Simulasi Jaringan Untuk CouchDB Dengan GNS3

Ivander [1] Justin Salim [2] Willsen Yogi Prasetia [3] Gavriel Joseph Lim [4] Sean Henry Wijaya [5]

[1)2)3)4)5)] Teknik Informatika, FTI, Universitas Tarumanagara
Jl. Letjen S. Parman No.1, RT.6/RW.16, Tomang, Kec. Grogol petamburan,
Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11440
[1)] *email : ivander.535220020@stu.untar.ac.id*, [2)] *justin.535220017@stu.untar.ac.id*, [3)] *willsen.535220010@stu.untar.ac.id*, [4)] *gavriel.535220049@stu.untar.ac.id*, [5)] *sean.535220019@stu.untar.ac.id*

ABSTRAK

Di era digital, institusi kesehatan kecil sering kesulitan membangun dan mengelola infrastruktur IT secara efisien, terutama dalam hal investasi sumber daya keuangan dan manusia. Penelitian ini mengusulkan solusi dengan menggunakan simulasi jaringan melalui Graphical Network-Simulator 3 (GNS3). Tujuannya adalah memberdayakan institusi kesehatan kecil dengan sistem keamanan komprehensif, termasuk server database dan hosting situs web. Dengan memanfaatkan Variable Length Subnet Masking (VLSM) untuk alokasi IP yang tepat, Network Address Translation (NAT) untuk keamanan akses internet, Virtual Private Connection (VPN) dengan enkripsi AES-256 dan SHA untuk komunikasi privat, serta Firewall untuk perlindungan jaringan, simulasi ini meningkatkan efisiensi operasional, mengamankan data pasien, dan menyediakan layanan kesehatan digital. Aspek aplikasi terdistribusi menggunakan Apache HTTP Server dan Apache CouchDB untuk hosting situs web dan manajemen data yang optimal.

Kata Kunci

CouchDB, GNS3, Infrastruktur IT, Keamanan Jaringan, Simulasi Jaringan

1. Pendahuluan

Dalam era digital ini, lembaga kesehatan kecil sering menghadapi kesulitan membangun dan mengelola infrastruktur IT secara efisien. Pembangunan infrastruktur seperti server, jaringan, dan sistem keamanan membutuhkan investasi finansial dan sumber daya manusia yang besar. Meskipun infrastruktur IT yang solid sangat penting untuk mendukung operasional sehari-hari dan memberikan layanan kesehatan yang optimal, banyak lembaga kesehatan kecil masih mengalami kendala dalam menyediakan infrastruktur IT yang memadai. Investasi yang besar dalam perangkat keras, perangkat lunak, dan tim IT menjadi hambatan utama. Oleh karena itu, diperlukan solusi alternatif yang efisien dan terjangkau agar lembaga kesehatan kecil dapat fokus pada pelayanan kesehatan tanpa terbebani oleh kompleksitas manajemen infrastruktur IT.

Salah satu solusi yang muncul sebagai alternatif cerdas untuk mengatasi tantangan ini adalah penggunaan simulasi infrastruktur dengan menggunakan platform seperti *Graphical Network-Simulator 3* (GNS3). GNS3 adalah perangkat lunak sumber terbuka yang digunakan oleh ratusan ribu insinyur jaringan di seluruh dunia untuk meniru, mengonfigurasi, menguji, dan memecahkan masalah jaringan virtual dan nyata. Dengan mendukung topologi kecil hingga jaringan besar yang dihosting di berbagai server atau bahkan di cloud, GNS3 memberikan fleksibilitas dalam pengembangan dan pengujian infrastruktur jaringan [1].

Dengan itu, tujuan dari penelitian ini adalah untuk membantu lembaga kesehatan kecil dengan menggunakan simulasi jaringan melalui GNS3 yang dilengkapi dengan sistem keamanan yang komprehensif, termasuk server database dan hosting website, dimana lembaga kesehatan kecil dapat meningkatkan efisiensi operasional, mengamankan data pasien dengan lebih baik, dan menyediakan layanan kesehatan secara digital. Selain itu, hal ini juga dapat memperkuat kerja sama internal antara berbagai departemen, meningkatkan aksesibilitas informasi medis, dan membantu dalam pengembangan solusi teknologi untuk mendukung proses pelayanan kesehatan.

