ashraf, S., Muhammad, D., & Aslam, Z. (2020). Analyzing challenging aspects of IPv6 over IPv4. J. Ilm. Tek. Elektro Komput. Dan Inform, 6(1), 54-67.

[4] Santoso, J. D. (2020). Analisis Perbandingan Metode Queue Pada MikroTik. Pseudocode, 7(1), 1-7.

[5] Ke, C. H., Lo, Y. W., Chen, Y. S., & Chen, H. P. (2023). An Enhanced Explicit Port Forwarding Solution for Improving Video Delivery over Software-Defined Networks. Journal of Internet Technology, 24(2), 313-321.

[6] Alamsyah, H. (2022). Perancangan dan Implementasi QoS Di MikroTik menggunakan Metode HTB (Studi Kasus SMP MBS Al Karimah Cibadak). Jurnal Teknik Informatika UNIKA Santo Thomas, 14-22.

[7] Hendrastuty, N., An'Ars, M. G., Damayanti, D., Samsugi, S., Paradisiaca, M., Hutagalung, S., & Mahendra, A. (2022). Pelatihan Jaringan Komputer (MikroTik) Untuk Menambah Keahlian Bagi Siswa

Sman 8 Bandar Lampung. Journal of Social Sciences and Technology for Community Service (JSSTCS), 3(2), 209-212.
[8] Ma, B., & Zhang, W. (2022). A Dynamic and Fair Timeout Heartbeat Detection Technique for Server Clusters Using Nginx Reverse Proxy. In Advances in Smart Vehicular Technology, Transportation, Communication and Applications: Proceedings of VTCA 2021 (pp. 341-349). Springer Singapore.
[9] E. C. Uwaezuoke and T. G. Swart, "Network Attack Analysis of an Indoor Power Line Communication Network," 2021 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), Aachen, Germany, 2021, pp. 96-101, doi: 10.1109/ISPLC52837.2021.9628606.
[10] OWASP. (2021). Owasp Top Ten. OWASP Top Ten | OWASP Foundation. https://owasp.org/www-project-top-ten
[11] Calderon, P. (2021). NMAP Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips. Packt Publishing Ltd.
[12] Punia, V., & Aggarwal, G. (2021). NETWORK FORENSIC TOOL: NMAP A PORT SCANNING TOOL [J]. Advance and Innovative Research, 8(1), 172.
[13] Liu, R. (2023, December). NMAP network scan performance optimisation. In Fourth International Conference on Signal Processing and Computer Science (SPCS 2023) (Vol. 12970, pp. 835-839). SPIE.
[14] R. Vadivel and S. Mayukha, "Port Scanning Mitigation Strategies for Penetration Testing: Blue Team Perspective," 2022 International Conference on Engineering and Emerging Technologies (ICEET), Kuala Lumpur, Malaysia, 2022, pp. 1-6, doi: 10.1109/ICEET56468.2022.10007258
[15] Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software NMAP. PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer, 7(2), 108-115.
[16] B. Hartpence and A. Kwasinski, "Combating TCP Port Scan Attacks Using Sequential Neural Networks," 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2020, pp. 256-260, doi: 10.1109/ICNC47757.2020.9049730.
[17] Liao, S., Zhou, C., Zhao, Y., Zhang, Z., Zhang, C., Gao, Y., & Zhong, G. (2020, October). A comprehensive detection approach of NMAP: Principles, rules and experiments. In 2020 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC) (pp. 64-71). IEEE.
[18] Regional Internet Registry (RIR) Statistics | The Number Resource Organization. (n.d.). https://www.nro.net/about/rirs/statistics/