2. Studi Pustaka

2.1 Jaringan dan Keamanan Komputer

Simulasi jaringan ini memerlukan beberapa *Virtual Machine* (VM) yang merupakan sumber daya yang menggunakan perangkat lunak daripada komputer fisik untuk menjalankan program dan mengimplementasikan aplikasi. VM dapat beroperasi secara terpisah satu sama lain, bahkan saat berjalan pada mesin fisik yang sama [2].VM yang akan digunakan adalah sebagai berikut:

1. Dua VM dengan sistem operasi *Lubuntu* untuk menyimulasikan perangkat yang akan digunakan.
2. Dua VM dengan sistem operasi *Ubuntu Server* untuk menyimulasikan server website dan database yang akan digunakan.

Untuk membagi IP kepada seluruh komponen di simulasi, kami menggunakan proses yang bernama subnetting. Subnetting adalah teknik di mana sebuah jaringan besar dibagi menjadi sejumlah jaringan yang lebih kecil, yang dikenal sebagai sub-jaringan atau subnet. Ini dilakukan untuk mengoptimalkan penggunaan alamat IP dan mengelola lalu lintas jaringan dengan lebih efisien. Dalam subnetting, setiap subnet memiliki batas alamat IP yang ditentukan oleh panjang awalan jaringan. Dua jenis subnetting umumnya digunakan, yaitu *Variable Length Subnet Mask* (VLSM) yang memungkinkan panjang awalan yang bervariasi untuk setiap subnet, dan *Fixed Length Subnet Mask* di mana semua subnet memiliki panjang awalan yang sama [3].

Proses subnetting yang akan digunakan adalah *Variable Length Subnet Mask* (VLSM) yang merupakan proses subnetting yang memungkinkan jaringan IP untuk menggunakan lebih dari satu subnet mask. Dalam VLSM, panjang awalan jaringan dapat bervariasi, memungkinkan pengelolaan alamat IP dengan lebih fleksibel.[3] VLSM di GNS3 membantu lembaga kesehatan kecil mengalokasikan alamat IP dengan presisi, efisien mendukung kebutuhan tiap departemen tanpa pemborosan sumber daya IP. Berdasarkan IP 192.168.1.0/24, subnet-subnet yang dipakai dalam simulasi ini adalah sebagai berikut:

1. Subnet A, 192.168.1.0/27 untuk 25 host
2. Subnet B, 192.168.1.32/29 untuk 15 host
3. Subnet C, 192.168.1.64/28 untuk 10 host
4. Subnet D, 192.168.1.80/29 untuk 5 host
5. Subnet E, 192.168.1.88/29 untuk 5 host

Network Address Translation (NAT) adalah teknik yang digunakan untuk menerjemahkan alamat IP privat menjadi alamat IP publik, memungkinkan perangkat di jaringan lokal untuk mengakses internet meski hanya memiliki satu alamat IP public [4]. Dalam simulasi jaringan untuk institusi kesehatan kecil, NAT dapat digunakan untuk memungkinkan perangkat di jaringan lokal institusi kesehatan untuk mengakses internet dan meningkatkan keamanan jaringan lokal dengan menyembunyikan alamat IP privat perangkat dari internet.

Simulasi ini juga menggunakan *Virtual Private Connection* (VPN), yang merupakan suatu metode untuk menyediakan jalur komunikasi pribadi dan aman di antara dua atau lebih perangkat, melalui jaringan publik, misalnya internet [5]. Pada simulasi ini, digunakan jenis VPN yang mengimplementasikan enkripsi *Advanced Encryption Standard* (AES) dengan panjang kunci 256 bit dan *Secure Hash Algorithm* (SHA) untuk verifikasi integritas data. AES-256 adalah metode enkripsi simetris, di mana kunci yang sama digunakan untuk enkripsi dan dekripsi data, sementara SHA digunakan untuk memastikan bahwa data yang dikirimkan melalui jalur VPN tetap tidak terubah dan utuh [6]. Keamanan yang tinggi dari AES-256, yang merupakan standar enkripsi yang sangat kuat, bersama dengan mekanisme verifikasi integritas menggunakan SHA, membuatnya cocok untuk melindungi data yang dikirimkan melalui jalur VPN.

Selain VPN, sebuah Firewall juga diterapkan untuk meningkatkan keamanan jaringan dari simulasi. Firewall adalah suatu perangkat atau perangkat lunak yang berfungsi sebagai baris pertahanan pertama untuk mencegah akses yang tidak sah atau potensial merugikan, dengan memantau, memfilter, dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan [7]. Dalam simulasi ini, implementasi Firewall menggunakan *Cisco ASA 9.8.1*, yang memastikan bahwa hanya aktivitas jaringan yang diizinkan dan aman yang dapat berinteraksi di jaringan simulasi.

Dengan demikian, simulasi ini dapat mengoptimalkan alokasi alamat IP melalui VLSM, meningkatkan keamanan jaringan dengan NAT, menyediakan jalur komunikasi pribadi dan aman melalui VPN dengan enkripsi AES-256 dan SHA, serta memastikan kontrol akses yang ketat melalui implementasi Firewall menggunakan *Cisco ASA 9.8.1*. Secara keseluruhan, implementasi ini akan memungkinkan lembaga kesehatan kecil untuk meningkatkan efisiensi operasional, mengamankan data pasien, dan menyediakan layanan kesehatan secara digital.

2.2 Aplikasi Terdistribusi

Dalam simulasi ini, dua server akan didedikasikan untuk tujuan spesifik. Salah satunya akan berfungsi sebagai server peng-hosting website menggunakan *Apache HTTP Server*, sementara server lainnya akan menangani hosting database yang berbasis *Apache CouchDB*.

Apache HTTP Server adalah perangkat lunak server web open-source yang dikenal sebagai salah satu server web paling handal dan populer di dunia. Digunakan oleh jutaan situs web, Apache menyediakan lingkungan yang kuat dan aman untuk meng-hosting konten web. Kelebihan utama *Apache HTTP Server* adalah fleksibilitasnya, mendukung berbagai modul tambahan dan konfigurasi yang memungkinkan administrator untuk menyesuaikan pengaturan sesuai kebutuhan spesifik.

Apache CouchDB, di sisi lain, adalah sistem manajemen basis data berbasis dokumen yang memungkinkan penyimpanan, pencarian, dan pengindeksan data dengan struktur semi-terstruktur. CouchDB menggunakan format JSON untuk menyimpan data, membuatnya ideal untuk aplikasi yang membutuhkan fleksibilitas dan skalabilitas. Database ini memiliki kemampuan replikasi yang kuat, memungkinkan data untuk disinkronkan antara beberapa node, yang berguna untuk meningkatkan ketersediaan dan ketahanan sistem.

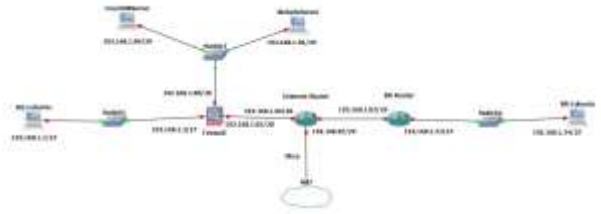
Kedua server ini, *Apache HTTP Server* dan *Apache CouchDB*, akan bekerja sama dalam simulasi ini untuk menyediakan lingkungan yang optimal bagi lembaga kesehatan kecil dalam meng-hosting website dan

mengelola data pasien dengan efisien. *Apache HTTP Server* akan memastikan pengiriman konten web yang cepat dan aman, sementara *Apache CouchDB* akan menyediakan sistem manajemen basis data yang andal dan skalabel.

3. Hasil Percobaan

3.1 Instalasi dan Pengaturan

Pertama-tama, kami akan menetapkan tata letak sesuai dengan Gambar 1 di dalam lingkungan simulasi GNS3. Ini mencakup penempatan VM *Lubuntu* dan *Ubuntu Server*, firewall *Cisco*, dan router *Cisco*. yang disesuaikan dengan kebutuhan simulasi, beserta pengaturan alamat IP untuk setiap komponen. Untuk memastikan kemudahan dan keterbacaan, kami akan menggunakan layanan *Sistem Nama Domain* (DNS) yang disediakan oleh *Google*.



Gambar 1. Layout GNS3

Untuk konfigurasi Firewall, dilakukan seperti yang bisa dilihat di Tabel 1. Dengan ini, interface *Gi0/0* dapat mengakses *Gi0/1* dan *Gi0/2*, interface *Gi0/1* hanya dapat mengakses *Gi0/2*, dan interface *Gi0/2* tidak dapat mengakses zona apapun.

Tabel 1 Konfigurasi alamat IP dan tingkat sekuritas di Firewall.

interface	Alamat IP (Subnet)	Tingkat Sekuritas	Nama Zona
Gi0/0	192.168.1.2 (27)	100	*inside*
Gi0/1	192.168.1.89 (29)	50	*dmz*
Gi0/2	192.168.1.65 (28)	0	*outside*

Semiripnya, konfigurasi Alamat IP untuk Internet-Router dapat dilakukan seperti di Tabel 2. Selain itu, perintah *ip route 192.168.1.32 255.255.255.224 192.168.1.82* akan juga dijalankan untuk membuat rute statis ke subnet D.

Tabel 2 Konfigurasi alamat IP di Internet-Router.

interface	Alamat IP (Subnet)
fa0/0	192.168.1.66 (26)
fa0/1	192.168.1.81 (29)
fa1/0	dhcp

Setelah konfigurasi alamat IP dan rute sukses, Internet-Router juga akan dipakai sebagai ‘penyambung’ ke Internet melalui NAT. Untuk melakukan itu, konfigurasi NAT serta *Access Control List* (ACL)-nya dapat dilakukan dengan perintah sebagai berikut.

1. ip nat outside
2. int fa0/0
3. ip nat inside
4. exit
5. access-list 1 permit 192.168.1.0 0.0.0.31
6. access-list 1 permit 192.168.1.64 0.0.0.15
7. access-list 1 permit 192.168.1.88 0.0.0.7
8. ip nat inside source list 1 interface fa1/0 overload

Dan untuk konfigurasi alamat IP yang terakhir, dapat dilihat di Tabel 3 untuk konfigurasi IP di BR-Router. Mirip seperti Internet-Router, kami juga akan membuat rute statis ke subnet E dengan menjalankan perintah *ip route 192.168.1.64 255.255.255.240 192.168.1.81*.

Tabel 3 Konfigurasi alamat IP di BR-Router.

interface	Alamat IP (Subnet)
fa0/0	192.168.1.82 (29)
fa0/1	192.168.1.33 (27)

Selanjutnya, kami akan mengkonfigurasikan DNS, rute default, dan mengelola lalu lintas ICMP serta mengatur NAT dinamis pada firewall dengan cara mengaktifkan DNS lookup untuk antarmuka outside dan mengatur server DNS dengan grup DefaultDNS menggunakan alamat 8.8.8.8 dan 8.8.4.4. Setelah itu, tentukan rute default ke 192.168.1.66, aktifkan inspeksi ICMP pada kebijakan global, dan terakhir, konfigurasi NAT dinamis untuk subnet *inside* dan *dmz* menuju *interface* outside.

Supaya perangkat yang berada di interface *outside* dapat mengakses server yang berada di interface *dmz*, kami harus menerapkan NAT statis untuk mentranslasi alamat untuk layanan server web dan server CouchDB. Dengan menggunakan alamat IP yang tidak dipakai di subnet C, yang merupakan subnet yang berada di interface *outside*, kami dapat menggunakan alamat 192.168.1.67 dan 192.168.1.68 untuk kedua server tersebut melalui port 80 untuk server web dan 5984 untuk server CouchDB.

Dan yang terakhir di GNS3, demi keamanan, akan ditambahkan VPN antara Internet-Router dan BR-Router menggunakan enkripsi AES-256 dan fungsi hash SHA. Keduanya berbagi kunci 'salim' untuk mengamankan komunikasi. Pengaturan mencakup pembentukan kebijakan ISAKMP, transform-set untuk enkripsi IPsec, dan pemetaan kripto untuk menentukan parameter keamanan. ACL juga diterapkan untuk membatasi lalu lintas yang dienkripsi, yaitu diantara subnet C dan subnet D.

Untuk kedua VM *Ubuntu Server*, jalankan perintah *sudo vim /etc/netplan/00-installer-config.yaml* dan isi file tersebut dengan tulisan yang dapat ditemukan di Gambar 2 yang berisi konfigurasi untuk VM Apache. Untuk VM CouchDB, ganti address-nya menjadi 192.168.1.90/29.

```
network:
  ethernets:
    enp0s3:
      #dhcp4: true
      addresses:
        - 192.168.1.91/29
      routes:
        - to: default
          via: 192.168.1.89
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

Gambar 2. Isi dari 00-installer-config.yaml untuk VM Apache

Setelah selesai, jalankan perintah *sudo netplan apply* di kedua VM tersebut untuk memperbarui konfigurasi network. Untuk meng-install dan menyalakan CouchDB, jalankan kumpulan perintah berikut di VM Apache:

1. sudo snap install couchdb
2. sudo snap set couchdb admin=password
3. sudo snap start couchdb
4. sudo snap connect couchdb:mount-observe
5. sudo snap connect couchdb:process-control

Jika instalasi CouchDB berhasil, akses menuju web interface-nya melalui interface *inside* adalah dengan membuka browser dan memasukkan URL http://192.168.1.90:5984/_utils/ dan jika melalui interface *outside* adalah dengan memasukkan URL http://192.168.1.67:5984/_utils/. Masukkan admin sebagai username dan password sebagai password.

Untuk meng-install dan menyalakan website di VM Apache, jalankan kumpulan perintah berikut:

1. sudo apt install apache2
2. sudo ufw allow “Apache Full”
3. sudo a2enmod ssl
4. sudo systemctl restart apache2
5. sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

Di bagian ini, input prompt yang penting hanya-lah pada bagian *Common Name*, input 192.168.1.91 saat prompt muncul. Setelah itu, lanjut dengan perintah *sudo vim /etc/apache2/sites-available/192.168.1.91.conf* dan input teks yang sesuai dengan Gambar 3 yang akan meredireksi HTTP ke HTTPS dan juga menambah sumber dari file website.

```
<VirtualHost *:443>
    ServerName 192.168.1.91
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
<VirtualHost *:80>
        ServerName 192.168.1.91
        Redirect / https://192.168.1.91/
</VirtualHost>
```

Gambar 3. Isi dari 192.168.1.91.conf

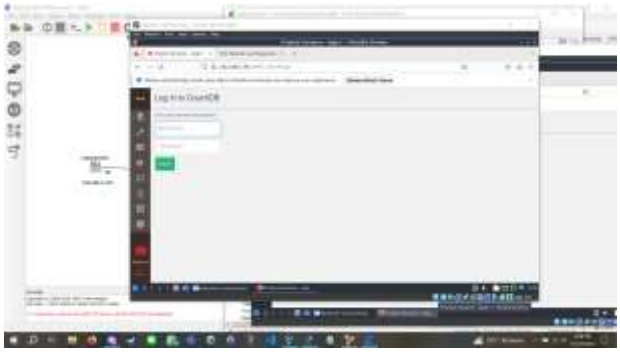
Setelah itu, jalankan perintah-perintah berikut:

1. sudo a2ensite 192.168.1.91.conf
2. sudo systemctl reload apache2

Jika konfigurasi server Apache betul, maka anda dapat mengakses website melalui URL 192.168.1.91 untuk perangkat di interface *inside* dan URL 192.168.1.68 jika berada di interface *outside*.

3.2 Hasil Simulasi

Pertama-tama, kami akan mencoba membuka database CouchDB melalui interface *inside* dengan URL http://192.168.1.90:5984/_utils/ dengan hasil seperti Gambar 4, dan membuka database CouchDB melalui interface *outside* dengan URL http://192.168.1.67:5984/_utils/ dengan hasil seperti Gambar 5.



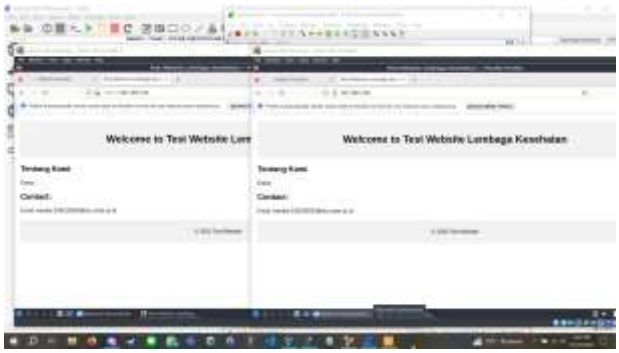
Gambar 4. CouchDB dari interface *inside*

Gambar 5. CouchDB dari interface *outside*

Setelah login, kita dapat memasukkan langsung data ke database dengan file JSON, misalnya data pasien, mau dari interface *inside* maupun interface *outside*. Di Gambar 6, bisa dilihat bahwa data yang di-input berhasil disimpan oleh database.

Gambar 6. Data pasien di CouchDB dari interface *inside*

Jadi dari sini, bisa disimpulkan bahwa server CouchDB telah berhasil di-inisialisasi dan berfungsi dari kedua interface. Berikutnya adalah uji coba untuk server Apache. Akses website melalui interface *inside* dengan URL 192.168.1.91 dan melalui interface *outside* dengan URL 192.168.1.68. Dari Gambar 7, dapat disimpulkan bahwa website dapat diakses dari kedua interface dengan tampilan yang sama.



Gambar 7. Tampilan website dari kedua interface

Dan yang terakhir, kami dapat melihat dari Gambar 8 bahwa VPN berfungsi dengan baik, karena ada protokol *Internet Security Association and Key Management Protocol* (ISAKMP) yang dipakai di jaringan penghubung saat mengakses kedua server diatas melalui interface *outside*.

Gambar 8. Hasil Wireshark dari BR-Router menuju Internet-Router

Beberapa kelebihan yang dapat diidentifikasi dari simulasi ini meliputi:

1. Topologi yang Mudah Dimengerti dan Murah untuk Dirawat: Simulasi menggunakan topologi yang sederhana dan mudah dipahami, memudahkan pengaturan dan pemeliharaan. Hal ini juga menjadi solusi yang ekonomis bagi lembaga kesehatan kecil.
2. Penggunaan VPN yang Aman: Implementasi VPN mengamankan koneksi dari interface outside, memberikan lapisan keamanan tambahan untuk komunikasi data yang sensitif.
3. Penggunaan Firewall yang Terkontrol: Firewall diterapkan dengan baik, memastikan bahwa setiap zona hanya dapat diakses oleh perangkat tertentu. Ini mengoptimalkan kontrol akses dan menjaga integritas jaringan.

Namun demikian, beberapa kekurangan masih dapat diidentifikasi:

1. Keterbatasan Fleksibilitas dan Skalabilitas Topologi: Meskipun topologi yang digunakan efektif untuk ukuran saat ini, namun mungkin kurang fleksibel dan skalabel untuk pertumbuhan masa depan. Pertimbangan perubahan topologi yang lebih dinamis dapat meningkatkan adaptabilitas.
2. Penyempurnaan Pengelolaan Sumber Daya: Upaya lebih lanjut dapat dilakukan untuk menyempurnakan pengelolaan sumber daya, memastikan optimalitas kinerja dan penggunaan resource pada setiap elemen jaringan.
3. Interface *outside* tidak memiliki akses internet karena tidak memiliki NAT yang memiliki ACL yang menerima perangkat-nya.

4. Kesimpulan

Secara keseluruhan, simulasi ini memberikan fondasi yang solid untuk infrastruktur IT lembaga kesehatan kecil. Dengan memperhatikan kelebihan dan kekurangan, perbaikan selanjutnya dapat difokuskan pada peningkatan fleksibilitas topologi, optimalisasi pengelolaan sumber daya, dan penambahan akses internet untuk interface *outside*.

REFERENSI

[1] Neumann, Jason C., 2015, "The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More 1st Edition", No Starch Press, California.
[2] Smith, J.E., Nair, Ravi., “The architecture of virtual machines”, IEEE Network, New Jersey.
[3] Semeria, Chuck., 1996, “Understanding IP Addressing: Everything You Ever Wanted To Know”, 3Com Corporation, Massachusetts.
[4] Muller, A., Carle, Georg., Klenk, Andreas., 2008, “Behavior and classification of Nat Devices and implications for Nat Traversal”, IEEE Network, New Jersey.
[5] Ferguson, Paul., Huston, Geoff., 1998, “What is a VPN?”, O'Reilly Media, California.
[6] Stallings, William., 2022, “Cryptography and Network Security: Principles and Practice, Global Edition”, Pearson Education Limited, Essex.
[7] Noonan, Wes., Dubrawsky, Ido., 2006, “Firewall Fundamentals: An introduction to network and computer firewall security”, Cisco Press, Indiana.